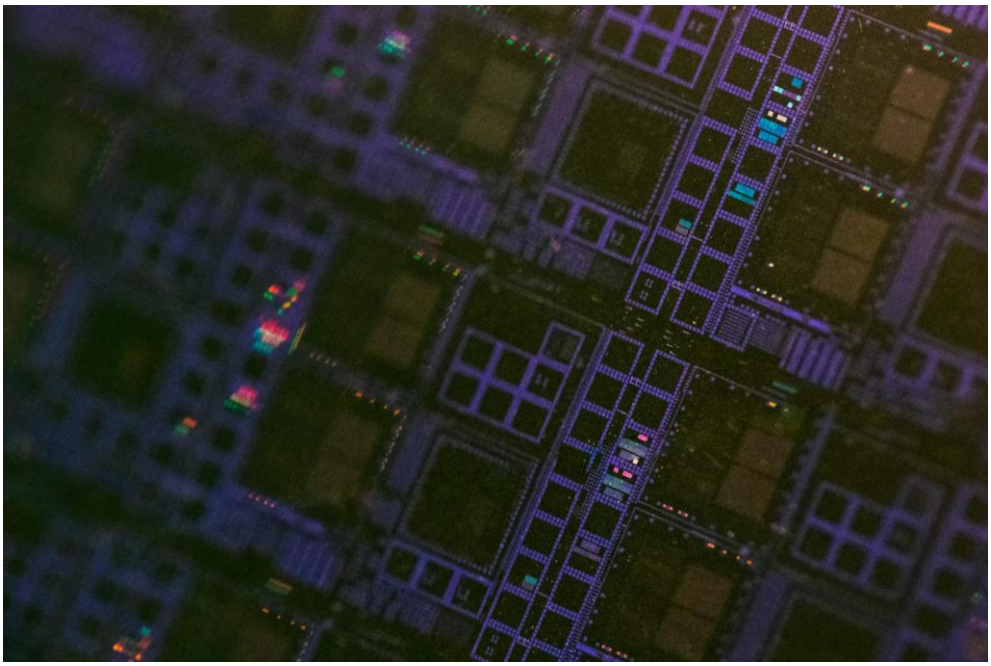
**Par Laetitia Della Torre**

# Numérique humanitaire et protection des données : colonialité, souveraineté et dignité



**Thèse présentée pour l'obtention du grade de Docteur de l'UTC**

Soutenue le 17 décembre 2024
Spécialité : Sciences de l'information et de la communication

**Université de technologie de Compiègne**

**École doctorale « Sciences de l'ingénieur »**

**Laboratoire COSTECH, EA 2223**

# Numérique humanitaire et protection des données : colonialité, souveraineté et dignité

Thèse de doctorat en Science de l'Information et de la Communication

présentée par

Laetitia DELLA TORRE

sous la direction de

Jérôme VALLUY

Soutenue publiquement le 17 décembre 2024

Membres du jury :

Didier Bigo, Professeur des Universités émérite, Sciences-PO Paris-CERI, King's College London.

David Flacher, Professeur des Universités, Université technologique de Compiègne.

Mathieu Quet, Directeur de recherche, HDR, Université Paris Cité, rapporteur.

Sandrine Turgis, Maîtresse de conférences, HDR, Université de Rennes 1, IODE (CNRS UMR 6262) et chercheuse-associée au CREC (Saint-Cyr Coëtquidan), Université Rennes 1, rapporteure.

Jérôme Valluy, Maître de conférences HDR, Université Paris 1 Panthéon-Sorbonne,

chercheur au COSTECH-UTC, directeur de thèse.

## Résumé

### Résumé français

Exploitation de données par des multinationales, cyberattaques, multiplication d'opérations de désinformation, l'espace numérique contemporain est agité par un nombre croissant de tensions qui n'épargnent pas les humanitaires, d'autant que le secteur a entamé depuis une dizaine d'années une numérisation de ses opérations. Les ONG ont en effet adopté progressivement une série d'outils numériques, que ce soient des logiciels de traitement de données géographiques, des drones, des dispositifs biométriques, des agents conversationnels, voire des blockchains ou des intelligences artificielles. Ces organisations sont donc particulièrement vulnérables aux dérives du capitalisme de surveillance et des tensions géopolitiques traversant l'espace numérique. Les bénéficiaires en sont les premières victimes. Et l'on en vient à la contradiction suivante : les humanitaires — des acteurs engagés dans la protection de victimes de crises — ont adopté des outils numériques qui peuvent porter atteinte à leur vie privée, voire les mettre en danger.

L'objectif de cette thèse est de tenter de comprendre la nature de ce paradoxe, ce qui nécessite de creuser les différentes dynamiques et tensions accompagnant la numérisation de l'humanitaire. Cette dernière découle tout d'abord de la quantification de l'aide, elle - même liée à l'exigence des bailleurs d'améliorer la redevabilité des ONG et la traçabilité des fonds. La numérisation de l'humanitaire s'inscrit en outre dans un rapprochement plus général du milieu de la solidarité internationale avec le secteur privé. Ce mouvement s'accompagne de la diffusion d'un impératif d'innovation ainsi que par un imaginaire solutionniste des nouvelles technologies. Mais cet impératif d'innovation relèverait plutôt pour des chercheuses comme Kristin Sandvik ou Mirca Madianou d'une forme de « technocolonialisme ». Des dynamiques de pouvoir résultant de legs coloniaux participent en effet à la construction des bénéficiaires comme de potentiels « sujet » passifs d'expérimentation, et ce aux dépens du respect de leur vie privée. Les crises relèvent en outre de régimes d'exception facilitant l'expérimentation de technologies dans un contexte de suspension du cadre juridique en vigueur. Toutefois, ce tableau peut être nuancé. On assiste en effet à une échelle plus générale à un mouvement de régulation de l'innovation, qui se traduit par une série de lois comme le règlement sur la protection des données (RGPD), le Digital Markets Act, l'Artificial Intelligence Act, etc. Et ces dernières concernent aussi l'humanitaire. Une partie de notre thèse est donc consacrée au travail des délégués à la protection des données intervenant dans les ONG humanitaires. On se demandera comment ils se sont emparés des différents outils de régulation du risque numérique imposés par le RGPD. Or ce dernier repose sur une démarche de compliance qui n'est pas sans limites.

On étudiera ensuite une deuxième dynamique contribuant à renforcer les risques liés à la numérisation du milieu de la solidarité internationale. Elle concerne le resserrement de l'espace humanitaire, en lien avec l'exercice des souverainetés étatiques, et sa traduction sur le plan informationnel et numérique. Dans un premier temps, on reviendra donc sur la façon dont les échanges de données entre ONG et États hôtes sont perçus et encadrés, ces derniers pouvant être considérés comme étant légitimes, mais aussi comme facteur de risque, surtout

s'ils sont associés à des formes de violence d'État et à une criminalisation des bénéficiaires de l'aide. Dans un second temps, on prendra en compte le fait que le processus de numérisation de nos sociétés accompagne et renforce aussi un phénomène au long cours de recompositions des souverainetés. Ce phénomène est aussi lié à l'entrée en scène d'une série d'acteurs non étatiques, des entreprises évidemment, comme les GAFAM, mais aussi d'autres groupes plus informels, comme des hackers. L'implication de cybercombattants dans des conflits contemporains s'inscrit dans un long mouvement de contestation du monopole de la violence des États du fait de la multiplication de conflits intraétatiques — à l'encontre de groupes terroristes par exemple — et l'implication d'acteurs privés dans la conduite de la guerre, comme des hackers donc. On s'intéressera aux impacts en matière de vie privée liés à deux sujets s'y rattachant : le contre-terrorisme ainsi que les cyberopérations touchant les ONG. Or ces dernières, en protégeant les bénéficiaires contre ces différentes menaces, courent le risque de réduire ces derniers à être de simples « objets de protection » et des victimes passives. Mais on verra que les humanitaires s'efforcent aussi de prendre en compte leurs droits garantis par le RGPD (notamment relatifs à leur autodétermination informationnelle) et de défendre ainsi leur dignité.

Mots clés :

Humanitaire, numérique, protection des données, cybersécurité, innovation, souveraineté

Résumé anglais :

The exploitation of data by multinationals, cyber-attacks, the proliferation of disinformation operations - today's digital environment is shaken by a growing number of tensions which do not spare humanitarian aid, especially as the sector has been digitalising its operations for the last ten years. NGOs have gradually adopted a series of digital tools, including data processing software, drones, biometric devices and conversational agents, blockchains and artificial intelligence. These organisations are therefore particularly vulnerable to the excesses of surveillance capitalism and the geopolitical tensions running through the digital space. The beneficiaries are the first victims. And this brings us to the following contradiction: humanitarians - actors committed to protecting the victims of crises - have adopted digital tools that can infringe on their privacy, or even put them in danger.

The aim of this thesis is to attempt to understand the nature of this paradox, which requires us to examine the different dynamics and tensions that accompany the digitalisation of the humanitarian sector. First of all, the digitisation of humanitarian aid stems from the quantification of aid, which is itself linked to donors' demands to improve the accountability of NGOs and the traceability of funds. The digitisation of the humanitarian sector is also part of a more general move by the international aid community towards the private sector. This movement is accompanied by the spread of an innovation imperative and by a solution-oriented vision of new technologies. But for researchers such as Kristin Sandvik and Mirca Madianou, this innovation imperative is more akin to a form of "techno-colonialism". The dynamics of power resulting from colonial legacies contribute to the construction of beneficiaries as potential passive 'subjects' of experimentation, at the expense of respect for

their privacy. The crises are also characterised by exceptional regimes that facilitate the experimentation of technologies in a context of suspension of the legal framework in force.

However, this picture can be nuanced. On a more general scale, we are witnessing a movement to regulate innovation, reflected in a series of laws such as the Data Protection Regulation (RGPD), the Digital Markets Act, the Artificial Intelligence Act, etc. These laws also affect humanitarian aid. Part of our thesis is therefore devoted to the work of data protection officers working in humanitarian NGOs. Part of our thesis is therefore devoted to the work of data protection officers attached to humanitarian NGOs. But we will also see that the latter is based on a compliance approach that is not without its limits.

We will then look at a second dynamic which is contributing to increasing the risks associated with the digitisation of the international solidarity sector. In short, it concerns the shrinking of humanitarian space, linked to the exercise of state sovereignty, and its translation into informational and digital space. Firstly, we will look at how data exchanges between NGOs and host countries are perceived and regulated. These exchanges can be seen as legitimate, but also as a risk factor, particularly if they are associated with forms of state violence and the criminalisation of aid beneficiaries.

Secondly, we will take into account the fact that the digitisation of our societies also accompanies and reinforces a long-term phenomenon of recompositions of sovereignty. This phenomenon is also linked to the entry onto the scene of a series of non-state actors, obviously companies such as the GAFAMs, but also other more informal groups such as hackers. The involvement of cybercombatants in contemporary conflicts is part of a long movement to challenge the State's monopoly on violence as a result of the proliferation of intra-State conflicts - against terrorist groups, for example. In short, we will be looking at the impact on privacy of two issues: counter-terrorism and cyber-operations affecting NGOs. But by protecting their beneficiaries against these various threats, NGOs run the risk of reducing them to mere 'objects of protection' and passive victims. However, we will see that humanitarians are also endeavouring to take account of the rights guaranteed by the RGPD (particularly with regard to their informational self-determination) and to defend their dignity.

Key words: humanitarian, data protection, cybersecurity, digitalization, innovation, sovereignty

## Remerciements

Avant toute chose, je tiens à exprimer mes remerciements les plus chaleureux à toutes les personnes m'ayant soutenue durant ma thèse.

Mes premiers remerciements vont à mon directeur de recherche, Jérôme Valluy, dont les encouragements enthousiastes et nombreux conseils m'ont grandement aidé tout le long de mes recherches.

Je dois en partie la décision de me lancer dans un doctorat aux exilés du camp de Katsikas, ils m'ont donné le courage nécessaire pour faire ce choix. Merci à vous !

Je témoigne aussi toute ma reconnaissance pour les structures m'ayant permis de réaliser cette thèse. Un très grand merci à l'Université de technologie de Compiègne et au laboratoire du Costech d'avoir contribué à la concrétisation de ce travail.

Une thèse devant beaucoup aux rencontres et aux recommandations de personnes appartenant, ou non, au monde académique, j'adresse donc mes plus vifs remerciements à l'ensemble des personnes qui ont pu inspirer les lignes qui vont suivre.

Je pense aux membres de l'équipe EPIN du Costech, ainsi qu'à Julien Rossi, sans qui je n'aurais sûrement jamais rien compris au RGPD.

Un grand merci à Charles Lenay et Cléo Collomb de m'avoir accompagné lors des différents Comités de suivi individuels, merci pour leurs retours et suggestions.

Toute ma gratitude va aux personnes que j'ai contactées et qui ont accepté de partager de leur temps si précieux pour répondre à mes questions.

Je suis aussi redevable de l'aide d'Alain et de Sylviane, mes relecteurs impitoyables, que je remercie pour leur assistance dans les derniers temps de la rédaction du manuscrit.

Ma thèse aurait été bien plus pénible sans tous mes proches qui ont égayé mon quotidien monacal de doctorante.

Merci à vous, Nadia, Célia et Pierrot pour votre singularité tout humaine.

Je remercie mes parents sans qui rien n'aurait été possible. Merci à ma mère, infirmière, pour m'avoir transmis sa ténacité et à mon père, ingénieur télécoms, sa curiosité intellectuelle. Cette thèse au croisement du numérique et de l'humanitaire vous doit évidemment beaucoup.

Merci à mon compagnon et camarade, Cyrille, d'avoir été toujours là — même dans les coups durs de la recherche — et d'avoir supporté mes obsessions rgpdiennes bien que tu aurais préféré discuter freudo-marxisme.

Enfin, je réserve mes derniers remerciements à mon chat, Apache, pour son soutien indéfectible, quand bien même il a grandement compliqué la rédaction de cette thèse en élisant régulièrement domicile sur le clavier de mon ordinateur.

## Table des matières

## Acronymes

ACF : Action Contre la Faim

ACLU : American Civil liberties union

ADN : acide désoxyribonucléique

AFD : Agence française de développement

AFPA : Agence nationale pour la formation professionnelle des adultes

AIPD : Analyse d'impact sur la protection des données

ANALP : Active Learning Network for Accountability and Performance in humanitarian action

ANSSI : Agence nationale de sécurité des systèmes d'information

APC : Association for Progressive Communications

APT : Advanced Persistent threat

ATM : Automated Teller Machine

AWS : Amazon Web Service

BATX : Baidu, Alibaba, Tencent et Xiaomi

BIMS : Biometric Identity management system

CDR : Call detail record

CEPD : Comité européen de la protection des données

CERN : Conseil européen pour la recherche nucléaire

CERT : Computer emergency response team

CGU : Conditions générales d'utilisation

CICR : Comité internationale de la Croix-Rouge

CJUE : Cour de justice de l'Union Européenne

CLOUD ACT : Clarifying Lawful Overseas Use of Data Act

CNCDH : Commission nationale consultative des droits de l'homme

CNIL : Commission nationale de l'informatique et des libertés

CPI : Cour pénale internationale

CRASH : Centre de réflexion sur l'Action et les savoirs humanitaires

CRF : Cellule de renseignement financier

DDOS : Distributed Denial Of Service attack

DJI : Da Jiang Innovation

DFID : Department for International Development

DHS : Department of homeland security

DIGID : Dignified Identities in Cash Assistance

DIH : Droit international humanitaire

DPO : Data protection officer

ECHO : European Civil Protection and humanitarian aid operation

ECPC : European Centre on Privacy and Cybersecurity

EDRI : European Digital Rights

EPFL : Ecole Polytechnique fédérale de Lausanne

FBI : Federal bureau of investigation

FISA : Foreign Intelligence surveillance act

FMI : Fond monétaire international

GAFAM : Google Amazon Facebook Apple Microsoft

GAFI : Groupe d'action financière

GAO : Government Accountability Office

GAVI : Global Alliance for Vaccines and Immunization

GCHQ : Government Communications Headquarters

GPA : Global privacy assembly

GPS : Global positioning system

Groupe URD : Groupe Urgence Réhabilitation Développement

GSMA : Global System for Mobile Communications Association

HART : Homeland advanced recognition technology

HHI : l'Harvard Humanitarian Initiative

HIP : Humanitarian Innovation Project

HOT : Humanitarian openstreetmap team

IA : Intelligence artificielle

ICE : United States Immigration and Customs Enforcement

IDENT : Automated Biometric Identification System

IFRC : International Federation of Red-Cross

IMCP : International Commission on Missing Persons

INTERPOL : International criminal police organization

IRD : Institut de recherche pour le développement

IVR : Interactive Voice Response

KYC : Know Your Customer

LBC/FT : lutte contre le blanchiment de capitaux et le financement du terrorisme

MIT : Massachusetts Institute of technology

MOU : Memorandum of understanding

MSF : Médecins sans Frontières

NATU : Netflix Airbnb Tesla Uber

NRC : Norwegian Refugees Council

NSA : National Security Agency

NTIC : Nouvelles technologies de l'information et de la communication

OCHA : United Nations Office for the Coordination of Humanitarian Affairs

OBIM : Office of biometric identity management

ODI : Overseas Development Institute

OCDE : Organisation de coopération et de développement économiques

OEWG : Open ended working group

AFD: Agence française de développement

OFAC : Office of Foreign Assets Control

OI : organisation internationale

OIM : Organisation internationale pour les migrations

OMS : Organisation mondiale pour la santé

ONG : Organisation non gouvernementale

ONU : Organisation des Nations unies

OS : Operating system

OSC : Organisations de la société civile

OSINT : Open source intelligence

OTAN : Organisation du traité de l'Atlantique nord

PICUM : Platform international cooperation on undocumented migrants

PIMS : Personal identity management system

PNUD : Programme des Nations-Unies pour le développement

PRIMES : Population registration and identity management ecosystem

PVS : Partner vetting system

PWC : PricewaterhouseCoopers

R&D : Research and development

RFL : Restoring Familly Links

RGPD : Règlement Général sur la protection des données

SIC : Sciences de l'information et de la communication

SIG : Système d'information géographique

SMS : Short message service

STS : Science and technology studies

TCP/IP : Transmission Control Protocol/Internet Protocol

TSC : Terrorist screening centre

TRACFIN : Traitement du renseignement et action contre les circuits financiers clandestins

UAV : Unmanned Aerial Vehicle.

UE : Union Européenne

UNESCO : United Nations Educational, Scientific and Cultural Organization.

UNHCR : United Nations High Commissioner for Refugees

UNICC : United Nations International Computing Centre

UNICEF : United Nations International Children's Fund

UNOSAT : United Nations Satellite Centre

UNRWA : United Nations Relief and Works Agency for Palestine Refugees in the Near East

UNWOMEN : United Nations Entity for Gender Equality and the Empowerment of Women

USAID : United States Agency for International Development

USSD : Unstructured Supplementary Service Data

WFP : World Food program

WP29 : The Article 29 Working Party

## Introduction

En 2019, une organisation internationale humanitaire impliquée dans la lutte contre la faim, le World food Program (WFP) a fait l'objet de vives critiques en raison d'un partenariat avec Palantir, une entreprise d'analyse de données massives [1]. En effet, cette firme a été financée par le fonds In-Q-Tel, soit un fonds de capital-risque de la Central Intelligence agency (CIA). Ajoutons que les logiciels fournis par Palantir sont utilisés par de nombreux services de renseignements, dont la Direction générale de la sécurité intérieure (DGSI), ainsi que par différentes armées, comme les forces ukrainiennes et israéliennes. La société a en outre noué un contrat avec le Service fédéral américain de l'immigration dans le cadre de la politique répressive de Donald Trump à l'égard d'exilés latino-américains.

Il est évident qu'un tel partenariat n'est pas sans risques en matière d'atteinte à la vie privée. En effet, étant donné la proximité de Palantir avec des services de renseignement, comment s'assurer que les données des bénéficiaires de WFP sont gardées confidentielles ? Le WFP s'est défendu en avançant que Palantir n'aurait pas accès aux données personnelles traitées par l'organisation humanitaire. Seule cette dernière pourrait les consulter sur ses serveurs. Cette affirmation a cependant été mise en doute au regard du manque de transparence imputé à Palantir[2].

En tout cas, le partenariat entre le WFP et Palantir a entrainé une levée de boucliers au sein du secteur humanitaire. Des tribunes et des articles de journaux ont été publiés dans la presse spécialisée. Or cette affaire n'est pas isolée. Le milieu de la solidarité internationale a été ébranlé par d'autres « techlash »[3]. On connait l'affaire Snowden ou Cambridge Analytica. Les humanitaires ont quant à eux dénoncé le transfert de données biométriques d'exilés rohingyas par le Haut-commissariat aux réfugiés (HCR) à la Birmanie[4]. Ils ont été indignés par l'arrêt de distributions alimentaires par le WFP à des bénéficiaires yéménites au motif d'un refus de partage de données biométriques[5]. Et ils ont été choqués par la cyberattaque d'ampleur ayant touché la base de données du service de rétablissement des liens familiaux du Comité international de la Croix-Rouge (CICR) début 2022. Cette dernière a exposé les données de près de 500 000 personnes, dont des bénéficiaires de l'organisation[6]. Ces

---

[1] « Ce partenariat s'appuie sur un projet pilote initial entre Palantir et le PAM, à l'origine de l'outil d'optimisation de la chaîne d'approvisionnement du PAM nommé Optimus. Cette application rassemble des données et permet la visualisation des valeurs nutritionnelles, lieux d'approvisionnement, délais de livraison et coûts de divers aliments, permettant aux utilisateurs de comparer toutes les options simultanément pour prendre de meilleures décisions. Jusqu'à présent, Optimus a permis au PAM d'économiser 30 millions de dollars ; les économies devraient atteindre 100 millions de dollars par an lorsque l'outil sera déployé dans toute l'organisation. »
WFP, "Palantir et le Programme Alimentaire Mondial forment un partenariat pour améliorer l'aide humanitaire mondiale", 5 février 2019, https://fr.wfp.org/communiques-de-presse/palantir-et-le-programme-alimentaire-mondial-forment-un-partenariat-pour Nous précisons que l'implication de Palantir dans l'action humanitaire daterait de 2013 (…), et que le WFP a travaillé avec Palantir depuis 2017 (les premiers contacts du WFP avec l'entreprise remonteraient à 2015 au Forum économique mondial) SCHROEDER Andrew, Directrelief, "Palantir Technology Enables Intelligent Typhoon Response", 22 novembre 2013, https://www.directrelief.org/2013/11/palantir-technology-enables-intelligent-typhoon-response/

[2] MARTIN, Aaron, "Aidwashing surveillance : critiquing the corporate exploitation of humanitarian crises", *Surveillance & society*, 21 (1), 2023, p.96-102

[3] Techlash, Anglicisme, mot valise composé de « tech » et « backlash ». Il désigne un « sentiment fortement négatif à l'encontre des technologies modernes et des grandes sociétés technologiques. »
https://dictionary.cambridge.org/dictionary/english/techlash

[4] Human Rights watch, "UN shared Rohingya data without informed consent", 15/06/2021 https://www.hrw.org/news/2021/06/15/un-shared-rohingya-data-without-informed-consent

[5] PARKER, Ben, SLEMROD, Annie, "UN gives ultimatum to Yemen rebels over reports of aid theft", *The New humanitarian,*17/06/2019 https://www.thenewhumanitarian.org/news/2019/06/17/un-yemen-rebels-aid-theft-biometrics

[6] The Guardian, AFP, "Hacking attack on Red Cross exposes data of 515,000 vulnerable people", 20/01/2022 https://www.theguardian.com/world/2022/jan/20/hacking-attack-on-red-cross-exposes-data-of-515000-vulnerable-people

quelques exemples sont révélateurs des nouvelles formes de vulnérabilité liées à la numérisation de l'humanitaire. On pressent également le type de risque que cette dernière peut représenter pour les bénéficiaires de l'aide. Et pourtant, les ONG publient des politiques de « transformation numérique ». Des postes de « digital transformation adviser » sont créés. Les ONG se dotent d'outils de gestion de données toujours plus pointus : IA, blockchains, etc. Et malgré les différents scandales qu'on a évoqués en ouverture, les NTIC sont en partie associées par les humanitaires à des valeurs positives. Les projets de cartographies participatives permettraient l'émancipation des bénéficiaires. Les applications d'agents conversationnels (chatbots) amélioreraient la communication entre ONG et victimes de catastrophes et de conflits. Dans le même temps, les intelligences artificielles rendraient l'aide plus efficiente, et assisteraient à la prise de décision en contexte de crise. Il est espéré qu'elles permettraient même d'anticiper des catastrophes naturelles. La biométrie et les blockchains réduiraient la fraude et faciliteraient la traçabilité de l'aide. En un mot, il existe au sein du secteur une conception instrumentale des nouvelles technologies (NTIC), voire une forme de technosolutionnisme. Par exemple, Patrick Vink définit le numérique humanitaire comme « l'utilisation de la technologie pour *améliorer* la qualité des efforts de prévention, d'atténuation, de préparation, de réaction, de récupération et de reconstruction. »[7] On en vient donc à la contradiction suivante : les humanitaires — des acteurs engagés dans la protection de victimes de crises — ont adopté des outils numériques qui mettent potentiellement en danger ces dernières. Or, les humanitaires eux-mêmes en sont — dans une certaine mesure — conscients. Pierrick Devidal, membre du CICR, formule lui-même ce paradoxe : « les technologies numériques sont des outils exceptionnels pour les humanitaires qui s'efforcent d'alléger les souffrances des populations touchées par les conflits et les catastrophes. (…) C'est le bon côté des choses, mais la transformation numérique rend aussi l'aide moins humaine et plus opaque. (…) Ces paradoxes numériques sont partis pour durer. »[8]

L'objectif de cette thèse est alors de tenter de comprendre la nature de ce paradoxe, ce qui nécessite de creuser les différentes dynamiques et tensions accompagnant la numérisation de l'humanitaire. Le cas de Palantir n'est pas isolé. Il a fait scandale, dans le sens où il déroge aux principes éthiques humanitaires, mais il est révélateur de tensions plus profondes entre redevabilité, nécessité d'efficience et protection des bénéficiaires. Un des arguments motivant la décision du WFP était en effet la nécessité de rendre plus efficace la délivrance des opérations humanitaires[9]. Or ce souhait traduit la diffusion d'un impératif d'innovation ainsi que par un imaginaire solutionniste des nouvelles technologies, renforcé par un rapprochement plus général du milieu de la solidarité internationale avec le secteur privé. Mais cet impératif d'innovation relèverait plutôt pour des chercheuses comme Kristin Sandvik ou Mirca Madianou d'une forme de « technocolonialisme », et plus généralement d'une forme de « colonialité » qu'ont pu analyser Nick Couldry et Ulisses Mejias. On peut ajouter

[7] « the use of technology to improve the quality of prevention, mitigation, preparedness, response, recovery and rebuilding efforts VINCK Patrick, "Humanitarian Technology, World Disasters Report", *International Federation of Red Cross and Red Crescent Societies*, 2013, www.ifrc.org/PageFiles/134658/WDR%202013%20complete.
pdf

[8] « Digital technologies are exceptional assets for humanitarians striving to alleviate the suffering of populations affected by conflict and disasters.(...) That's the bright side.The digital transformation is also making aid less human and more opaque. (...) These digital paradoxes are here to stay. »
DEVIDAL, Pierrick, ""Back to basic" with a digital twist : humanitarian principles and dilemmas in the digital age.", *Humanitarian Law & Policy*, 02/02/2023, https://blogs.icrc.org/law-and-policy/2023/02/02/back-to-basics-digital-twist-humanitarian-principles/

[9] PORCARI, Enrica, "A statement on the WFP-Palantir partnership", Medium, 07/02/2019
https://medium.com/world-food-programme-insight/a-statement-on-the-wfp-palantir-partnership-2bfab806340c

que les ONG sont aussi particulièrement vulnérables à des dynamiques rattachées aux répercussions de l'exercice des puissances étatiques dans le cyberespace. Il nous faudra donc définir le concept de souveraineté, ainsi que ses traductions numériques et la manière dont les ONG perçoivent ces risques et tentent de protéger leurs bénéficiaires contre ces derniers, quitte à les réduire à un statut de victime. Toutefois, on resituera notre dernier concept, celui de dignité. En effet, si l'humanitaire peut être analysé sous le prisme de la notion de biopolitique, et si ce concept a été largement employé pour décrire le secteur de l'aide, ce dernier aussi caractérisé par un régime moral spécifique, qui ne se limite pas à être une « politique de la vie ». Les humanitaires sont aussi attachés à la défense des droits des bénéficiaires accordés par les lois relatives à la protection des données, et les acteurs de la solidarité internationale accordent une grande importance à une série de principes normatifs qu'on va détailler.

## État des connaissances scientifiques

### Définir l'humanitaire : principes éthiques et lecture biopolitique de l'aide

Définir le secteur humanitaire est certes un enjeu scientifique, mais il s'agit également d'un acte de légitimation[10] de la part d'acteurs appartenant à un champ professionnel plus fragilisé qu'il le semblerait. À vrai dire, certains chercheurs évoquent même une « crise identitaire » de l'humanitaire. Cette dernière serait pour partie due à une technicisation de l'aide, à une perte de sa dimension militante, à un rapprochement avec le secteur privé, voire avec des acteurs militaires[11]. L'espace humanitaire se serait complexifié. Dans les crises interviendrait maintenant une multiplicité d'acteurs, que ce soit des acteurs étatiques ou privés, que se soit l'armée ou des Casques bleus, ou des entreprises.

Alors, peut-être en réaction à cette complexification de l'aide, certains humanitaires donnent une définition du secteur très restrictive. Par exemple, un praticien comme Rony Brauman, membre fondateur de Médecins sans frontières (MSF), a commencé par limiter l'humanitaire à la médecine d'urgence[12]. Il justifie cette définition resserrée par une critique du « tout humanitaire », et par son regret « que tout ce qui, de près ou de loin, peut être présenté ou perçu comme une action secourable est étiquetée humanitaire. » [13] Or cette limitation de l'aide à la médecine d'urgence peut être critiquée. Tout d'abord parce que la frontière entre urgence et temps long du développement est régulièrement discutée, une même organisation

[10] « Elle est ligne de partage dans les esprits ; elle organise les perceptions, les discours, les pratiques. Elle est constamment négociée, bougée (y compris imperceptiblement) et remise en jeu par ses usages. Ibid.

[11] AUDET, François. « L'acteur humanitaire en crise existentielle : les défis du nouvel espace humanitaire. » *Études internationales*, volume 42, numéro 4, décembre 2011, p. 447–472. https://doi.org/10.7202/1007550ar
« Cette tension – à la fois crise de croissance et crise d'identité – est profonde et générale. Elle tire le mouvement humanitaire vers deux « sorties », deux fins et deux reconversions : la privatisation de l'humanitaire d'une part, l'humanitaire d'État d'autre part » AGIER, Michel, *Gouverner les indésirables, des camps de réfugiés au gouvernement humanitaire*, Paris : Flammarion, 2008,352 p.

[12] « À travers prises de parole publiques, articles, livres [Brauman et Portevin, 2006 ; Brauman, 2010], elle est à la fois exigeante, centrée sur le non-gouvernemental et limitative. Pour Brauman, n'ont vocation à recevoir le qualificatif d'"humanitaires" que des organisations avant tout privées, agissant dans une temporalité restreinte et essentiellement axée sur l'urgence, prioritairement médicale. » RYFMAN, Philippe, *L'histoire de l'humanitaire*, Paris : La Découverte, 2016, p.115.

[13] BRAUMAN, Rony, « Contre l'humanitarisme. » *Esprit (1940-)*, no. 177 (12), 1991, p. 77–85.

pouvant jouer sur plusieurs registres et des échelles de temps différentes[14]. Et le mandat d'ONG humanitaire s'est élargi à d'autres champs que la médecine. Rony Brauman a toutefois élargi progressivement sa définition. Dans un article publié sur le site du centre de recherche de MSF, il indique trois « balises » pour naviguer dans le paysage flou de l'aide : le contexte de crise (qu'il décrit comme une rupture brutale d'équilibre) ; l'indépendance du champ politique, nécessaire à une action déployée en confiance ; et enfin l'intentionnalité du geste humanitaire, caractérisé par le souci de l'autre et non la défense d'intérêts[15].

Cette définition de l'humanitaire a une dimension normative. Et il est vrai que pour différencier ce qui en relève ou non, certains acteurs de l'aide ont eux-mêmes largement recours à des valeurs morales. Le cadre éthique forgé par le CICR fait référence. Il est résumé par les principes humanitaires d'Humanité, d'Impartialité, de Neutralité, d'Indépendance, voire de Volontariat, d'Unité et d'Universalité[16]. Ces derniers permettraient de préserver la dignité des bénéficiaires, en fondant leur action sur un cadre éthique. Ils sont également essentiels afin de préserver ce qui a été conceptualisé comme « espace humanitaire ». Rony Brauman, ancien président de Médecins Sans Frontières, le décrit comme suit : il s'agit « un espace symbolique, hors duquel l'action humanitaire se trouve détachée [de son] fondement éthique et qui se constitue à l'intérieur des repères suivants : accès, dialogue, indépendance, impartialité. Ceci implique d'une part la liberté de dialogue, la possibilité de parler librement avec les gens au service de qui l'on travaille, sans subir de pression systématique de quiconque. C'est une question élémentaire de dignité qui ne va pourtant pas d'elle-même. Il faut d'autre part la liberté de mouvement et d'évaluation des besoins, dans toute la mesure où les conditions pratiques le permettent, bien sûr. » [17]

Ce souci de l'autre peut aussi relever de l'ordre de l'affectif. Ainsi Didier Fassin a utilisé une catégorie — la raison humanitaire — reposant sur le principe d'un traitement moral de la vie humaine qui est placée au-dessus des autres valeurs[18]. Cette dernière s'appuie sur une morale de la compassion et sur le fait de considérer la vie comme un bien ultime, soit une forme de « biolégitimité »[19]. Plus précisément, Didier Fassin s'intéresse à la circulation d'émotions et de

---

[14] OLIVIER DE SARDAN, Jean-Pierre, « Aide humanitaire ou aide au développement ? La "famine" de 2005 au Niger », *Ethnologie française*, 2011/3 (Vol. 41), p. 415-429 https://www.cairn.info/revue-ethnologie-francaise-2011-3-page-415.htm
DAVEY, Eleonor, « L'action humanitaire au-delà des French doctors », *Alternatives humanitaires*,n°1 Février 2016 https://www.alternatives-humanitaires.org/fr/2016/01/10/laction-humanitaire-au-dela-des-french-doctors/

[15] BRAUMAN, Rony, « L'Action humanitaire », MSF CRASH, 01/05/1994 https://msf-crash.org/fr/publications/acteurs-et-pratiques-humanitaires/laction-humanitaire

[16] « Les principes humanitaires définissent ce en quoi consiste l'aide humanitaire : apporter une aide vitale aux populations dans le besoin, sans établir aucune distinction pénalisante entre elles. Ils distinguent l'aide humanitaire des autres activités, de nature notamment politique, religieuse, idéologique ou militaire. »
Direction générale de la protection civile et des opérations d'aide humanitaire européennes (ECHO), Les Principes humanitaires, https://civil-protection-humanitarian-aid.ec.europa.eu/who/humanitarian-principles_fr Protection civile et Operation d'Aide humanitaire européennes, Les principes humanitaires.
PICTET, J. « Les principes du droit international humanitaire », *Revue Internationale de la Croix-Rouge*,48(573),1996, p.411-425.
PALMIERI,Daniel, "Les principes de la Croix-Rouge: une histoire politique", *ICRC*, 06/07/2015
https://www.icrc.org/fr/document/les-principes-fondamentaux-de-la-croix-rouge-une-histoire-politique

[17] BRAUMAN, Rony, *Humanitaire, le dilemme*, Paris, Textuel, 1996, p.29

[18] FASSIN, Didier, *La raison humanitaire, Une histoire morale du temps présent*, Paris : Seuil, 2010, 368 p.

[19] « C'est dire que plutôt que le biopouvoir, qui est un pouvoir sur la vie, l'étude des sociétés contemporaines invite à considérer la biolégitimité, qui est la légitimité de la vie, autrement dit la reconnaissance de la vie biologique comme bien suprême. D'un concept à l'autre, c'est — pour penser une fois encore avec Michel Foucault — une nouvelle problématisation de la vie qui s'opère. Il ne s'agit pas de saisir comment on la façonne, la régule, la normalise. Il s'agit, dans une démarche très différente et presque inverse, de comprendre comment

normes dans l'espace social, caractérisant un moment historique particulier, les années 1990. Ces dernières correspondent à la cristallisation d'un gouvernement humanitaire. Ce terme — comme l'auteur le précise — désigne un ensemble très large de dispositifs pour administrer et favoriser l'existence des êtres humains[20]. Il inclut ainsi à la fois des acteurs étatiques que des ONG. Cette description est donc très englobante, mais elle nous permet de nous rappeler que le mandat premier des organisations humanitaires n'est pas la défense des droits de l'homme, mais la préservation de l'existence des êtres humains. La valeur cardinale de l'humanitaire serait de reconnaitre la légitimité de la vie biologique[21]. D'ailleurs, pour Hugo Slim, spécialiste en éthique, le principe d'humanité, qui est au cœur de la définition de l'humanitaire, équivaut à : « l'attitude humaine de prendre soin des autres humains en raison d'une profonde et universelle conviction que la vie est meilleure que la mort, et que vivre bien signifie être traité humainement. » [22] Mais l'humanitaire court alors le risque d'être réduit à la préservation de la « vie nue », et donc à la protection d'un corps sans droits. Les bénéficiaires seraient incarnés par la figure de l'« homo sacer » pour reprendre la notion de Giorgio Agamben. Et pour le chercheur Bernard Hours[23], les humanitaires placeraient le droit à la vie comme droit absolu, aux dépens des autres droits de l'homme garantis à tout à chacun. Les bénéficiaires de l'aide auraient un statut de victimes passives, et seraient maintenus dans leur situation d'exclus. Et le geste humanitaire se réduirait à la gestion et à la gouvernance d'indésirables. Ainsi Michel Agier résume le gouvernement humanitaire[24] par les termes d'exclusion, d'extraterritorialité et d'exception.

Le gouvernement humanitaire opère tout d'abord dans des zones extraterritoriales, que Michel Agier décrit comme des « hétérotopies », soit un concept forgé par Foucault en 1967 dans sa conférence « des espaces autres »[25]. En effet, en raison de leur situation excentrée, les camps sont la traduction géographique de l'exclusion sociale des réfugiés. Par exemple, le chercheur Romain Huet a pu rattacher la condition migratoire à l'expérience de la défamiliarisation et par conséquent de la perte de toute vie privée. Les exilés sont en effet réduits à être « ballotés » de non-lieux en non-lieu[26].

---

elle s'inscrit de manière complexe, incertaine, ambiguë au cœur de nos systèmes de valeurs et d'actions, de nos économies morale et politique. »
FASSIN, Didier « La biopolitique n'est pas une politique de la vie », *Sociologie et sociétés* 38, nº 2 (2006), p. 35–48. https://doi.org/10.7202/016371ar

[20] FASSIN, Didier, « Et la souffrance devint sociale. De l'anthropologie médicale à une anthropologie des afflictions », *Critique*, 2004/1-2 (n° 680-681), p. 16-29. https://www-cairn-info.ezproxy.utc.fr/revue-critique-2004-1-page-16.htm

[21] « la gestion des réfugiés en France et le traitement du sida en Afrique du Sud mettent en jeu des politiques de la vie qui, au-delà d'évidentes différences du point de vue des problématiques et des contextes, participent d'une même configuration morale dans laquelle la vie physique s'impose comme valeur supérieure et la raison humanitaire comme idéal éthique. C'est dire que plutôt que le biopouvoir, qui est un pouvoir sur la vie, l'étude des sociétés contemporaines invite à considérer la biolégitimité, qui est la légitimité de la vie, autrement dit la reconnaissance de la vie biologique comme bien suprême. »

[22] SLIM Hugo, "The Power of humanity : of being human now and in the future", *ICRC blog*, 30 /06/2019, https://blogs.icrc.org/law-and-policy/2019/07/30/power-of-humanity-being-human-now-future/
« Humanity in this sense is human behavior that cares for other humans because of a profound and universally held conviction that life is better than death, and that to live well means being treated humanely in relationships of mutual respect. »
FAST, Larissa, "Unpacking the principle of humanity: Tensions and implications", *IRRC*, No. 897/898, 2016

[23] HOURS, Bernard, *L'idéologie humanitaire ou la spectacle de l'altérité perdue,* Paris: Les Éditions L'Harmattan, 1998, 173 p.

[24] Michel Agier utilise le terme de « gouvernement humanitaire », pour décrire un dispositif dédié à la gestion des indésirables. Ce dispositif est mondialisé, réticulaire, et se déploie sur plusieurs continents. Il adopte diverses formes, et inclue des ONG, mais aussi des intervenants publics et privés, gouvernementaux, ou non. Le camp de réfugiés en est l'incarnation la plus aboutie et complète.

[25] FOUCAULT, Michel, « "Des espaces autres" », *Empan*, 2004/2 (nº54), p. 12-19. https://www.cairn.info/revue-empan-2004-2-page-12.htm

[26] HUET, Romain, "Expérience de l'exil, de la précarité et performativité politique : un questionnement philosophique sur l'expérience sociale de « l'exilé »", *Implications philosophiques*, 19/01/2018 https://www.implications-philosophiques.org/experience-de-lexil-de-la-precarite-et-performativite-politique/

Deuxièmement, le gouvernement humanitaire est un espace d'exception, dans le sens où il serait placé en dehors du système juridique usuel. En effet, les ONG interviennent elles-mêmes dans des camps ou des lieux de rétentions[27]. Ce sont des espaces de non-droit, à la définition juridique incertaine, comme les hotspots par exemple[28], les zones d'attentes[29], ou encore les centres de détention administrative. Et les ONG opèrent aussi dans des situations de crises, de conflits ou de catastrophes, soit des moments de suspension du droit commun. Les moments de crises peuvent donner lieu à l'instauration d'un état d'urgence, ou bien de régimes juridiques dérogatoires, ce qui n'est évidemment pas sans implications sur l'application de lois de protection des données.

Enfin, le gouvernement humanitaire est un espace d'exclusion, de gestion des indésirables. Michel Agier emprunte à Hannah Arendt sa figure de l'apatride, du « sans droit »[30]. La gestion des parias suppose une série d'opérations de gouvernance, à savoir leur identification, leur classification, leur contrôle, et en fin de compte leur mise à distance et exclusion de la Cité. Et le gouvernement humanitaire met donc une balance entre modèle sanitaire (prophylactique) et sécuritaire (policier). Michel Agier met alors en regard le criminel, ayant perdu ses droits, bannis de la Cité, et la victime. Toutefois, Michel Agier se distancie de la pensée de Giorgio Agamben et de sa notion de « vie nue », qui fige les rapports de pouvoirs et ne permet pas d'envisager ce que Michel Agier a pu qualifier des formes de « resubjectivation » de la part d'exilés, des formes de résistance au gouvernement humanitaire[31]. De surcroit, les ONG n'auraient pour finalité que la préservation de la vie des bénéficiaires ? On peut nuancer ce point[32]. Il existerait plutôt, comme on le verra, une tension entre le fait de remplir les besoins minimaux des bénéficiaires, mission de protection de ces derniers et la nécessité de défendre leurs droits, cristallisée par la notion de dignité.

---

[27] FISCHER, Nicolas, « Un lieu d'exception ? Retour sur le statut de la rétention administrative dans un contexte démocratique », *Politix*, 2013/4 (N° 104), p. 181-201. https://www.cairn.info/revue-politix-2013-4-page-181.htm

[28] RODIER,Claire, « Le faux semblant des *hotspots* », *La Revue des droits de l'homme*, 13 | 2018 http://journals.openedition.org/revdh/3375
BEULAY, Marjorie, CHAUMETTE, Anne-Laure, DUBIN, Laurence, EUDES, Marina, *Encampés de quel(s) droit(s) ?,* Institut francophone pour la justice et la démocratie, n°25 V1, 2020, 480 p.
BASILIEN,GAINCHE, Marie Laure, « Les droits de migrants en Europe : la normalisation de l'exception », in MARTI,G., CARPANO, E., *L'Exception en droit de l'Union européenne,* PUR, 2019, p. 249-264.

[29] CHOWRA, Makaremi, « Les "zones de non-droit" : un dispositif pathétique de la démocratie. », *Anthropologie et Sociétés*, volume 32, number 3, 2008, p. 81–98. https://doi.org/10.7202/029717ar

[30]« Les individus sans-Etat représentent le phénomène le plus nouveau de l'époque contemporaine. On ne retrouve en eux aucune des catégories ni des règlements issus de l'esprit du XIX[e] siècle. Ils sont tout aussi éloignés de la vie nationale des peuples que les luttes de classe de la société. Ils ne sont ni des minoritaires, ni des prolétaires, ils sont en dehors de toutes les lois. » ARENDT, Hannah, *Le déclin de l'Etat-nation et la fin des Droits de l'Homme*, in: Hannah Arendt, *Les origines du totalitarisme. L'impérialisme* (tome 2), Paris : Points essais,1982, p. 253

[31] « Ce qui pose problème dans cette affirmation d'Agamben n'est pas tant le concept de « vie nue » qui synthétise les multiples formes du pouvoir absolu sur la vie (et donc du pouvoir de mort) que peuvent avoir à un moment donné en un lieu donné les institutions et organisations qui décident de soigner et de ne pas soigner des personnes à l'abandon, les faire vivre ou les laisser mourir. Cela est pour ainsi dire une des formes possibles du « monde vide » déjà évoqué plus haut. Ce qui pose problème dans les analyses d'Agamben est la supposée transformation de ce pouvoir (plus précisément ce « biopouvoir ») en un modèle de la politique et l'idée de l'incarnation exacte de ce modèle dans la forme du camp. Par cette figuration abstraite et déductive, le camp est ramené en dernière analyse à un pur espace de mort, une mort sociale avant d'être une mort physique comme l'ont été les camps d'extermination auxquels Agamben réduit finalement la figure et le sens du camp en général, ce que contredisent toutes les enquêtes de terrain dans les camps existants. » AGIER, Michel. "Quel Temps Aujourd'hui En Ces Lieux Incertains?" *L'Homme*, no. 185/186, 2008, p 105–20 http://www.jstor.org/stable/40379454.
AGIER, Michel, « Penser le sujet, observer la frontière », *L'Homme*, p. 203-204, 2012, http://journals.openedition.org/lhomme/23096

[32] DELPHA,Isabelle, » humanitaire et biopolitique », Université Européenne d'été du réseau OFFRES, 2003, Nice, France. p.75-90.

## Le numérique humanitaire

Cette section a pour objectif de préciser ce qu'est le « numérique humanitaire ». Pour ce faire, on commencera par brosser un premier tableau de la littérature académique existante, afin d'avoir un aperçu de la façon dont est abordé cet objet par différentes disciplines, spécifiquement par les sciences de l'information et de la communication.

Pour effectuer cette revue de la littérature, nous avons évidemment consulté de façon extensive les différentes bases de données à notre disposition (Cairn, Google scholar, Erudit, etc.). On a parcouru des sites de laboratoire de recherche travaillant sur l'humanitaire, ou pouvant s'y rapprocher (études africaines, études de développement). On a vérifié que ce sujet n'avait pas été traité dans des carnets de recherche (comme Hypothèses). On s'est aidé de la base de données du site Internet de Calenda, pour rechercher des appels à projets sur ce sujet. On a également utilisé des mots clefs plus thématiques, par types de technologies (intelligence artificielle, drone, blockchain, cartographie, etc.). On a exploré les publications de plusieurs groupes de recherche comme celui d'Urgence Réhabilitation Développement (URD). On a lu des publications d'Alternatives Humanitaires, du groupe de recherche de MSF et de la revue de Médecins du monde, Humanitaires, enjeux, pratiques, débats. Et donc encore une fois, on n'a en fin de compte, déniché que quelques publications

Or, on s'est rapidement rendue compte qu'il n'existe, à notre connaissance, que de rares travaux francophones sur le sujet. Cela est aussi valable pour les sciences de l'information et de la communication. D'ailleurs, le mot clef « humanitaire » sur le site de la SFIC n'a donné que peu de résultats. Il existe quelques articles ponctuels de chercheur, comme celui de Florine Garlot[33]. Un numéro d'Hermès de 2022 a été publié sur cette question[34], ou encore plus récemment les Cahiers du Numérique porte sur ce sujet[35]. Les chercheurs axent leur article sur la communication des organisations, et la façon dont elles sont médiatisées par la presse. L'humanitaire y est traité comme un objet communicationnel. Cet angle est toutefois adopté plus largement par des chercheurs d'autres disciplines. Luc Boltansky — auteur de l'ouvrage « La souffrance à distance »[36] — est par exemple sociologue. L'urgentiste Rony Brauman et le journaliste René Backman ont également écrit « Les médias et l'humanitaire »[37]. Le politiste Pascal Dauvin « La communication humanitaire. »[38] Ces recherches portent sur ce qui pourrait constituer une « rhétorique humanitaire », usant majoritairement du registre moral et émotionnel[39]. D'autres chercheurs questionnent le recours du secteur à des agences de communication et ses conséquences en matière de surenchère communicationnelle[40].

---

[33] GARLOT, Florine, « Pourquoi (re)penser la communication de solidarité internationale ? », *Communiquer*, n° 29, 2020.
[34] OUSTINOFF Michael**,** RUIZ Ugo (dir.), *Les ONG à l'épreuve de la com',* Hermès, 2022/1 (n° 89) p. 272
[35] La désintermédiation des ONG en Europe, Communications et pratiques face au défi du numérique, 2024/1-2 (Vol.20), 98 p.
[36] BOLTANSKI, Luc, *La Souffrance à distance. Morale humanitaire, médias et politique*, Paris: Éditions Métailié, 1993,288 p.
[37] BRAUMAN, Rony, BACKMANN, René, *Les médias et l'humanitaire, éthique de l'information ou charité-spectacle*, Paris : CFPJ, 1998, 176 p.
[38] DAUVIN, Pascal, *La communication des ONG humanitaires*, Paris : L'Harmattan, 2010, 202 p.
[39] PEROUSE DE MONTCLOS, Marc-Antoine, « Du développement à l'humanitaire, ou le triomphe de la com' »*, Revue Tiers-Monde*, Armand Colin, 2009, vol. 0(4), p.751-766.
NGOUANA, Lyonnelle, «L'espace de la communication des organisations humanitaires comme espace de négociation d'enjeux de légitimité », *Études internationales*, volume 51, number 3, fall 2020, p. 455–479. https://doi.org/10.7202/1085606ar
[40] Publics des ONG humanitaires, http://publictionnaire.huma-num.fr/notice/publics-des-ong-humanitaires/

De surcroit, à l'heure de la rédaction de la thèse, il semblerait que l'usage des réseaux sociaux à des finalités de communication par les acteurs humanitaires ait été peu abordé. On a pu toutefois trouver quelques articles plus généraux portant sur les formes de philanthropies individuelles sur les réseaux, sur l'usage de ces derniers pour soutenir des mobilisation d'ONG militantes (notamment auprès d'exilés à Calais)[41], ou sur les collectifs citoyens appuyant les ONG, par exemple autour de groupes de cartographie participative[42]. Citons un article de Marina Duféal et de Matthieu Noucher, non pas sur l'humanitaire, mais sur OpenStreetMap, qui a collaboré à multiples reprises avec des ONG[43]. Il semblerait que jusqu'alors les sciences de l'information et de la communication (SIC) ont cependant peu couverts les autres aspects du numérique humanitaire.

Concernant les études de politiques de développement, notons le travail de Alain Kiyindou, directeur de publication de la revue *Communication, technologie et développement*, fondée en 2014, ou encore celui de chercheurs approchant les études de développement non pas depuis les sciences de l'information, mais depuis les Sciences and Technology Studies (STS). On pense aux travaux de chercheurs rattachés au Centre Population et développement comme Mathieu Quet ou Marine Al Dahdah. Ces derniers défendent la nécessité d'un décentrement des STS. Ce mouvement passe par une réflexion sur la façon dont la discipline des STS envisage la rupture Nord/Sud, sur le type de terrain à couvrir, sur la façon d'inclure des objets de recherches depuis des pays dits du Sud Global. Cela implique la prise en compte des conséquences méthodologiques d'un tel décentrement, en particulier en ce qui concerne le type d'outils conceptuels et théoriques pouvant être adoptés et les liens pouvant être établis entre les STS et les théories postcoloniales et décoloniales. Et enfin, décentrer les STS implique de considérer la façon de faire science, de repenser la production de savoir entre les pays occidentaux et émergents[44].

Quant aux SIC, comment ce mouvement de décentrement a-t-il été opéré ? Certains travaux se situent résolument depuis les pays du Sud global, comme c'est le cas des recherches d'Antonio Casilli sur les « microtravailleurs » du numérique, les « travailleurs du clic ». Récemment, des chercheurs ont pu aborder les enjeux liés au traitement du racisme dans la presse et dans les médias[45], et le sujet du lien entre discriminations raciales et algorithmes[46]. Il faut noter aussi un pan de recherche émergent sur l'usage de plateformes numériques (YouTube, Facebook) depuis les Sud, notamment avec un ancrage disciplinaire proche des

---

[41] GARDENIER, Matthijs, MONIE, Aymeric « De l'utilisation de Facebook à des fins de mobilisation par le groupe Sauvons Calais », *Communication*, vol. 35/1, 2018, http://journals.openedition.org/communication/7660

[42] FILALI Manon, « Lorsque les réseaux sociaux servent l'humanitaire », *Rhizome*, 2016/3 (N° 61), p. 19-19. https://www.cairn.info/revue-rhizome-2016-3-page-19.htm

LUANGSAY-CATELIN Carine, « La diplomatie humanitaire ou l'impact du numérique sur la mobilisation (cyber)citoyenne », *Hermès, La Revue*, 2018/2 (n° 81), p. 115-121. https://www.cairn.info/revue-hermes-la-revue-2018-2-page-115.htm

[43] DUFEAL**,** Marina, NOUCHER, Matthieu, « Des TIC au TOC. Contribuer à OpenStreetMap : entre commun numérique et utopie cartographique », *Netcom* 31-1/2 | 2017, http://journals.openedition.org/netcom/2635

[44] DAHDAH AL, M., QUET,M., « Between Tech and Trade, the Digital Turn in Development Policies », *Development*, 2020, 63, p.219–225, https://doi.org/10.1057/s41301-020-00272-y

DUMOULIN KERVRAN, David, KLEICHE-DRAY, Mina, QUET, Mathieu, « Les STS ont-elles un Sud ? Penser les sciences dans/avec les Suds », *Revue d'anthropologie des connaissances*, 2017/3 (Vol. 11, N°3), p. 423-454. https://www.cairn.info/revue-anthropologie-des-connaissances-2017-3-page-423.htm

[45] REBILLARD Franck, NOUS Camille , « La médiatisation analysée au prisme de la racialisation. Antériorités états-uniennes et tendances de la recherche française », *Réseaux*, 2020/5 (N° 223), p. 9-42. https://www.cairn.info/revue-reseaux-2020-5-page-9.htm

[46] TIGHANIMINE, Mariame**,** « Les algorithmes sont-ils racistes ? », *Socio*, 18 | 2023, http://journals.openedition.org/socio/14648

« cultural Studies »[47]. Ce serait une approche encore émergente, et surtout, les travaux empruntant aux théories décoloniales restent dans les SIC encore rares, également en ce qui concerne le numérique humanitaire.

À vrai dire, de manière générale, on dispose de bien plus de littérature sur les liens entre NTIC et migration, un champ de recherche également très dynamique dans le secteur académique anglophone [48] . Cette dernière provient en majorité de la sociologie ainsi que de l'anthropologie et des sciences politiques (voire plus spécifiquement les études africaines). Des universitaires comme Dana Diminescu ont étudié l'usage du numérique par des migrants lors de leurs parcours migratoires ainsi que la présence en ligne de diasporas. Ils ont permis de repenser la figure de l'exilé, le lien entre les pays d'accueil et le pays d'exil. L'usage de Facebook préserverait les réfugiés de l'isolement social[49]. Un autre pan de recherche se situe au croisement des « border studies » et des « surveillance studies », et également en lien avec les études critiques de sécurité. Ainsi, Didier Bigo[50], lequel a analysé la manière dont la criminalisation des migrants est portée par un assemblage d'acteurs et d'institutions (agences publiques, gouvernements, organisations internationales, acteurs) ; et se traduit par des pratiques et des discours hétérogènes, inscrits à l'échelle transnationale[51]. Ces dernières visent à assurer le contrôle des flux migratoire, notamment par des dispositifs numériques divers (des bases de données[52], mais aussi des drones, des caméras thermiques, de l'intelligence artificielle,[53] etc.). Autant d'outils au service de l'identification et du triage des personnes considérées comme « indésirables ». Des travaux ont pu adopter un angle plus directement juridique dans le traitement de différentes dimensions relatives aux données des exilés. C'est le cas d'un ouvrage récent dirigé par Sandrine Turgis décrivant les bases de données liées aux politiques de rejet des exilés, mais aussi les pratiques numériques des ONG venant au secours des réfugiés, la répercussion de leurs pratiques informationnelles en matière d'atteinte à la vie privée, ainsi que les conséquences de la numérisation de la présence en ligne des exilés, comme facteur de vulnérabilité et de risque de persécution. Il y est aussi surligné le fait que les traces en ligne peuvent être prises en compte dans l'examen

---

[47] BOUQUILLON, Philippe, ITHURBIDE, Christine, MATTELART, Tristan, "Digital Platforms and the Global South, Reconfiguring power relations in the cultural industries", Routledge, 2023, 256 p.

[48] SEUFERLING, Philipp, PFEIFER, Michelle, "Smart borders and their critiques are too focused on the tech: why we need a historical approach to envision a historical approach to envision different futures", LSE blog, 01/02/2024
https://blogs.lse.ac.uk/medialse/2024/02/01/smart-borders-and-their-critiques-are-too-focused-on-the-tech-why-we-need-a-historical-approach-to-envision-different-futures/
CHOULIARAKI, Lilie, GEORGIOU, Myria, *The Digital Border: Migration, Technology*, Power NYU Press,2022, 256p.
VAVOULA, Niovi*, Immigration and Privacy in the Law of the European Union – The Case of Information Systems,*Leyde : Brill Nijhoff, 2022,780 p.
TAZZIOLI, M., "Counter-mapping the techno-hype in migration research", *Mobilities*, *18*(6), 2023, p. 920–935. https://doi.org/10.1080/17450101.2023.2165447
LEURS, Koen, PONZANESI, Sandra (eds.), *Doing digital migration studies : theories and practices of the everyday*, Amsterdam University Press, 2024, 388 p.

[49] DEMORY,Matthieu,GAD, Nouran, « Expériences migratoires et communications numériques en Méditerranée », *Socio-anthropologie*, 40 | 2019 http://journals.openedition.org/socio-anthropologie/6031

[50] BIGO, Didier, « Sécurité et immigration : vers une gouvernementalité par l'inquiétude ? », *Cultures & conflits*, 1998, 31-32, p.13-38
BIGO, D, " Security and Immigration: Toward a Critique of the Governmentality of Unease", *Alternatives*, 2002, *27*(1_suppl), p. 63-92. https://doi.org/10.1177/03043754020270S105

[51]BIGO, Didier, « Le "*nexus*" sécurité, frontière, immigration : programme et diagramme », *Cultures & Conflits*, 84 , 2011, p.7-12
BIGO, Didier, "La Mondialisation de l'(in)Sécurité? Réflexions Sur Le Champ Des Professionnels de La Gestion Des Inquiétudes et Analytique de La Transnationalisation Des Processus d'(in)Sécurisation", *Cultures et Conflits*, no. 58, 2005, p. 53–100
ABOUT, Ilsen « De la libre circulation au contrôle permanent », *Cultures & Conflits* 76 | hiver 2009, http://journals.openedition.org/conflits/17757

[52] PREUSS-LAUSSINOTTE, Sylvia « L'élargissement problématique de l'accès aux bases de données européennes en matière de sécurité », *Cultures & Conflits*,74, 2009

[53] SIBLEY Anna, CHAPPART Pascaline, « Frénésie sécuritaire : l'algorithme du rejet », *Plein droit*, 2024/1 (n° 140), p. 3-6. https://www.cairn.info/revue-plein-droit-2024-1-page-3.htm

des demandes d'asile, mais aussi servir de preuve en matière d'enquête contre des violations des droits de l'homme[54]. Au-delà de cet ouvrage, on compte également des publications sur les politiques d'identification[55] et de mise en nombre des réfugiés par l'État[56] ou des ONG[57]. Léa Macias a par exemple concentré ses recherches sur la quantification de l'aide et les usages du numérique par les humanitaires dans la gestion des camps de réfugiés[58], qu'elle a analysée sous le prisme d'une dialectique entre « care » et contrôle[59] . Notre recherche s'appuiera évidemment sur l'ensemble de ces travaux, tout en s'en distinguant. Tout d'abord, nous nous intéressons au secteur humanitaire de façon plus générale, et non pas seulement aux exilés. Cela suppose d'aborder d'autres acteurs de l'aide, comme le CICR par exemple, dont le mandat originel n'est pas l'assistance aux migrants. Et surtout, notre recherche insistera de façon plus frontale sur l'action des délégués à la protection des données (DPO), des acteurs qui n'ont, à notre connaissance pas été encore abordés directement. On reviendra donc – sans adopter une approche strictement juridique – sur la façon dont les ONG mettent en œuvre le droit de la protection des données et prennent en compte les risques en matière de vie privée.

Pour ce faire, on s'est largement appuyée sur la littérature anglophone traitant de l'usage des NTIC par les humanitaires et revenant sur la numérisation du secteur, qui connait un premier tournant en 2010 et plus précisément lors du tremblement de terre survenu alors à Haïti. Cette date est mentionnée dans de nombreux rapports d'acteurs du milieu comme un moment phare de l'adoption du numérique lors d'une gestion de crise et elle correspond aussi au début de la médiatisation de la numérisation de l'aide[60]. Cela dit, la numérisation de l'humanitaire est évidemment d'un long processus, à la fois antérieur et postérieur à cette date. Au milieu des années 2010, la numérisation des opérations humanitaires était encore partielle et inégale, comme nous le raconte un enquêté : « *en 2015, ils en étaient encore au papier et au crayon et ça n'avait rien à voir avec la période actuelle, où l'on souhaite tout numériser*. »[61] A contrario, la numérisation du secteur s'amorce à la fin des années 1990. Cette période correspond en effet à la diffusion progressive de logiciels de cartographie informatique, au décloisonnement d'images satellitaires et à leur usage dans des opérations

---

[54] TURGIS,Sandrine (dir.), *Les données numériques des migrants et des réfugiés sous l'angle du droit européen*, Presses universitaires de Rennes, 2020, 236 p.

[55] SOUFFRON,Valérie**,** « La mal-mesure de l'âge », *Socio-anthropologie*, 40 | 2019, http://journals.openedition.org/socio-anthropologie/5808

[56] HAMZAOUI, Ouassim**,** « Mesurer et tracer les flux », *Socio-anthropologie*, 40 | 2019, http://journals.openedition.org/socio-anthropologie/5736

[57] AHOUGA, Younès, « L'Organisation internationale pour les migrations et la surveillance des populations de déplacés du Sud », *Revue européenne des migrations internationales*, 2022/3-4 (Vol. 38), p. 139-160.

[58]MACIAS, Léa « Usages expérimentaux des nouvelles technologies par l'action humanitaire : un data colonialisme ? », *Hommes & migrations*, 1337 | 2022, http://journals.openedition.org/hommesmigrations/13907

[59] AMELUNG, N, 'Crisis', "control and circulation: Biometric surveillance in the policing of the 'crimmigrant other'", *International Journal of Police Science & Management*, Vol. 25, 3, 2023, p.297-312

EWERT, " Displaced, Profiled, Protected? Humanitarian Surveillance and New Approaches to Refugee Protection". In: LEMBERG-PEDERSEN, Martin, FETT, Sharla, MAYBLIN, Lucy, SAHRAOUI, Nina, STAMBOL, Eva Magdalena, (eds), *Postcoloniality and Forced Migration*, Bristol University Press, 2022 https://doi.org/10.51952/9781529218213.ch00

[60] "Much as large established humanitarian NGOs have their foundational moments and myths such as the Battle of Solferino for the ICRC and the Biafran conflict for MSF, digital humanitarians anchor their narrative in a foundational moment. The earthquake in Haiti in 2010 is most commonly given as the step change or turning point for digital humanitarianism. " « Tout comme les grandes ONG humanitaires établies ont leurs moments fondateurs et leurs mythes, tels que la bataille de Solférino pour le CICR et le conflit du Biafra pour MSF, les humanitaires numériques ancrent leur récit dans un moment fondateur. Le tremblement de terre en Haïti en 2010 est le plus souvent cité comme le changement d'étape ou le tournant de l'humanitarisme numérique. » READ, R., TAITHE, B., MAC GINTY, R., "Data hubris? Humanitarian information systems and the mirage of technology", *Third World Quarterly*, 37(8), 2016, p.1314–1331

[61] Entretien n° 7, OI2, DPO, 11/12/2019

humanitaires[62]. En outre, la démocratisation de la téléphonie mobile, dans des pays du Sud global, a alors permis le lancement des premiers programmes de transfert monétaires ou encore de dispositifs de santé mobile[63]. Cependant, l'ampleur de la crise haïtienne de 2010, l'ampleur de la réponse humanitaire[64] ainsi que de sa médiatisation visibilisent la place du numérique dans le secteur de la solidarité. Tout juste un an avant l'engouement pour l'usage des réseaux sociaux lors des printemps arabes, les journalistes se sont enthousiasmés pour le travail de « crowdsourcing » de volontaires en ligne cartographiant à distance la catastrophe en collectant des données sur Twitter, Facebook et des numéros d'urgence. Leur tâche était donc de sélectionner des données permettant de localiser les besoins et les acteurs présents sur place. Les données étaient ensuite labélisées de façon coordonnée afin de permettre leurs classements, et de s'assurer de leur exactitude ainsi que de leur représentativité. Ces données étaient enfin publiées sur des logiciels de cartographie[65], entre autres sur la plateforme de « crowdsourcing » baptisée Ushahidi[66], une partie des cartographes étant sous la houlette d'un membre de l'équipe du logiciel, Patrick Meier, qui dès la fin des années 2000 et avant même les Printemps arabes a soutenu l'utilisation de réseaux sociaux dans des mouvements sociaux en contexte autoritaire, au Moyen-Orient[67]. Les opérations de crowdsourcing ont fait l'objet de nombreuses publications, pointant leurs limites. Paradoxalement, si la médiatisation de ces groupes coïncide avec l'avènement du numérique humanitaire, les réseaux de crowdsourcing sont des acteurs en partie étrangers au secteur de la solidarité. Ce sont des collectifs proches de la cartographie participative. En tout cas, les ONG, déjà submergées d'information, n'auraient pas eu systématiquement recours aux cartes produites par les collectifs volontaires, auxquels elles accordaient une confiance relative du fait de leur extériorité au monde humanitaire[68]. Ajoutons que des chercheurs se sont inquiétés de l'exclusion potentielle de personnes ne disposant pas d'accès aux réseaux sociaux ou de téléphones mobiles. Cette critique a amorcé à diverses réflexions sur la façon de dépasser cette fracture numérique (grâce à la formation des populations, à l'amélioration de la connectivité locale)[69]. Pour certaines ONG, le droit à la connectivité pour les bénéficiaires est

---

[62] « Cartographie humanitaire : nos représentations en question », *Revue humanitaire, enjeux, pratiques, débats*, n°32, 2012 https://journals.openedition.org/humanitaire/1289
Analp, *World Disasters Report 2005 - Focus on information in disasters*, https://www.alnap.org/help-library/world-disasters-report-2005-focus-on-information-in-disasters

[63] AL DAHDAH, Marine, « Les géants du numérique au chevet de l'Afrique. Le téléphone portable comme nouvel outil de santé globale », *Politique africaine*, 2019/4 (n° 156), p.101-1019, https://www.cairn.info/revue-politique-africaine-2019-4-page-101.htm
AL DAHDAH Marine, « Between Philanthropy and Big Business: The Rise of mHealth in the Global Health Market », *Development and change*, Volume 53, issue 2, 2022, p. 376-395

[64] A la date 13 août 2010, USAID avait engagé plus de 655 millions d'USD en approvisionnements, subventions et soutien

[65] ERTZSCHEID, Olivier, « Secousses syntaxiques et tremblements motorisés : Google, Twitter et Haïti », *Affordance*, janvier 2010, https://affordance.framasoft.org/2010/01/google-twitter-haiti-secousses-tremblements/
MEIER, Patrick, LEANING Jennifer, « Applying Technology to Crisis Mapping and Early Warning in Humanitarian Settings », *Harvard Humanitarian Initiative,* 2009, https://hhi.harvard.edu/publications/applied-technology-crisis-mapping-and-early-warning-humanitarian
MEIER, Patrick, "New information technologies and their impact on the humanitarian sector ", *International Review of the Red Cross*, Vol. 93, N° 884,2011, p. 1239-1263.
BOERSMA Kees, FONIO Chiara, *Big data surveillance and crisis management,* Routledge studies in surveillance, 2019,246 p

[66] Ushahidi est une plateforme de cartographie participative, crée en 2008, au Kenya, lors de violence postélectorales. Ushaidi permet de collecter des témoignages envoyés par courrier électronique ou SMS et les publier ensuite sur une carte en ligne.

[67] MEIER, Patrick," Do "liberation technologies" change the balance of power between repressive states and civil society?" PHD Thesis, Degree of doctor of Philosophy,The Fletcher School of Law and Diplomacy

[68] OCHA UN Foundation, Vodafone Foundation, « Disaster Relief 2.0: The Future of Information Sharing in Humanitarian Emergencies », 2011, https://hhi.harvard.edu/publications/disaster-relief-20-future-information-sharing-humanitarian

[69] CRAWFORD Kate, FINN Megan, « The Limits of Crisis Data: Analytical and Ethical Challenges of Using Social and Mobile Data to Understand Disasters », *GeoJournal*,80, 2015, p.491–502

devenu un sujet en soi, l'enjeu étant alors d'assurer l'accès à une connexion, sans créer de nouvelles dépendances des bénéficiaires aux organisations humanitaires.

Par la suite, certaines organisations de volontaires se sont structurées et se sont impliquées dans des projets de cartographie, parfois en collaboration avec des ONG, comme c'est le cas pour le groupe « Digital Humanitarian network », ou encore l'organisation Stand By force. Mais de manière générale, on a assisté à une professionnalisation du travail cartographique au sein même des ONG (via l'utilisation de logiciels cartographiques, de drones ou d'images satellitaires). Parallèlement, différentes initiatives de cartographies participatives humanitaires ont vu le jour, comme le projet « missing map » initié en 2014 par la Croix Rouge américaine, MSF et Open Street map ou encore des projets de cartographies menés par le HCR[70]. Ces projets reposent sur l'inclusion de populations locales. Ils sont donc proches des démarches de cartographies radicales et ambitionnent de cartographier des lieux en intégrant d'autres formes de représentations de l'espace. Ils s'inspirent parfois de la géographie critique et se situant dans le lignage de Mike Harvey ont pu travailler sur le numérique humanitaire. C'est le cas de Doug Spech, rattaché au « Communication and Media Research Institute » de Westminster. Il s'est intéressé aux problématiques de cartographies participatives, aux enjeux épistémologiques liés à la production et la codification de connaissance. Toujours dans cette perspective, il ne faut pas oublier le géographe canadien Ryan Burns. D'abord spécialisé dans l'étude de systèmes d'information géographique (SIG), comme l'Open street map, il s'est ensuite penché sur les collectifs de cartographies humanitaires bénévoles. Son objectif est de mettre en lumière « les spatialités, les modalités et les inégalités sociopolitiques qui émergent de l'humanitarisme numérique, ainsi que l'imbrication mutuelle de l'humanitarisme numérique et de réformes politico-économiques plus larges. »[71]

La carte ne serait plus un instrument de pouvoir au service d'actions soit coloniales ou militaires, mais permettrait de servir d'autres finalités, comme la réappropriation d'un territoire invisibilisé. Toutefois, selon leur modalité de mise en œuvre, ces projets reposent sur différents présupposés pouvant être déconstruits : la valorisation apriori et parfois non-critique de savoirs locaux, la réification de structures sociales de type communautaire. La dimension participative de ces initiatives a également ses propres limites en fonction du statut des participants et de leurs modes d'implication[72], de la possibilité pour eux d'avoir accès en fin de projet aux cartes qu'ils ont réalisées et d'être rémunéré pour le travail fourni[73].

Cette valorisation des approches participatives peut être expliquée par la nécessité pour les humanitaires d'être redevable auprès de leurs bénéficiaires. Le terme de redevabilité englobe toute une série d'actions réalisées afin de minimiser les dynamiques de pouvoir circulant entre

---

[70] https://www.esri.com/about/newsroom/arcnews/gis-for-refugees-by-refugees/

[71] « spatialities, modalities, and socio-political inequalities that emerge from digital humanitarianism, as well as the mutual-imbrication of digital humantarianism and broader political-economic reforms » https://geog.ucalgary.ca/manageprofile/profiles/ryan-burns?thickbox=1_target%252525252525253D

YUMMO WANG, Ben,RAYMOND, Nathaniel,GOULD, Gabrielle, BAKER, Isaac, « Problems from Hell, Solution in the Heavens?: Identifying Obstacles and Opportunities for Employing Geospatial Technologies to Document and Mitigate Mass Atrocities », *Stability: International Journal of Security & Development*, 2(3): 53, 2013, p. 1-18, DOI: http://dx.doi.org/10.5334/sta.cn

[72] DOUG, Specht,(ed.), Mapping Crisis: Participation, Datafication and Humanitarianism in the Age of Digital Mapping, London: University of London Press, 2020, 278 p.

[73] MACIAS, Léa « La mise en nombre des réfugiés syriens », Socio-anthropologie, 40 | 2019, mis en ligne le 08 janvier 2020, http://journals.openedition.org/socio-anthropologie/5664

agences humanitaires et personnes secourues. La redevabilité passe surtout par des mécanismes de consultation et de recueil de retours sur la nature et la qualité de l'aide. Le numérique semble être un outil adapté à ce type de finalité. Les ONG peuvent avoir recours à des lignes téléphoniques, des groupes WhatsApp ou encore des agents conversationnels en ligne. Comme l'a montré Mirca Madianou, ces mécanismes de communication ont plusieurs limites : l'existence de fracture numérique (selon les infrastructures locales, le contexte culturel, le degré de littératie des bénéficiaires), et les rapports de pouvoir et de dépendance entrant en jeu. Il n'est pas toujours simple de faire des retours critiques à des ONG dont on dépend pour sa survie[74]. À vrai dire, les approches participatives se limiteraient bien souvent à une approche restreinte de participation, et consisteraient simplement à recueillir des retours des bénéficiaires sans impulser de véritable dialogue. Les bénéficiaires resteraient en outre exclus du design des outils numériques leur étant imposé. En réaction, des laboratoires technologiques humanitaires ont alors été fondés à l'échelle locale. Leur démarche s'inscrit dans l'agenda de localisation de l'aide[75]. Ainsi, le « Localization lab »[76] datant de 2012, promeut l'usage de technologies « open sources », prenant en compte la diversité culturelle et linguistique.

Le numérique représente donc un espoir d'émancipation. Il semble une solution idéale pour impliquer les bénéficiaires, réduire les inégalités entre ONG et victimes de crise[77]. Mais cet idéal peut croiser un imaginaire néolibéral, se cristallisant dans la figure du bénéficiaire entrepreneur[78]. Ce dernier récit se retrouve aussi dans la multiplication de projet de transferts monétaires[79] ou de dispositifs d'identités souveraines. L'allocation de ressources financières permettrait de laisser libre le bénéficiaire de ses choix de consommation, ce qui entrainerait quasiment de fait leur « encapacitation »[80].

De surcroit, la notion de redevabilité a également une deuxième facette. En effet, les ONG doivent aussi être redevables auprès de leurs bailleurs de fonds. Et là encore, recourir au numérique parait être une bonne idée. La redevabilité peut ainsi passer par l'adoption de dispositifs numériques visant à améliorer la traçabilité des fonds et éviter la fraude, notamment grâce à de la biométrie et/ou des blockchains. L'adoption de ce type de dispositif

---

[74] MADIANOU, Mirca, LONGBOAN, Liezel, CORPUS ONG, Jonathan, " Finding a voice through humanitarian technologies?Communication technologies and participation in disaster recovery ", International journal of communication, Vol 9, 2015

[75] On trouverait des premières traces de cet impératif au milieu des années 2000, l'expression s'est depuis ancrée dans les discours et normes humanitaires. Il s'agit de rééquilibrer les relations entre parties prenantes, en donnant plus de place aux organisations locales dans la délivrance des programmes.
COORDINATION SUD, "La localisation de l'aide, plus de proximité permet-il d'assurer l'autonomie des projets déployés ?", 2019 https://www.coordinationsud.org/wp-content/uploads/synthese-etude-localisation-aide.pdf

[76] https://www.localizationlab.org/ Le site affirme travailler au développement de logiciels dans quelques 220 langages.

[77] AL DAHDAH, Marine « Les mobiles du développement : le téléphone portable comme outil d'empowerment des femmes des Suds ? », *Terminal* , 125-126 | 2019, http://journals.openedition.org/terminal/5013

[78] BACQUE, Marie-Hélène, BIEWENER Carole, « l'empowerment, un nouveau vocabulaire pour parler de
Participation ? », *Réseau Canopé*, 2013/3 N° 173, p. 25-32

[79] AWANIS, Aramé,LOWE Christopher, ANDERSSON-MANJANG Simon K., LINDSE Doninica, "State of the Industry Report on Mobile Money", GSMA,2022 https://www.gsma.com/sotir/wp-content/uploads/2022/03/GSMA_State_of_the_Industry_2022_English.pdf
HUTTON, Josephine, BOESER, Shawn, GROOTENHUIS, Floor, "A Review of Cash Transfer Programming and the CALP Network 2005–2015 and Beyond", *Calpnetwork*, 2015 https://www.calpnetwork.org/publication/a-review-of-cash-transfer-programming-and-the-cash-learning-partnership-calp-2005-2015-and-beyond/
KREIDLER Corinna, TAYLOR Glyn, "Where next? The evolving landscape of cash and voucher policies", *Calpnetwork*, December 2022. https://www.calpnetwork.org/publication/where-next-the-evolving-landscape-of-cash-and-voucher-policies/

[80] CHEESMAN, Margie, "Infrastructure justice and humanitarianism : blockchain's promises in practice", Phd Thesis, Phil in Digital Social Science at the Oxford Internet Institute, University of Oxford, January 2022

serait parfois même en partie imposée par les bailleurs. Le récent rapport de l'organisation sur les droits humains en ligne, the Engine Room, est clair sur ce point : « les attentes en matière d'information financière ont poussé les organisations à vérifier l'exactitude de leur comptabilité. Cette pression découle en partie du désir des donateurs de maximiser leurs contributions — une demande qui se traduit de plus en plus par l'exigence d'une mise en œuvre plus efficace des programmes. Ces dernières années, le niveau de connaissance des dépenses souhaité par les donateurs, ainsi que leur insistance sur l'efficacité, a rendu les solutions technologiques (et leurs promesses de vérifiabilité et de transparence) plus attrayantes. »[81]

Cette exigence de redevabilité prend racine dans la crise de légitimité ayant touché l'humanitaire dans les années 90. Elle serait en partie déclenchée par l'échec de l'intervention de la communauté internationale au Rwanda[82]. L'historien Joël Glasman a montré comment, en réaction, se sont progressivement structurés des mécanismes de redevabilité[83]. Ces derniers permettraient alors d'assurer la qualité de l'aide et ont accompagné sa professionnalisation. Ils recourent à des indicateurs standardisés, comme ceux développés par le projet Sphere en 1997, ainsi qu'à différentes méthodologies d'évaluation, de monitoring, et d'audit par des bailleurs[84]. Il s'en est logiquement suivi une quantification progressive du secteur[85] et un investissement quasi moral des statistiques, qui seraient alors associées aux principes humanitaires[86], principalement celui d'impartialité.

Il peut s'agir de données socio-économiques, démographiques, de santé, alimentaire ; des données environnementales et géographiques, permettant de localiser les bénéficiaires, mais aussi des données financières de programmes de « cash », des données biométriques, iris et empreintes digitales ; des données concernant le management des programmes, comme des indicateurs de management, de performance, de budgets, etc. Ces données sont récoltées pour nourrir divers supports, des évaluations de besoin, des analyses de vulnérabilité des bénéficiaires, des analyses de risque, des audits financiers. Ce recueil s'effectuait à la main puis grâce à des outils numériques plus diversifiés, comme le logiciel « kobotoolbox » développé par l'Humanitarian Initiative.

---

[81] « Extensive financial reporting expectations have resulted in pressure for organizations to verify the accuracy of their accounting. This impetus stems in part from donor desire to maximise their contributions– an ask that is increasingly translated into demands for more efficient program delivery. In recent years the level of insight into spending that donors desire, along with their insistence on efficiency, has made technological solutions (and their promises of verifiability and transparency) more appealing" PEROSA, Teresa, TSUI, Quito, SINGLER, Samuel, "Biometrics in the humanitarian sector, a current look at risks, benefits and organizational policies", The Engine Room, July 2023 https://www.theengineroom.org/wp-content/uploads/2023/07/TER-Biometrics-Humanitarian-Sector.pdf

[82] BORTON, John, "Twenty years on: the Rwandan genocide and the evaluation of the humanitarian response", *Overseas Development Institute*, 2014, https://odihpn.org/publication/twenty-years-on-the-rwandan-genocide-and-the-evaluation-of-the-humanitarian-response/

[83] GLASMAN, Joel, *Humanitarianism and the Quantification of human needs, minimal humanity,* Routledge, 2019,274 p.

[84] LAURENT, Catherine, BAUDRY, Jacques, BERRIET-SOLLIEC Marielle, *(et al.)*, « Pourquoi s'intéresser à la notion d' « evidence-based policy » ? », *Revue Tiers Monde*, 2009/4 (n° 200), p. 853-873. https://www.cairn.info/revue-tiers-monde-2009-4-page-853.htm

PÉROUSE DE MONTCLOS, Marc-Antoine. « le bilan impossible. Limites de l'évaluation et du contrôle», In : *Pour un développement « humanitaire » ? Les ONG à l'épreuve de la critique*, Marseille : IRD Éditions, 2015, http://books.openedition.org/irdeditions/8729

[85] MACIAS Léa, « La mise en nombre des réfugiés syriens », *Socio-anthropologie*, 40 | 2019, http://journals.openedition.org/socio-anthropologie/5664

[86] »Entretien avec Joel Glasman : statistiques humanitaires », *Alternatives humanitaires*, n°14, 2020https://www.alternatives-humanitaires.org/fr/2020/07/23/statistiques-humanitaires/

GLASMAN, Joel, « L'invention de l'impartialité : histoire d'un principe humanitaire, entre raisons juridique, stratégique et algorithmique » *Alternatives humanitaires,* n°15, novembre 2020, p.8-21https://www.alternatives-humanitaires.org/wp-content/uploads/2020/11/AH_N15_2_Perspectives_Glasman_VFR-1.pdf

De surcroit, adopter des technologies innovantes permettrait d'assurer la redevabilité et l'efficience de l'aide. Elles permettraient d'allouer précisément les fonds selon les besoins, et de prendre des décisions ciblées et efficaces[87], d'où le succès des approches « pilotées par la donnée » (« Data driven decision »). Ces dernières reposent en effet sur le fait de disposer d'information en temps réel afin de pouvoir adapter son action à un contexte volatile[88].

L'idéal serait de pouvoir anticiper le cours des événements, en recourant à des systèmes d'alerte rapide, voire plus récemment à de l'intelligence artificielle, afin de prévenir des catastrophes ou des déplacements de population[89]. Sachant que Claudia Aradau et Mark Duffield rappellent comment ce mouvement va de pair avec la redéfinition de la nature d'une catastrophe, à une nouvelle épistémologie des crises, et à l'évolution des techniques de gestion de risque[90]. Enfin, certains praticiens continuent de critiquer la mauvaise qualité des données humanitaires, collectées dans l'urgence[91], sans concertation. Ils regrettent le fait que les données gérées par des ONG soient potentiellement redondantes, stockées en silo, ne produisant en fin de compte qu'une connaissance partielle des crises[92]. En réaction, une meilleure coordination de la gestion d'information est souhaitée [93] afin d'améliorer l'interopérabilité entre bases de données d'ONG[94].

Mais surtout, si le numérique donnerait l'impression d'être au cœur des crises et d'acquérir une compréhension plus fine de ces dernières, il permet aussi de les observer à distance. Comme l'a observé de façon critique Mark Dufield, le recours à des dispositifs cartographiques et à des images satellitaires ou à des drones permet de maintenir la continuité de l'aide en palliant la complexification de l'accès au terrain, surtout dans des contextes sécuritaires dégradés[95]. Mais ceci se ferait au prix d'une coupure d'avec les populations et du report du risque sur les structures d'aide locales. Toutefois, le numérique n'est pas un espace « bunkerisé » permettant le pilotage à distance d'opération de façon sécurisé. Et selon Kristin Sandvik, s'il permet d'étendre la possibilité d'action des ONG, l'on assisterait dans le même

---

[87] VERITY, Andrej,"OCHA's 3W Purpose, Target Audience, Scope and Products", 2013 https://www.humanitarianresponse.info/sites/www.humanitarianresponse.info/files/documents/files/ocha_3ws.pdf

[88] BOERSMA Kees, FONIO Chiara, *Big data surveillance and crisis management,* Routledge studies in surveillance, 2019, p.246

[89] BEDUSCHI, A., MCAULIFFE M. Mc, 2021. « Artificial Intelligence, migration and mobility: implications for policy and practice » In MCAULIFFE, M., TRIANDAFYLLIDOU, A., eds., *World Migration Report 2022*, International, Organization for Migration (IOM), Geneva, 2022

[90] DUFFIELD Mark, *Post humanitarianism governing precarity in the digital world*, Cambridge : Polity Press, 2019.

ARADAU Claudia, VAN MUNSTER Rens, *Politics of catastrophe genealogies of the Unknown*, Routledge, 2011 : « A new ontology of disaster emerged. Rather than a modernist separation from society, disaster became a defining characteristic of society and its inner vulnerabilities and weaknesses The earlier social and political views of famine gave way to complexity thinking and indeterminacy. Experimentation with early warning transformed famines into the signals and alerts thrown off by behavioural change. Rather than theory, the new emphasis. These developments exemplified the coming of age of an essentially cybernetic understanding of liberal security. In anticipating the post social, was operationality. the fantastic NGO invasion also piloted the projectized forms of livelihood support and community development. While anticipatory, however, the project form, together with the direct humanitarian action of the period, were still vested in the primacy of human agency and grounded engagement »

TOBIAS, Blanke, ARADAU, Claudia, *Algorithmic Reason, The New Government of Self and Other*, Oxford University Press, 2022, 282 p.

[91] FAST, Larissa, « Diverging Data: Exploring the Epistemologies of Data Collection and Use among Those Working on and in Conflict », in *International Peacekeeping*, *24*(5), 2017, 706–732 https://doi.org/10.1080/13533312.2017.1383562

[92] MOE FEJERSKOV, Adam, CLAUSEN, Marie-Louise, SEDDIG, Sarah, " Humanitarian ignorance : towards a new paradigm of non-knowledge in digital humanitarianism", Disaster, 2024, VOl.48, Issue 2 https://doi.org/10.1111/disa.12609

[93] SCHOEMAKER, Emrys, CURRION, Paul, PON, Bryan, « identity at the margins : identification system for refugees », *Caribou digital*, 2018, https://assets.publishing.service.gov.uk/media/5cecedd6ed915d2475aca8c5/Identity-At-The-Margins-Identification-Systems-for-Refugees.pdf

[94] IFRC, "Investigating safe data sharing and systems interoperability in humanitarian cash assistance", 2023, https://cash-hub.org/wp-content/uploads/sites/3/2023/11/DIGID-Interoperability-Investigating-Safe-Data-Sharing-and-Systems-Interoperability.pdf

[95] DONINI, Antonio, MAXWELL, Daniel,"From face-to-face to face-to-screen: remote management, effectiveness and accountability of humanitarian action in insecure environments", *International Review of the Red Cross*, 2013, 95 (890), p.383-413

DUFFIELD, Mark, "Disaster-Resilience in the Network age, access denial and the rise of cyber-humanitarianism", DISS Working Paper, 2013

temps à la réduction de ce même espace numérique humanitaire, du fait de la volonté d'États de le contrôler, de garder un droit de regard sur les données que les ONG collectent sur leur population[96], ainsi que du fait de la multiplication de cyberattaques touchant les ONG.

Une part de la recherche universitaire met donc l'accent sur les risques liés à la numérisation du secteur, entre autres en s'appuyant sur les « surveillance studies ». La notion de surveillance et l'image foucaldienne du panoptique sont alors utilisées pour décrire la balance entre « care » et « contrôle » propre au numérique humanitaire[97]. La tribune du chercheur Mark Latonero « Stop surveillance humanitarism » publiée dans le New York Time est représentative de ce type d'approche[98]. L'auteur s'alarme des risques provoqués par un usage non éthique du numérique par les ONG, ainsi que de l'impact de la collecte massive de données sur les bénéficiaires.

Cette approche par les risques est aussi celle du Peace research Institut (PRIO)[99], qui soutient un autre projet dénommé « Do no Harm : innovation humanitaire éthique et corps numériques », porté entre autres par Kristin Sandvik. L'institut se veut pluridisciplinaire. Mais l'essentiel des recherches produites se rattache aux études de sécurité. Et les chercheurs de l'institut centrent leurs travaux sur les formes de conflictualités contemporaines, sur les politiques de consolidation de la paix et sur le terrorisme, ainsi que le numérique humanitaire. Les principaux axes de recherches concernent la place des données et des corps numériques dans les opérations humanitaires ; les dispositifs de traçage dans l'humanitaire ; les liens entre humanitaire-numérisation-sécurité ; l'éthique des innovations humanitaires. La protection des données y est abordée selon une approche de type « do no harm » (traduisible par l'expression française « ne pas nuire »). Principe éthique clef de l'aide, il désigne l'obligation de minimiser les éventuels dommages causés par les acteurs humanitaires (et leurs usages numériques) et touchant les bénéficiaires. Mais si Kristin Sandvik se penche sur le système éthique mobilisé par les ONG et adopte un prisme d'analyse de type sociojuridique, ses recherches font le constat d'un manque d'encadrement de l'innovation humanitaire, et n'abordent donc pas le travail d'acteurs qui occuperont une place majeure dans cette thèse : les délégués à la protection des données.

---

[96] SANDVIK, Kristin, "The humanitarian cyberspace: shrinking space or an expanding frontier?", *Third World Quarterly*, 37(1), 2016, p. 17–32.

[97] MADIANOU, M., "The Biometric Assemblage: Surveillance, Experimentation, Profit, and the Measuring of Refugee Bodies", *Television & New Media*, *20*(6), 2019, p. 581-599. https://doi.org/10.1177/1527476419857682

FAST, L., JACOBSEN, K. L., "Rethinking Access: How Humanitarian Technology Blurs Control and Care", *Disasters*, 2019, 43(S2), p.151-168

MARTIN, A., TAYLOR, L."Exclusion and inclusion in identification: regulation, displacement and data justice", *Information Technology for Development*, 2020,*27*(1), 50–66. https://doi.org/10.1080/02681102.2020.1811943

PARAGI, B., ALTAMIMI, A., "Caring control or controlling care? Double bind facilitated by biometrics between UNHCR and Syrian refugees in Jordan", *Society and Economy*, 2022, *44*(2), p. 206-231. https://doi.org/10.1556/204.2021.00027

[98] LATONERO, Mark, "Stop surveillance humanitarianism", *The New York Times*, 11/07/2019, 11/07/2019https://www.nytimes.com/2019/07/11/opinion/data-humanitarian-aid.html

[99] L'institut de recherche sur la Paix d'Oslo ( le Peace research Institute of Oslo, PRIO), a été fondé par Johan Galtung, chercheur ayant contribué à formaliser les « peace studies » (l'irénologie). L'institut se veut pluridisciplinaire. Mais l'essentiel des recherches produites se rattache aux études de sécurité. Et les chercheurs de l'institut centrent leurs travaux sur les formes de conflictualités contemporaines, sur les politiques de consolidation de la paix et sur le terrorisme. L'institut a soutenu un premier projet-pilote très court, baptisé « Critical humanitarian technology » (mené de mai 2013 à décembre 2013). Il était centré au départ sur les drones, et il a donné lieu à de nombreuses publications sur le sujet, notamment un article programmatique intitulé « Humanitarian technology : a critical research agenda » et publié par Kristin Bergtora Sandvik, Maria Gabrielsen Jumbert, John Karlsrud et Mareile Kaufmann.

## Arrimage théorique de la question initiale : « data colonialisme » et souverainetés étatiques

Cette revue de la littérature sur le numérique humanitaire doit être maintenant remise en perspective en approfondissant les différentes dynamiques expliquant les risques liés aux NTIC. Sachant qu'on se concentrera dans cette thèse sur les risques relatifs aux atteintes à la vie privée et leurs liens avec trois notions : celles de colonialité, de souveraineté et de dignité.

Une première remarque pour commencer : le concept de vie privée est considéré comme ayant des racines occidentales et libérales. Nos sociétés se sont progressivement construites sur la dissociation d'une sphère privée et d'une sphère publique, comme l'ont montré Philippe Ariès ou encore Jurgen Habermas[100]. Ce processus s'est cristallisé sur le long terme. Mais d'un point de vue juridique, le droit à la vie privée est en fin de compte relativement récent. Il est fait généralement mention de l'article de deux juristes américains Samuel Warren et Louis Brandeis, publié en 1890 dans la Harvard Law review. Dans cette publication, ils défendent la nécessité du « droit d'être laissé tranquille », notamment face aux intrusions de la presse. Son inscription effective dans le droit est cependant plus tardive. La notion de vie privée ferait une première apparition à la fin de la Seconde Guerre mondiale sous la forme de l'article 12 de la déclaration universelle des droits de l'homme de 1948[101]. Puis c'est au cours des années 1960 que se construit le droit à la vie privée. Un processus décrit par le chercheur Julien Rossi. Différents éléments ont participé à la mise à l'agenda du « problème » de la vie privée. Aux États-Unis, les premiers développements de l'informatique sont perçus — entre autres en raison de son origine militaire — comme autant de menaces à l'encontre des citoyens. De surcroit, cette période correspond au développement de base de données informatisées à des fins de marketing[102]. Le contexte de guerre froide a pu jouer aussi. Le Maccarthisme s'est associé de politique de surveillance, mais dans le même temps les défenseurs du droit à la vie privée ont pu être mis en avant ses racines libérales, et l'ont opposé au régime soviétique, considéré comme valorisant le collectif au détriment des droits des individus[103]. Toujours est-il que son inscription dans le droit est entérinée avec le vote du Privacy Act en 1974 aux États-Unis, qui réglemente les données gérées par l'Etat, mais ne couvre pas le secteur privé. Parallèlement, une série de lois relatives à la protection de la vie privée sont votées en Europe : en 1973 en Suède avec la loi « Data Act », en 1978 en France avec la loi « informatique et vie privée ».

Dans le champ académique, la notion de vie privée a été largement explorée à partir de la fin des années 1990, tout d'abord par les « surveillance studies »[104]. Les auteurs rattachés à ce

---

[100] HABERMAS, Jurgen, *L'espace public*, Paris : Payot, 1988, 330 p.
ARIES, Philippe, DUBY, Georges (eds), *Histoire de la vie privée, 5 tomes*, Paris : éditions du Seuil, 1985/87

[101] Art.12 Déclaration universelle des droits de l'homme « Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes. » https://www.un.org/fr/universal-declaration-human-rights/

[102] ATTEN, Michel, « Ce que les bases de données font à la vie privée. L'émergence d'un problème public dans l'Amérique des années 1960 », *Réseaux*, 2013/2-3 (n° 178-179), p. 21-53. https://www.cairn.info/revue-reseaux-2013-2-page-21.htm
MASUTTI, Christophe*, Affaires privées : aux sources du capitalisme de surveillance*, Caen : C&F Editions, 2020, 475 p.

[103] CHRISTIAN Michel, « Le parti et la vie privée de ses membres en RDA », *Histoire@Politique*, 2009/1 (n° 7), p. 3 https://www.cairn.info/revue-histoire-politique-2009-1-page-3.htm

[104] CASTAGNINO, Florent, « Critique des *surveillances studie*s. Éléments pour une sociologie de la surveillance », *Déviance et Société*, 2018/1 (Vol. 42), p. 9-40. https://www.cairn.info/revue-deviance-et-societe-2018-1-page-9.htm
AÏM Olivier, *Les théories de la surveillance. Du panoptique aux Surveillance Studies ,* Paris : Armand Colin, « Collection U », 2020,256 p.

champ se sont penchés sur les formes de surveillances associées aux nouvelles technologies par des acteurs privés et publics (bien que les frontières entre ces deux formes de surveillances soient poreuses). Cela dit, certains chercheurs de ce champ d'études sont plus critiques qu'on pourrait l'imaginer à l'égard du concept de vie privée[105]. Ce concept ne serait pas pertinent pour John Gilliom pour décrire l'expérience de personnes, surtout en ce qui concerne les personnes vulnérables, ciblées par des formes de surveillances. Ce dernier écrit que : « lorsque nous avons interrogé des bénéficiaires de l'aide sociale sur leurs interactions avec un nouveau système informatisé de surveillance des finances, des prestations et de l'éligibilité, ils n'ont que peu parlé de vie privée — ils ont plutôt parlé de peur, de dégradation, de besoin et de lutte. »[106] En outre, il ne rendrait pas bien compte des formes de contrôle social et des différentes inégalités qui les accompagnent. On lui reproche alors son origine libérale et son caractère individualiste[107]. D'où la tentation de forger une définition communautaire de la vie privée. Toutefois, l'opposition entre dimension collective et individuelle ne tient pas toujours. Sa défense est nécessaire à l'exercice d'une participation politique démocratique : un bon nombre de chercheur ont pu rappeler que la vie privée garantit la liberté d'exercice de débat nécessaire à la pluralité d'opinion[108].

Autre critique, le concept de vie privée serait anachronique. Du moins, c'est ce que déclare Mark Zuckerberg, qui a pu décréter que la vie privée serait une norme éculée dans nos sociétés contemporaines, l'entrepreneur mettant plutôt en avant des vertus comme la transparence et le partage d'information sur les réseaux sociaux. Plus finement, des chercheurs ont plutôt montré qu'il est possible d'être préoccupé par la protection de leur vie privée, tout en l'exposant sur les réseaux. Depuis, ce « privacy paradox » a fait l'objet de nombreux

[105] "first, let me note that it is not 'privacy' that should be done away with, but the regime of privacy.By this, I mean, the intellectual regime which insists that privacy be the central theme or even the very terrain for every discussion of surveillance.Privacy is an important part of what we study, but we must and we are moving quickly away from an era in which it was the defining element of the field.The fact that we now have a leading scholar in the leading journal arguing for its salvation underscores the progress that has been made.But the mission of post-privacy scholars is not and really cannot reasonably be to remove privacy from the field of study—the mission has been (at least for me) to remove it from its position of intellectual and political monopoly.In the end, it is my belief that research-oriented participants in the field will do best to keep privacy in its proper place—as one part of the cultural politics of surveillance, but not as the organizing matrix for the field « Tout d'abord, permettez-moi de souligner que ce n'est pas la « vie privée » qu'il faut supprimer, mais le régime de la vie privée, c'est-à-dire le régime intellectuel qui insiste pour que la vie privée soit le thème central, voire le terrain même de toute discussion sur la surveillance.La vie privée est une partie importante de ce que nous étudions, mais nous devons nous éloigner rapidement d'une époque où elle était l'élément déterminant du domaine.Le fait que nous ayons maintenant un chercheur de premier plan dans la revue de premier plan qui plaide pour son salut souligne les progrès accomplis. Mais la mission des chercheurs de l'après-privacité n'est pas et ne peut raisonnablement pas être de supprimer la vie privée du champ d'étude — la mission a été (du moins pour moi) de la retirer de sa position de monopole intellectuel et politique. En fin de compte, je crois que les participants à la recherche dans le domaine feront mieux de garder la vie privée à sa place — comme une partie de la politique culturelle de la surveillance, mais pas comme la matrice d'organisation du champ d'étude. » GILLIOM, John, "A response to Bennett's "in defence of privacy", *Surveillance&Society*, 8(4), 2011, p.500-504

[106] "when we interviewed welfare clients about their interactions with a new computerized finance, benefits, and eligibility surveillance system, they only said a little about privacy—they spoke more of fear, degradation, need, and struggle." GILLIOM, John, ibid.

[107] "Privacy's individualization partially explains why surveillance studies has had an uneasy relationshipto privacy, despite the seeming centrality of the concept. Rightfully, surveillance scholars often consider privacy to be "a largely individualistic concept that is poorly suited to account for discrimination against groups"and is "empirically inaccuratein representing the concerns of marginalized populations"(Monahan and Murakami Wood 2018:" MARWICK, Alice, "Privacy Without Power: What Privacy Research Can Learn from Surveillance Studies" *Surveillance & Society*,20(4), 2022, p. 397-405.https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/16009/10519

[108] ROUVROY, Antoinette, POULET, Yves, "The Right to informational self-determination and the value of self-development : reassessing the importance of privacy for democracy", in, GUTWIRTH, Serge, POULLET, Yves, HERT, Paul, TERWANGNE, Cécile, NOUWT, Sjaak (ed), *Reinventing data protection?,* New-York : Springer, 2009, p.45-76

REGAN, Priscilla, "Privacy as a common good in the digital world", Annual Meeting of the American political science association, September 1999

développements, notamment par Alessandro Acquisti ou encore Antonio Casilli [109]. L'exposition de soi serait fondée soit sur le calcul coût/avantage des utilisateurs. Les chercheurs insistent sur la nature incitative des réseaux, poussant les utilisateurs (inquiets malgré tout) à s'exposer toujours plus, en raison de leur conception, de leur « affordance ». En réaction est prônée la création de projets de technologies reposant sur une « privacy by design. » En attendant, pour certains chercheurs, l'hypothèse de la fin de la vie privée ne serait pas vérifiée. On assisterait plutôt à une évolution de cette dernière. Elle serait contextuelle et négociée. Avant de publier un contenu, un internaute opérerait par phase de test et de « feed-back » pour « prendre la température » et évaluer les risques associés au partage d'un contenu en fonction de sa nature et de son contexte [110]. Cela dit, cette possibilité de négociation dépend du degré de littératie de l'internaute, ainsi que du rapport de force entre usagers, plateformes et algorithmes. Il s'agit de se mettre en scène, de maitriser l'image qu'on donne de soi. Mais à vrai dire, pour Antoinette Rouvroy, le modèle de la surveillance fondée sur l'intrusion et l'atteinte à la vie privée de la personne n'est plus pertinent pour envisager les formes contemporaines d'exploitations des données en ligne. Ce qu'elle nomme « gouvernementalité algorithmique » ne s'exerce pas sur notre personne. Cette dernière reposerait sur l'exploitation de traces que laissent les internautes, permettant l'élaboration de profils types. Ce qui inquiète la chercheuse n'est donc pas tant la façon dont les algorithmes portent atteinte à la vie privée des individus, mais la façon dont ils conduisent à une forme de dépossession de soi, voire à une réification des personnes, qui seraient réduites à des profils constitués d'une série d'éléments discrets[111].

D'ailleurs, Shoshana Zuboff la rejoint en partie sur ce point. Le concept de vie privée est pour elle aussi essentiel sans suffire pour autant. On peut le lire dans son ouvrage phare sur le capitalisme de surveillance qu' : « on recourt à des catégories telles que le monopole ou la "vie privée" pour contester les pratiques du capitalisme de surveillance. Or, bien que ces questions soient vitales, alors même que les opérations capitalistes de surveillance sont et constituent une menace pour la vie privée, les catégories actuelles sont néanmoins insuffisantes pour identifier et contester les faits sans précédent les plus cruciaux de ce nouveau régime »[112]. Shoshana Zuboff parle de « surplus comportemental ». Ce dernier est le produit de l'exploitation des traces et données nourrissant des algorithmes de recommandations. Par conséquent, des entreprises comme Google ou Facebook ne chercheraient pas tant à monétiser notre identité, mais plutôt à influer sur nos comportements. On assisterait moins à une « automatisation des flux d'information nous concernant » qu'« à une automatisation de qui nous sommes. » Shoshana Zuboff prend donc clairement la défense d'un individualisme libéral, protégeant les droits des personnes, leur libre arbitre et leur autonomie. En bref, leur dignité. Elle écrit ainsi que « la modernité

[109] NORBERG Patricia A., HOME Daniel R., et HOME David, « The Privacy Paradox : Personal Information Disclosure Intentions versus Behaviors », *Journal of Consumer Affairs*, n° 41, 2007, p. 100-126.
ACQUISTI, Alessandro, MICHELE, Francine, MBO'O Ida, et ROCHELANDET Fabrice, « Les comportements de vie privée face au commerce électronique ». *Réseaux*, n° 167, 2011, p. 105-130

[110] MARWICK, A. E., BOYD, danah, « Networked privacy: How teenagers negotiate context in social media », *New Media & Society*, *16*(7), 2014, 1051-1067. https://doi.org/10.1177/1461444814543995
CASILLI, Antonio, « Contre l'hypothèse de la "fin de la vie privée" », *Revue française des sciences de l'information et de la communication,* 3 | 2013, http://journals.openedition.org/rfsic/630

[111] ROUVROY, Antoinette, BERNS, Thomas, « Gouvernementalité algorithmique et perspectives d'émancipation, le disparate comme condition d'individuation par la relation? », Réseaux, 2013/1,n° 177, p. 163-196

[112] ZUBOFF, Shoshana, *L'Age du capitalisme de surveillance*, Paris : Zulma, coll. Essais 2020, p.864.

occidentale s'était formée autour d'un canon de principes et de lois qui confère des droits individuels inviolables et reconnait le caractère sacré de chaque existence individuelle ».[113] Ces principes seraient menacés par le « pouvoir instrumentarien » exercé par le capitalisme de surveillance, lequel conduirait à la mort de l'individualité. Or c'est précisément cet ancrage libéral qui lui est parfois reproché. Ses analyses resteraient ancrées dans une conception occidentale de la personne[114]. Et certains chercheurs tentent de décentrer la notion de vie privée, par une critique de son fondement individualiste ou en la travaillant à partir d'un prisme de lecture décoloniale[115]. Il nous semble judicieux de s'y référer pour la suite de notre thèse, les ONG opérant souvent dans des terrains géographiques extraeuropéens et extraétatsuniens. Les lignes qui suivent porteront donc sur ce type d'approche, puis on en précisera ses apports à l'étude du numérique humanitaire.

### Approches décoloniales de la protection des données

Ce tournant décolonial est par exemple représenté par Nick Couldry et Ulises Mejias et leur théorie du « colonialisme des données ». Trois caractéristique du numérique contemporain justifient pour les chercheurs le fait de parler de colonialisme : le caractère global de la numérisation, sa dimension monopolistique et extractive[116]. Mais cette fois-ci, il ne s'agit pas simplement de récolter une ressource naturelle, ce sont nos vies quotidiennes qui seraient « exploitées ». Bien plus, ces dernières seraient façonnées de manière à générer de la valeur exploitable, à savoir des données. Cela suppose donc l'émergence d'une configuration sociale favorisant une économie fondée sur l'extraction informationnelle. Cette dernière repose sur des mécanismes incitatifs enjoignant à la production accrue de traces, les entreprises dominant l'écosystème numérique pouvant alors en tirer profit. Cette « mise en donnée » s'opèrerait au cours des différentes facettes de nos existences. Elle concerne le travail, via sa numérisation, notre santé, via la multiplication d'objets connectés et par l'émergence de mouvement de type « quantification de soi ». Enfin, elle englobe évidemment nos vies sociales par l'avènement de réseaux comme Facebook ou Tweeter. Or ce processus extractif exercerait une forme de violence sur les individus. Nick Couldry et Ulises Mejias sont sans appel : « Le problème le plus profond est la violence que le fait même de collecter des données par le biais de la surveillance fait subir à l'intégrité minimale du soi. »[117] Le « colonialisme de la donnée » aboutirait à la dissolution d'un « espace du moi » préservé de toute ingérence, d'un espace intérieur abritant la part réflexive de nous-mêmes.

---

[113] *Ibid*, p.61.

[114] FLAHAULT, François, « Interrogations sur la conception occidentale de l'individu », in : LE BART, Christian, et al. (eds), *L'individu aujourd'hui*, Presses universitaires de Rennes, 2010, https://doi.org/10.4000/books.pur.13638.

[115]COULDRY, Nick, MEJIAS, Ulises Ali,"The decolonial turn in data and technology research: what is at stake and where is it heading?", *Information, Communication & Society*, 26:4, 2023, p.786-802, DOI: 10.1080/1369118X.2021.1986102

[116] Sachant que les chercheurs définissent le terme de « donnée » comme suit : « c'est le matériel produit par un processus d'abstraction du monde en catégories, mesures et autres formes de représentation qui constituent les éléments de base à partir desquels l'information et la connaissance sont créées « Data is the "material produced by abstracting the world into categories measures and other representational forms that constitute the building blocks from which information and knowledge are created." MEJIAS, U. A., COULDRY, N., « Datafication. », *Internet Policy Review*, 8(4)., 2019, https://doi.org/10.14763/2019.4.1428

[117] « The deepest problem is the violence that the very fact of data collection through surveillance does to the minimal integrity of the self. » COULDRY, Nick, MEJIAS, Ulises*, The Cost of connection*, Palo Alto, Standford University Press, 2019, p.156.

Le « colonialisme de la donnée » s'attaquerait ainsi à la substance de notre « moi profond »[118]. Or laisser à découvert ce « moi » profond implique le fait de potentiellement perdre ce qui en constitue sa substance même : « C'est la réalité même du "moi" en tant que "moi" qui est en jeu. C'est l'intégrité minimale de la vie humaine qui doit être protégée. Cette réalité, que chaque sujet peut reconnaître en l'autre, ne peut être échangée sans mettre en danger les conditions fondamentales de l'autonomie humaine. »[119] Les auteurs font ainsi clairement référence à Giorgio Agamben et à son concept de « vie nue » pour décrire ce dépouillement de l'identité en jeu dans le « colonialisme de la donnée ». Or, pour Nick Couldry et Ulises Mejias préserver un espace intérieur est nécessaire pour conserver une forme d'autonomie. Ils écrivent ainsi que « l'espace du soi peut être compris comme l'espace ouvert dans lequel un individu donné expérimente, réfléchit et se prépare à décider de sa ligne de conduite. » Deux remarques, cependant. Tout d'abord, Nick Couldry et Ulises Mejias fondent leur réflexion sur la notion d'autonomie sans la lier à celle de dignité, et ce alors qu'elles sont profondément liées, comme on le verra par la suite. Cela est flagrant dans le droit à la protection des données, surtout au sujet de la notion d'autodétermination informationnelle. En outre, Nick Couldry et Ulises Mejias remarquent que cette notion d'autonomie est intellectuellement située, liée à l'histoire théorique occidentale, et justement critiquée par les tenants de la pensée décoloniale. Ils proposent ainsi d'en donner une version remaniée, moins centrée sur une conception individualiste de la personne. Mais ils ne rentrent pas dans le détail d'une telle refondation du concept, et ils ne se réfèrent pas aux théories du « care ». Pourtant les auteurs y étant rattachés ont repensé cette notion en lien avec celle de vulnérabilité, comme on l'abordera dans notre troisième partie.

Le deuxième trait du « colonialisme de donnée » est son caractère monopolistique. Pour Nick Couldry et Ulises Mejias, le processus d'extraction propre au « colonialisme de donnée » est conduit par un ensemble d'acteurs appartenant à ce qu'ils ont qualifié de « secteur de la quantification sociale ». Les GAFAM y occupent de fait une position centrale. Et les deux chercheurs rappellent le poids bien connu des GAFAM dans l'ensemble des couches constitutives du numérique (de l'infrastructure technique à la brique logicielle)[120]. Nick

---

[118]« L'espace du soi peut être compris comme l'espace ouvert dans lequel un individu donné expérimente, réfléchit et se prépare à adopter sa ligne de conduite. »
« The space of the self can be understood as the open space in which any given individual experiences, reflects, and prepares to settle on her course of action. » COULDRY, Nick, MEJIAS**,** Ulises, « Le colonialisme des données : repenser la relation entre le big data et le sujet contemporain », *Questions de communication*, 42, 2022, http://journals.openedition.org/questionsdecommunication/29845

[119]COULDRY, Nick, MEJIAS**,** Ulises,ibid.

[120]On retrouve cette domination sur les différentes couches du cyberspace. Ainsi au niveau de l'infrastructure (câble et centre de données), d'après le recensement de la plateforme Cloudscene, 2701 centres de données étaient installés aux États-Unis au mois de septembre 2022. Ils dominent ainsi très largement le classement mondial des data centers. https://fr.statista.com/infographie/24147/pays-avec-le-plus-de-data-centers-centres-de-donnees/
Au niveau logiciel, Microsoft domine le marché des systèmes d'exploitation, tout comme Google, Facebook, Yahoo etc. Pour chiffres, on peut se référer à un rapport du Sénat français de 2019. Selon cette source, Microsoft (Windows) et Apple (OS X) disposent respectivement de 78,43 % et de 13,53 % du marché des systèmes d'exploitation pour les ordinateurs personnels, Linux ne représentant que 1,6 % du marché ; ajoutons que Google (Chrome) détient près de 65 % et Apple (Safari) 15,15 % du marché des navigateurs web ;
- De surcroit, Google et Facebook détiennent plus de la moitié du marché de la publicité en ligne ; - Amazon représente près ou plus de la moitié du marché du commerce en ligne dans de nombreux pays ; Enfin, Amazon (33 %), Microsoft (16 %) et Google (8 %) représentent plus de la moitié (57 %) du marché des infrastructures de services d'informatique en nuage... LONGUET, Gérard, MONTAUGE, Franck, « Commission d'enquête sur la souveraineté numérique », Rapport Sénat, octobre 2019https://www.senat.fr/rap/r19-007-1/r19-007-11.pdf
COEHLO, Ophélie, *Géopolitique du numérique : l'impérialisme à pas de géants*, Paris: éditions de l'atelier, 2023, 256 p.
Précisons au passage que leur domination connaitrait ces deux dernières années un léger infléchissement d'après le chercheur Nikos Smyrnaios, sans pour autant que leur hégémonie soit remise en cause : « Ainsi, en 2022, la rentabilité exceptionnelle des géants de la Silicon

Couldry et Ulises Mejias s'inscrivent alors dans un ensemble plus général de travaux s'étant attelés à la description de la nature de la domination économique et politique des acteurs clefs du capitalisme numérique. Les angles d'attaque diffèrent cependant. Notons que l'usage de l'acronyme « GAFAM » tend à être critiqué. Certains auteurs préfèrent le terme de « Bigtech ». Il permettrait d'inclure d'autres acteurs du numérique détenant également un capital économique et symbolique d'influence (PayPal, Twitter, Tesla). Certains chercheurs y ajoutent les NATU (Netflix, Airbnb, Tesla et Uber), pour partie des plateformes désintermédiation de service. Pour d'autres chercheurs, comme Asma Mhalla, au-delà des indicateurs économiques, c'est le poids structurel et leur pouvoir d'influence qui justifient le choix du terme « Big tech ». L'auteure ne se concentre pas sur la dimension extractive de ces acteurs. Au contraire d'autres chercheurs qui choisissent de se restreindre à l'étude d'acteur dont le modèle marchand est fondé sur l'exploitation des données. Et s'ils rejettent l'usage de l'acronyme « GAFAM », c'est qu'il ne permet pas de différencier pas le schéma économique des différents acteurs le composant[121]. Par exemple, Shoshana Zuboff concentre son analyse sur Google, acteur à l'origine du modèle d'extraction du surplus comportemental[122]. Elle met de côté Apple, dont le modèle économique n'est pas pour elle centré sur l'exploitation des données[123]. Mais elle rappelle qu'il est aussi nécessaire d'inclure dans le capitalisme de surveillance d'autres acteurs a priori plus modestes, comme la compagnie Verizon, dont le modèle économique repose aussi sur l'exploitation de données personnelles.

Pour revenir à Nick Couldry et Ulise Mejias, dans le premier ouvrage *The Cost Of Connection* , les auteurs décrivent, classiquement, la domination des « Big Five ». Toutefois, leur ouvrage plus récent en exclut, sans que le choix soit explicité, Microsoft[124]. Il est maintenant question de « Big Four ». Mais au-delà de ces variations, le point le plus important est que Nick Couldry et Ulises Meijias ne limitent pas leur analyse à ces mastodontes. Le colonialisme des données repose aussi sur un ensemble d'acteurs techniques rendant possible le travail d'extraction.

---

Valley a décliné. Sous la pression des investisseurs, des coupes drastiques ont été effectuées, notamment dans les effectifs. Les chiffres donnent le tournis : entre janvier et décembre, plus de neuf cents entreprises technologiques ont licencié près de cent cinquante mille de leurs salariés. » ; Davantage scrutées pas les investisseurs et par les régulateurs, leurs activités risquent d'être moins juteuses que par le passé. Leur pouvoir de marché est progressivement restreint et leur influence politique plus encadrée. Cependant, les conditions objectives de leur hégémonie demeurent. Les gafam disposent toujours d'énormes réserves financières. Ils contrôlent l'essentiel de l'infrastructure logicielle de l'économie numérique et une grande partie de sa base matérielle. Si leur rentabilité est moindre, leur chiffre d'affaires continue de croître. « SMYRNAIOS Nikos, « Les GAFAM, entre emprise structurelle et crise d'hégémonie », *Pouvoirs*, 2023/2 (N° 185), p. 19-30. https://www-cairn-info.ezproxy.utc.fr/revue-pouvoirs-2023-2-page-19.htm

[121] ISAAC Henri, « Pour en finir avec l'acronyme GAFAM », *Pouvoirs*, 2023/2 (N° 185), p. 7-17. https://www-cairn-info.ezproxy.utc.fr/revue-pouvoirs-2023-2-page-7.htm

[122] « De même que le capitalisme de surveillance ne se réduit pas à la technologie, cette nouvelle logique d'accumulation ne peut être réduite à une seule entreprise ou à un groupe. Les cinq géants du web – Apple, Google, Amazon, Microsoft et Facebook – sont souvent considérés comme une seule entité aux stratégies et aux intérêts similaires, mais quand il s'agit du capitalisme de surveillance, ce n'est pas le cas. »

[123] « Ainsi, Apple s'est jusqu'ici fixé une ligne de conduite, en promettant de s'abstenir de nombreuses pratiques que je range dans le régime capitaliste de surveillance. Son comportement à cet égard n'est pas parfait, sa ligne est parfois floue, et il se pourrait qu'Apple change d'orientation ou se contredise. » (référence) ZUBOFF
Ainsi, le rapprochement récent entre Apple et Open Ai a été interprété comme un tournant pour l'entreprise de Steve Jobs en matière de protection de la vie privée de ses utilisateurs.
TAR, Julia, "Apple : l'intégration de ChatGPT soulève des questions de concurrence et de confidentialité des données », *Euractiv*, 17/06/2024 https://www.euractiv.fr/section/application-de-la-loi/news/apple-lintegration-de-chatgpt-souleve-des-questions-en-matiere-de-concurrence-et-de-confidentialite-des-donnees/

[124] Et ce alors que Zuboff note bien son importance au sein du capitalisme de surveillance : « Parmi les trois autres entreprises Internet les plus importantes, à savoir Microsoft, Apple et Amazon, ce fut Microsoft qui se tourna la première, et sans hésiter, vers le capitalisme de surveillance comme moyen de restaurer son leadership dans le secteur Tech, avec la nomination de Satya Nadella au poste de PDG en février 2014. Microsoft avait notoirement manqué plusieurs fois l'occasion de concurrencer Google en matière de recherche et de développer ses capacités dans le domaine de la publicité ciblée. Dès 2009, quand il était encore vice-président et directeur de la division Business, Nadella critiqua publiquement l'entreprise pour n'avoir pas su reconnaître les opportunités associées à cette première phase du capitalisme de surveillance. » ZUBOFF, Shoshanna, *L'âge du capitalisme de surveillance*, Paris : Zulma poche, 2019, p.224-225

Leur analyse englobe donc également des acteurs, comme les fabricants de hardware[125], de software[126], des objets connectés et des plateformes de divertissement. Les chercheurs y incluent aussi un ensemble d'acteurs impliqué dans l'exploitation de données, des « data scientist », des courtiers en données, mais aussi toute une série d'acteurs impliqués dans le travail du clic (décrits par Antonio Cassili). Notons que d'autres chercheurs, comme Sébastien Broca, rappellent que les géants du Web dépendent également d'une série de sous-traitants, situés pour certains dans les pays dits du Sud[127], d'où une dimension globale du colonialisme des données. D'ailleurs pour Nick Couldry et Ulises Meijias, il est nécessaire de prendre en compte d'autres zones géographiques que les USA. Et ces derniers incluent donc dans leur analyse les « homologues » chinois des GAFAM, les BATX, à savoir Baidu, Alibaba, Tencent, Xiaomi. Une dernière question reste en suspens à la lecture de l'ouvrage de Nick Couldry et Ulises Meijias : qu'en est-il des formes de résistances au secteur de la quantification sociale, et comment sont envisagés des usages numériques alternatifs ? C'est dans un second ouvrage des auteurs, plus récent, qu'on peut trouver des éléments de réponse à cette question. Nick Couldry et Ulises Meijias y décrivent les différentes modalités de résistance au système extractif. Elles comprennent des acteurs s'opposant aux Big Tech et aux GAFAM. Il s'agit soit d'acteurs proches du logiciel libre, soit d'acteurs défendant un idéal de « souveraineté numérique ». Mais plutôt que de souveraineté européenne[128], les auteurs se tournent vers des initiatives venant du Sud Global, notamment du continent latino-américain[129].

Remarquons ensuite qu'on n'a pour le moment parlé que d'entreprises. Or, si Ulises Mejias et Nick Couldry se concentrent en grande partie sur les firmes privées, si ces dernières jouent un rôle central au sein du « capitalisme de la donnée », ce sont les États qui auraient rendu possible son avènement. Nick Couldry et Ulises Mejias rappellent en effet que les acteurs étatiques ont favorisé le développement du secteur des technologies par un cadre juridique favorable, via sa dérégularisation. Et ils ajoutent que les données extraites par les firmes seraient réutilisées par les gouvernements, et remployées à des fins de contrôle social ou sécuritaire.

Cela dit, leur relation serait caractérisée par une forme d'interdépendance, qui n'est pas exempte de contestation de la part du secteur privé, comme a pu le montrer le politiste

---

[125] « The hardware area includes manufacturers of digital devices that extract and use social data, from laptops and tablets to phones and watches to gaming consoles, robots, cars, drones, and so on. A manufacturer of a "dumb" television set would not be part of the social quantification sector, but any manufacturer of a "smart" device (a product that collects and analyzes information about its user) would be included. This sector also includes the manufacturers of the infrastructure required to run the social quantification sector (routers, servers, transmitters, and so on) and the service providers that deploy hardware to deliver internet and phone access to individuals. » « " COULDRY, Nick, MEJIAS, Ulises*, The Cost of connection*, Palo Alto: Standford University Press, 2019, P.51

[126] "Soft ware includes the developers of the programs and environments that support social quantification, including operating systems, websites, applications, services, games, apps, and plug-ins. Examples in this domain include Google, Apple, Microsoft, and Ubisoft." COULDRY, Nick, MEJIAS, Ulises, Ibid.

[127]« la perspective du système-monde permet également de porter le regard, non pas uniquement vers les grandes entreprises issues du nouveau centre hégémonique, mais vers des acteurs périphériques et semi-périphériques souvent moins visibles. Le capitalisme numérique repose en effet sur des chaînes de valeur globales, au sein desquelles se nouent des relations asymétriques. Les acteurs économiques centraux y captent la majeure partie de la valeur produite, tout en externalisant et en sous-traitant un grand nombre d'activités industrielles et informationnelles comme la fabrication des terminaux (Qiu, 2016), la modération des contenus sur les réseaux sociaux commerciaux (Roberts, 2020), ou encore la constitution des bases de données servant à "entraîner" les programmes d'intelligence artificielle (Casilli, 2019). » BROCA Sébastien, « Le capitalisme numérique comme système-monde. Éléments pour une métacritique », *Réseaux*, 2022/1 (N° 231), p. 167-194. https://www-cairn-info.ezproxy.utc.fr/revue-reseaux-2022-1-page-167.htm

[128] LETERME, Cédric, « Mirages de la « souveraineté numérique européenne », *Le Vent se lève*, 28/05/2024 https://lvsl.fr/mirages-de-la-souverainete-numerique-europeenne/#sdfootnote8anc

ÁVILA PINTO Renata, « La souveraineté à l'épreuve du colonialisme numérique », dans : Cédric Leterme éd., *Impasses numériques. Points de vue du Sud.* Paris, Éditions Syllepse, « Alternatives Sud », 2020, p. 25-35. https://www.cairn.info/impasses-numeriques--9782849508183-page-25.htm

[129] MEJIAS, Ulises, COULDRY, Nick, *Data Grab, the new colonialism of Big Tech and how to fight back*, WH allen, 2024, 320 p.

Charles Thibout[130]. Nick Couldry et Ulises Mejias ne décortiquent cependant pas les modalités de circulation de données (et d'acteurs) entre États et entreprises[131]. Les chercheurs évoquent aussi assez brièvement les effets du réemploi de données en matière de contrôle social, sur lequel David Lyon ou d'autres chercheurs, comme Virginia Eubanks, ont pu travailler. Et Nick Couldry et Ulises Mejias ne détaillent également pas les usages sécuritaires par les États de données collectées par les entreprises.

Shoshana Zuboff adopte un angle d'étude différent. Selon elle, la dimension sécuritaire a au contraire joué un rôle moteur dans l'élaboration du capitalisme de surveillance. Elle a recours au concept webérien d'affinité élective pour décrire les liens entre les entreprises privées et l'État américain, notamment ses agences de renseignement (comme la NSA). Elle note ainsi que : « Ces affinités électives ont soutenu l'exceptionnalisme de surveillance et contribué au terreau sur lequel la mutation du capitalisme de surveillance s'est développée jusqu'à sa pleine maturité. »[132] Citons encore un autre passage de cette auteure dans lequel elle déclare que « sans l'exceptionnalisme de la surveillance, il est possible que ces données n'existent même pas, du moins pas dans leur volume et leur détail actuels. L'exceptionnalisme en matière de surveillance a contribué à déterminer l'évolution du capitalisme de l'information en créant un environnement dans lequel les pratiques de surveillance naissantes de Google ont été recherchées plutôt que contestées. »[133]

Nick Couldry et Ulises Mejias se détachent cependant de ce prisme américain. Pour eux, le colonialisme des données constitue un phénomène global. Ils insistent toutefois sur le fait que ses conséquences se font plus sentir dans des zones marquées par un héritage colonial, ainsi que chez des groupes sociaux rattachés au Sud global[134]. Nick Couldry et Ulises Mejias prennent l'exemple des biais des algorithmes, pouvant exprimer des discriminations de genre, de classe ou de race, en fonction des préconceptions inhérentes aux ingénieurs les développant. Cela dit, précisons que pour Nick Couldry et Ulises Mejias le « colonialisme des données » n'oppose pas l'Occident au reste du monde, puisqu'il comprend un autre pôle de puissance, la Chine. Les chercheurs précisent ainsi que ce choix complique leur « notion géographique du Sud global, un concept qui, jusqu'à présent, permettait de situer la résistance et la perte d'identité selon les démarcations géographiques entre anciens colonisateurs et anciens colonisés. Au lieu de cela, le nouveau colonialisme des données agit à la fois depuis

---

[130] THIBOUT Charles, « Google et l'État fédéral états-unien : interdépendance, contestation et hybridation », *Entreprises et histoire*, 2021/3 (n° 104), p. 142-163. https://www.cairn.info/revue-entreprises-et-histoire-2021-3-page-142.htm
THIBOUT Charles, « Les GAFAM et l'État : réflexion sur la place des grandes entreprises technologiques dans le champ du pouvoir », *Revue internationale et stratégique*, 2022/1 (N° 125), p. 75-88. https://www.cairn.info/revue-internationale-et-strategique-2022-1-page-75.htm

[131] MHALLA, Asma, « Les *Big Tech*, de nouveaux États parallèles ? », *Pouvoirs*, 2023/2 (N° 185), p. 69-81. https://www-cairn-info.ezproxy.utc.fr/revue-pouvoirs-2023-2-page-69.htm

[132] « These elective affinities sustained surveillance exceptionalism and contributed to the fertile habitat in which the surveillance capitalism mutation would be nurtured to prosperity. »ZUBOFF, Shoshana, *L'Age du capitalisme de surveillance*, Paris, Zulma, 2020, p.80.

[133] « Had it not been for surveillance exceptionalism, it is possible that these data would not even exist, at least not in their current volume and detail. Surveillance exceptionalism helped to shape the evolutionary course of information capitalism by creating an environment in which Google's budding surveillance practices were coveted rather than contested. »
ZUBOFF, Shoshana, *ibid.* p.83.

[134] « la thèse du colonialisme de données n'est pas limitée à des sites historiques particuliers d'exploitation coloniale. Les ressources du colonialisme de données sont partout (la vie humaine est partout). Ses conséquences sont cependant particulièrement néfastes lorsqu'elles se superposent à l'héritage colonial historique. »« The data colonialism thesis is not limited to particular historical sites of colonial extraction. This new colonial appropriation can occur wherever the resources it extracts are situated, which means potentially anywhere (since human life is everywhere), even if its consequences are particularly malign where it overlaps with historic colonialism's legacy. » COULDRY, Nick, MEJIAS, Ulises, "The decolonial turn in data and technology research: what is at stake and where is it heading?", *Information, Communication & Society*, 26:4, 2023, p. 786-802, DOI: 10.1080/1369118X.2021.1986102

l'extérieur à l'échelle mondiale et depuis l'intérieur sur ses propres populations. Les élites du colonialisme des données (Facebook par exemple) bénéficient de ces deux dimensions de la colonisation et les divisions Nord-Sud et Est-Ouest n'ont plus la même portée. »[135] Leurs analyses se distancient quelque peu — d'autres chercheurs s'attachant à prendre en compte la division Nord-Sud dans leurs travaux sur les répercussions en matière de vie privée d'acteurs clefs du numérique. On pense par exemple à Stefania Milan et Emiliano Treré. Ces derniers nous invitent à travailler sur les conséquences de la datafication sur d'autres aires, rattachées au Sud global, sur d'autres acteurs, situés « en bas de la pyramide des données ». Et ils appellent à déconstruire ainsi ce qui constitue pour eux un prisme occidentalocentré et universaliste des « data studies ».

Ainsi, certains chercheurs réfléchissant sur les effets politiques et sociaux de la numérisation de nos sociétés inscrivent leurs pensées directement dans la lignée des problématiques des études postcoloniales. Ils font référence à des auteurs, comme Edward Said, Gayatri Chakravorty Spivak et Homi Bhabha. Ces derniers proviennent des « Cultural studies » et s'intéressent à des enjeux de représentations et de rationalisation comme dispositifs de pouvoir. Nick Couldry et Ulises Mejias, préfèrent alors parler de « colonialité », concept forgé par deux philosophes proches de la pensée décoloniale : Anibal Quijano et Nelson Maldonado Torres. Ce concept désigne alors la persistance malgré la décolonisation d'une structure hiérarchique raciale, économique et épistémique, distinguant Occidentaux et non-Occidentaux.

Ainsi Paula Ricaurte se concentre sur les épistémologies associées aux connaissances de type « pilotées par la donnée » (« data driven »), en pointant les formes de domination qu'il charrie. D'autres travaux rattachés à cette approche mobilisent de façon plus centrale la notion de vie privée, la plupart adoptant un point de vue critique du fait de son caractère occidentalocentré. La notion de vie privée ne serait pas adaptée pour analyser des situations extraeuropénnes et extraaméricaines. Il serait donc nécessaire de réfléchir à des notions locales équivalentes, ou bien construire de nouveaux concepts plus appropriés. Olinger et Britz tentent ainsi d'inclure dans leurs réflexions la structuration communautaire de certaines sociétés africaines. Ils proposent ainsi de forger une conception de la vie privée fondée sur le concept d'Ubuntu. Ce terme est issu des langues australes et popularisé lors de l'apartheid par Nelson Mandela et Desmond Tutu. Il mettrait en lumière l'interdépendance des individus. Leur démarche prend cependant le risque d'un certain culturalisme. La chercheuse Payal Arora adopte une analyse plus nuancée. Le concept de vie privée est certes situé. Il reste ancré dans les schèmes intellectuels occidentaux. Cette position a cependant deux conséquences qu'elle critique. Premièrement, elle implique que les personnes de culture non occidentale auraient une conception de l'intime irrémédiablement différente de celles des Occidentaux. Les « privacy studies » se sont construites sur un « exceptionalisme ». La vie privée serait un concept occidental, n'étant pas pertinente pour analyser les relations sociales hors Europe. Mais dans le même temps, cet « exceptionalisme » se doublerait d'un universalisme : le RGPD devient le texte de référence en matière de droit de la protection des données, voué à s'exporter mondialement. Pour elle, cet universalisme résulte de dynamiques de dominations

[135] COULDRY, Nick, MEJIAS, Ulises A., « Le colonialisme des données : repenser la relation entre le big data et le sujet contemporain », *Questions de communication*, 42 | 2022, http://journals.openedition.org/questionsdecommunication/29845

proprement occidentales. Et le RGPD ne refléterait pas les réalités locales. Pour comprendre les répercussions en matière de vie privée dans le Sud global, il est nécessaire selon Payal Arora d'en saisir les spécificités. Cela nécessite pour la chercheuse de s'intéresser à l'histoire longue, à savoir les déterminismes passés et les legs coloniaux. Mais dans le même temps, Payal Arora surligne le fait qu'il est nécessaire de déconstruire l'image d'un Sud global figé, d'autant que l'ordre géopolitique contemporain est en pleine évolution. Elle invite à se méfier des approches adoptant un prisme trop général, passant à côté du fait que le Sud global est composé de réalités plurielles. Ainsi elle remet en perspective la dichotomie Nord/sud propre aux approches post coloniales en rappelant que : « les violations à la vie privée peuvent aussi venir des périphéries. »[136]

Antonio Casilli rejoint les réflexions de Payal Arora. Ce dernier adopte un usage critique du terme de colonialisme. Certes, Antonio Casilli s'est spécialisé sur le « digital labor ». Il a visibilisé l'exploitation de travailleurs du Sud global par des plateformes. Ces formes d'exploitation s'inscrivent effectivement dans une logique de dépendance économique, héritée d'une longue histoire de dépendance. Mais pour Antonio Casilli, utiliser le terme de « colonialisme » risque de le galvauder, de le déshistoriciser. Il repose une forme d'orientalisme. Et l'employer risque de réduire les pays du Sud à des acteurs passifs, pris dans des rapports de domination. En outre, le clivage Nord/Sud peut être nuancé, au regard des reconfigurations géopolitiques actuelles. En matière de numérique, les anciens empires coloniaux, la Grande-Bretagne, la France ou l'Espagne n'ont que peu d'importance face à d'autres joueurs comme les États-Unis ou la Chine. Enfin, ces derniers opèrent largement au-delà de leurs sphères historiques d'influence, comme en Afrique[137]. Si Nick Couldry et Ulises Mejias insistent sur le fait que s'il faut étudier les asymétries politiques, économiques et culturelles entre le Nord et le Sud, certains chercheurs appellent aussi à dépasser les caractéristiques historiques du colonialisme. Par exemple, Antonio Cassili donne une interprétation très large du terme de « colonialité », dans le sens où il renvoie à un « ressenti que l'on peut tout aussi bien trouver dans des pays sans histoire coloniale. »[138] Il se réfère ainsi aux travaux de Nelson Maldonado-Torres pour qui la notion de colonialité décrit de « vielles structures de pouvoir issues du colonialisme, mais qui déterminent la culture, le travail, les relations intersubjectives et la production de connaissances bien au-delà des limites strictes des administrations coloniales. »[139]

Mais maintenant que le cadre théorique est posé, que faire de ce dernier ? La littérature sur le numérique humanitaire s'est-elle emparée de ces travaux ? Et si oui, comment ? En somme, comment s'exprime le colonialisme informationnel dans l'espace humanitaire ? Il se trouve que Nick Couldry et Ulisses Mejias sont régulièrement cités dans les articles relatifs au

---

[136] ARORA, P. "Decolonizing Privacy Studies", *Television & New Media*, *20*(4), 2019, p.366-378. https://doi.org/10.1177/1527476418806092

[137] CASILLI, Antonio, "Digital Labor studies go global: toward a digital decolonial turn." *International Journal of Communication*, 11, 2017, p.3934-3954

CASILLI, Antonio, "Is There a Global Digital Labor Culture? : Marginalization of Work, Global Inequalities, and Coloniality", 2nd symposium of the Project for Advanced Research in Global Communication (PARGC), Apr 2016, Philadelphie, United States.

[138] CASILLI, Antonio, ibid.

[139] "long-standing patterns of power that emerged as a result of colonialism, but that define culture, labor, intersubjective relations, and knowledge production well beyond the strict limits of colonial administrations" MALDONADO-TORRES, N. "On the Coloniality of Being: Contributions to the Development of a Concept", *Cultural Studies*, 2007, 21(2-3), p. 240-270

numérique humanitaire. Par exemple, Mirca Madianou se réfère explicitement à ces auteurs. Son approche diffère cependant quelque peu de celle de Nick Couldry et Ulisses Mejias qui adoptent une approche globalisante. Mirca Madianou se concentre sur les dynamiques internes au champ de l'humanitaire. Mais surtout, si Nick Couldry et Ulisses Mejias s'intéressent aux effets du colonialisme des données dans des contextes extraoccidentaux, pour Mirca Madianou, leur modèle théorique n'est pas suffisant pour saisir la spécificité des sociétés du Sud global. Elle déclare ainsi que : « certains de ces arguments passent sous silence les asymétries structurelles entre le Nord et le Sud, qui sont au cœur de la notion de technocolonialisme. » [140]

Par voie de conséquence, les pratiques informationnelles des ONG reflètent selon la chercheuse des relations de pouvoir dues à la dimension spécifiquement néocoloniale de l'aide. La continuité entre humanitaire et passé colonial se manifesterait par des inégalités structurales entre bailleurs, travailleurs humanitaires et bénéficiaires. Afin de conforter son analyse, Mirca Madianou s'appuie sur le travail d'Ann Stoler[141]. Elle reprend son concept de « débris d'empires coloniaux ». Mirca Madianou n'utilise donc pas le terme de « colonialisme » comme une forme de métaphore, ni ne considère qu'on assisterait à une nouvelle forme de colonialisme. Les empires coloniaux se sont effondrés, mais il resterait des traces du colonialisme, dont l'humanitaire fait partie.

Pour décrire la numérisation croissante de ce secteur, Mirca Madianou a ainsi forgé le terme de « technocolonialisme », qui lui permet de théoriser la façon dont la numérisation vient réactiver le passé colonial de l'humanitaire. Sachant que le terme de technocolonialisme permet de décrire « comment l'innovation numérique, les données et les pratiques d'intelligence artificielle renforcent les asymétries de pouvoir et engendrent de nouvelles formes de violence structurelle et de nouvelles inégalités entre le Sud et le Nord. Le technocolonialisme éclaire la convergence des développements numériques avec les structures humanitaires, le pouvoir de l'État et les forces du marché, et la mesure dans laquelle ils revigorent et retravaillent les relations coloniales. «[142]

Pour la chercheuse le numérique servirait de révélateur. Il mettrait à jour des inégalités préexistantes : « Comment le numérique retravaille-t-il et revitalise-t-il les "débris impériaux" ? Les interventions numériques rendent-elles tangible ce qui était auparavant intangible ? Révèlent-elles ou occultent-elles davantage les histoires de l'exploitation ? Je soutiens que la technologie numérique et les pratiques en matière de données matérialisent

[140] MADIANOU, M., "Technocolonialism: Digital Innovation and Data Practices in the Humanitarian Response to Refugee Crises." *Social Media + Society*, *5*(3), 2019. https://doi.org/10.1177/2056305119863146
"Some of these arguments gloss over the structural asymmetries between the global north and south which are at the heart of the notion of technocolonialism."
[141] STOLER, Ann Laura (dir), *Imperial debris : on ruins and ruination*, Duke University Press, 2013, 384 p.
[142] "how digital innovation data and AI practices entrech power asymmetries and engender new forms of structural violence and new inequities and between the Global South and North. Technocolonialism illuminâtes the convergence of digital developments with humanitarian structures, state power and market forces and the extent to which they reivigorate and Rework colonial relationships.
the digitalization of EU borders and the production of vulnerabilities",Heinrich Boll Stiftung, 13/06/2024 https://www.youtube.com/live/rtRAAOY1EkU

les formes et les débris intangibles de l'héritage colonial. En outre, les inégalités sont ancrées dans la nature extractive du technocolonialisme. »[143]

Le technocolonialisme serait ainsi pour elle associé à trois caractéristiques : sa dimension extractive, son caractère expérimental, sa finalité de contrôle et de surveillance des individus. Précisons enfin que Mirca Madianou ne travaille pas spécifiquement sur les enjeux de vie privée. Elle prend en compte l'ensemble des discriminations et des inégalités associées au numérique humanitaire. Cependant, les trois facettes du technocolonialisme concernent la protection des données. Il s'agit tout d'abord de sa dimension extractive. Mirca Madianou montre comment les bénéficiaires sont dépossédés de leurs propres données. Elle revient en partie sur le non-respect dans l'humanitaire de certains droits propres au RGPD, surtout ceux liés à l'autodétermination informationnelle des bénéficiaires. Une deuxième dimension du technocolonialisme est relative à sa dimension expérimentale. Le technocolonialisme se déploie dans des zones de non-droit et ne suit donc pas les standards des lois sur la protection des données. Et une dernière facette du technocolonialisme concerne l'usage de dispositifs numériques, comme la biométrie, à des finalités de surveillance des populations dans le cadre d'une forme de gouvernance humanitaire, mêlant « care » et « contrôle », qui impose aux bénéficiaires des violences à la fois symboliques et physiques.

On peut donc retenir ces trois points qu'on développera dans la suite de la thèse. Effectivement, notre travail s'appuie en partie directement sur les analyses de Mirca Madianou. Mais nous les nuancerons et complèterons. En effet, selon nous, les humanitaires prennent en compte ces effets de pouvoir qui percutent leur propre cadre éthique. Une partie des acteurs appartenant à ce secteur tentent donc d'y remédier.

### Souveraineté étatique et espace humanitaire numérique

Une deuxième dynamique contribue à renforcer les risques liés à la numérisation du secteur de la solidarité internationale. Elle concerne les répercussions de l'exercice des souverainetés étatiques sur ce qui est qualifié d'« espace humanitaire », dont l'intégrité serait alors remise en cause. Un bon nombre d'auteurs parlent en effet de « rétrécissement » et de perte d'indépendance de ce dernier. Cette proposition soulève une série de questions. En effet, quel lien est-il possible d'établir entre les atteintes portées à l'espace humanitaire et les enjeux de protection des données ? Comment envisager la dimension numérique de cet espace ? Et enfin, comment le protéger ?

Mais avant de répondre à ces interrogations, il est impératif de définir le concept de souveraineté. Tout d'abord, ce serait Jean Bodin qui au XVIe siècle en donne une première théorisation. La souveraineté désigne alors la faculté d'avoir la maitrise d'un territoire et d'y

[143] "how does the digital rework and revitalize "imperial debris"? Do digital interventions make tangible the previously intangible, do they reveal or further occlude histories of exploitation? I argue that digital technology and data practices materialize the intagible forms and debris of colonial legacies. Furthermore, inequalities are entrenched by the extractive nature of technocolonialism." MADIANOU, M., "Technocolonialism: Digital Innovation and Data Practices in the Humanitarian Response to Refugee Crises." *Social Media + Society*, *5*(3), 2019. https://doi.org/10.1177/2056305119863146

être l'autorité suprême, la « puissance absolue et perpétuelle » selon les mots de Jean Bodin[144]. Cette première conception de la souveraineté a évidemment connu par la suite des variations selon les traditions juridiques et selon les différents auteurs de philosophie politique. Sans rentrer dans le détail de la cristallisation de ce concept, ajoutons que pendant un temps, il a été commun de parler de souveraineté interne et externe. Ainsi, le principe de souveraineté d'un point de vue externe s'inscrit à l'échelle internationale. Il désigne le respect par l'ensemble des acteurs étatiques du principe de non-intervention. D'un point de vue interne, la souveraineté signifie le fait d'assoir son autorité sur l'ensemble des acteurs présents sur le territoire. Cela va de pair avec le contrôle de sa population, mais aussi avec l'obligation d'assurer l'ordre et la sécurité sur un territoire[145] et la prérogative sur un certain nombre de pouvoirs et de devoirs qualifiés de régaliens, comme le fait d'assurer la sécurité des citoyens d'un Etat et d'assurer la défense de son territoire.

Mais il est admis qu'on assisterait à une recomposition, voire à un effritement plus général des souverainetés étatiques. Cela en raison de nombreux facteurs. Tout d'abord, cette érosion des souverainetés étatiques, dont l'ampleur reste discutée, résulte de l'influence de la globalisation[146] et de l'intensification de dynamiques transnationales.

Cela se traduit par l'entrée en scène d'autres acteurs concurrençant les États dans l'exercice de leur souveraineté comme des organisations internationales, régionales, des groupes armés non étatiques ou d'acteurs privés comme des firmes transnationales[147]. Cette dualité entre échelle nationale et échelle transnationale a pu être nuancée, notamment par Didier Bigo[148], qui a pu mettre en avant l'action d'acteurs associés à des activités régaliennes, sécuritaires et policières investissant l'échelle internationale, via des organisations internationales et des réseaux de coopération. Cela est également le cas des réseaux de renseignements financiers qu'on abordera dans notre 4ème chapitre sur le contrôle du financement du terrorisme.

---

[144] « Le but politique poursuivi par Bodin consiste à donner une théorie systématique du pouvoir et du droit nécessaire à la refondation des institutions politiques de la monarchie française, en face de l'Empire et du Saint-Siège. Il le fait en relisant de façon critique la tradition philosophique et juridique de l'imperium et de la potestas, et en appelant de ses vœux une rupture nette avec les vestiges du féodalisme, c'est-à-dire avec ce qui restait de l'émiettement territorial du pouvoir et de l'hétérogénéité des formes d'autorité. D'où l'affirmation de l'unité de la source de la législation. La souveraineté vraie est « puissance absolue et perpétuelle ». La formule signifie que le souverain peut s'affranchir des lois et règles existantes. La nouveauté est que Bodin en fait non pas une pratique exceptionnelle, mais l'essence même du pouvoir politique, transposant la potestas absoluta que s'était attribuée le pouvoir pontifical bien avant lui. La nouveauté, en effet, est qu'elle s'applique non plus au seul pape, comme l'avaient conçue les canonistes et les glossateurs pontificaux, mais au roi, ou plus exactement à tous les souverains, roi, aristocratie ou peuple, puisque ce qui est en cause, ce n'est pas l'une des formes possibles de pouvoir, et encore moins un monarque en particulier, mais la forme même de l'État." DARDOT, Pierre, LAVAL, Christian, *Dominer: enquête sur la souveraineté de l'État en Occident*, Paris: la Découverte,2020, p.358

[145] Pour Foucault se serait opérée au XVIème une rupture dans l'exercice de la souveraineté des États, qui engloberait désormais « une rationalité gouvernementale ». Comme le résument Pierre Dardot et Christian Laval : « Désormais, la souveraineté ne se résumera plus comme chez Bodin au monopole de la loi, elle consistera dans l'imposition de règlements et de codifications dans tous les domaines de l'existence. On aurait ainsi grand tort de penser que le déploiement administratif de la police se fait au détriment de la souveraineté. La police générale, c'est le pouvoir général du souverain d'administrer et de réglementer le royaume, et donc la faculté qu'il se donne de se mêler aux choses les plus concrètes et les plus diverses de la vie de la population, aux mœurs, à la religion, à la circulation des produits et des hommes, au commerce, à la communication des idées, à l'hygiène, à la santé, à la subsistance, etc. » DARDOT Pierre, LAVAL Christian, « Chapitre 6. Raison d'État, souveraineté et gouvernementalité », dans : DARDOT, Pierre, LAVAL, Christian (dir.), *Dominer.Enquête sur la souveraineté de l'État en Occident*, Paris, La Découverte, « Sciences humaines », 2020, p. 303-358.

[146] SASSEN, S., *Losing Control : Sovereignty in an Age of Globalisation,* New York: Columbia University Press, 1995, 128 p.
BADIE, Bertrand, *Un monde sans souveraineté. Les États entre ruse et responsabilité*, Paris: Fayard, 1999, 304 p.

[147]HIBOU, Béatrice, éd., *La privatisation des États,* Paris: Karthala, « Recherches internationales », 1999, 400p.

[148] BIGO, Didier, « Pour une sociologie des guildes transnationales », *Cultures & Conflits* , 109 | 2018, http://journals.openedition.org/conflits/19739

On assisterait parallèlement à une complexification des conflits et à la multiplication de guerres civiles, de conflits asymétriques, de conflits de basses intensités, interprétées comme portées par des dynamiques identitaires[149]. On peut noter que l'idéal type de l'État souverain sert de contrepoint à des États jugés fragiles, d'États qualifiés de « faillis » aux souverainetés défaillantes, stigmatisées, car représentant une menace pour l'ordre mondial[150]. Et si le Sud global a pu être considéré comme le principal champ de périls et pourvoyeur de risque, pour les États dits du Sud, le terme de souveraineté a aussi acquis une connotation spécifique. Il signifie aussi la volonté de construire et renforcer leur indépendance face aux anciennes puissances coloniales, auxquelles les ONG peuvent être dans certains cas associées[151]. Sachant, en outre, que ce désir d'indépendance et de souveraineté est éminemment politique[152]. Il peut être ainsi instrumentalisé, comme a pu le montrer le chercheur Kévin Limonier sur le terrain africain, où les contestations contre l'influence persistante d'acteurs occidentaux sont attisées, entre autres par le gouvernement russe[153].

Enfin, il faut ajouter un dernier facteur de recomposition des souverainetés étatiques : l'émergence d'un espace numérique, qualifié parfois de cyberspace. En effet, ce dernier échappe, en partie, au contrôle des États. Il déborde les territoires physiques et les frontières nationales, du fait de l'interconnexion des systèmes d'information. Autre difficulté, les États doivent partager le contrôle du cyberspace avec d'autres acteurs qui y jouent un rôle primordial, les entreprises privées, dont les GAFAM[154], voire des acteurs plus informels, comme les hackers qui contestent le monopole de la violence étatique. Les États dépendent en outre de technologies produites et maitrisées par d'autres nations, notamment par les États-Unis, ainsi que la Chine.

Retrouver une forme de souveraineté numérique nécessite de prendre en compte la capacité d'un État à agir dans le cyberspace. Différents entrepreneurs de cause, politiciens, entrepreneurs, clament alors la nécessité alors de se doter d'outils numériques souverains afin de pouvoir contrôler les réseaux, les communications électroniques et les données, publiques ou personnelles. La maitrise de cet espace numérique est associée à de multiples enjeux, économiques, juridiques et géopolitiques[155]. Pour certains acteurs, la maitrise des technologies va de pair avec une politique de relance industrielle, à l'échelle française ou européenne.

---

[149] MARCHAL Roland, MESSIANT Christine, « Les guerres civiles à l'ère de la globalisation. Nouvelles réalités et nouveaux paradigmes », *Critique internationale*, 2003/1 (nº 18), p. 91-112. https://www.cairn.info/revue-critique-internationale-2003-1-page-91.htm

[150] ZARTMAN, W, *Collapsed Sates. The Desintegration and Restauration of Legitimate Authority*, Commons Boulder : Lynne Rienner Publishers, 1995, 304 p.
GAULME, François, « « États faillis », « États fragiles » : concepts jumelés d'une nouvelle réflexion mondiale », *Politique étrangère*, 2011/1, p. 17-29. https://www.cairn.info/revue-politique-etrangere-2011-1-page-17.htm

[151] ÁVILA PINTO, Renata, « La souveraineté à l'épreuve du colonialisme numérique », dans : LETERME, Cédric (éd.), *Impasses numériques. Points de vue du Sud,* Paris: Éditions Syllepse, « Alternatives Sud », 2020, p. 25-35. https://www.cairn.info/impasses-numeriques--9782849508183-page-25.htm

[152] NOCETTI, Julien, « La souveraineté numérique, un instrument de politique étrangère », in : *La souveraineté numérique : dix ans de débats, et après ?*, Annales des mines, n° 23, septembre 2023, p.18 https://www.annales.org/enjeux-numeriques/2023/en-23-09-23.pdf

[153] LIMONIER, Kevin, « La "souveraineté numérique", nouveau vecteur de l'influence russe en Afrique francophone? », *Le Rubicon*, 01/02/2024 https://lerubicon.org/la-souverainete-numerique-nouveau-vecteur-de-linfluence-russe-en-afrique-francophone/

[154] NOCETTI, Julien, « Des acteurs systémiques ? Les GAFAM au centre des jeux internationaux », dans: TAILLAT, Stéphane, (éd.), *La Cyberdéfense. Politique de l'espace numérique,* Paris: Armand Colin, « Collection U », 2023, p. 174-181. https://www.cairn.info/la-cyberdefense--9782200634223-page-174.htm

[155] DANET Didier, DESFORGES Alix, « Souveraineté numérique et autonomie stratégique en Europe : du concept aux réalités géopolitiques », *Hérodote*, 2020/2-3 (N° 177-178), p. 179-195. https://www.cairn.info/revue-herodote-2020-2-page-179.htm

Mais garder la main sur les informations stockées sur les dispositifs numériques nécessite aussi de s'assurer de leur contrôle grâce au droit et se mettre à l'abri de lois extraterritoriales, comme le Cloud Act américain. Elle est aussi associée à des enjeux géopolitiques[156], de défense nationale, puisqu'il est question de défendre son territoire numérique face à des ingérences étrangères[157]. Pour certains chercheurs, la notion de souveraineté numérique devrait être analysé comme une représentation , portée par différents acteurs, qui dépend du contexte et sert un objectif politique. Ainsi, le sens donné au terme de « souveraineté » diffère grandement selon qu'elle est envisagée selon les prismes nationaux, et varie selon qu'il s'agit d'une doctrine française, européenne, ou russe ou chinoise[158], la volonté de souveraineté pouvant aller jusqu'à entrainer une possible fragmentation de l'espace numérique ( ou une balkanisation de ce dernier)[159]. Enfin, la possibilité de retrouver une totale maitrise d'un espace numérique circonscrit est discutée. Pour certains chercheurs, il ne serait plus question de souveraineté pleine et entière, mais de souveraineté « plurielle » et « partagée »[160].

## Souveraineté étatique et espace humanitaire numérique

Or la notion de souveraineté renvoie dans le secteur de la solidarité internationale à une série d'enjeux bien spécifiques. Disons pour commencer que le rapport des humanitaires aux souverainetés étatiques est complexe. Dans un bon nombre de cas, l'action humanitaire se fait actuellement en coopération avec les États et avec leur accord. Mais le sans-frontiérisme historique de MSF ou d'autres ONG repose sur le contournement de ces dernières[161]. Et dans des États dits « failli », « fragiles » ou « défaillant », l'action des ONG aboutirait à se « subsidier » aux fonctions de protection des populations, aux gouvernements locaux. L'action l'action des ONG pourrait dans certains cas aboutir à la constitution d'espaces extraterritoriaux et d'enclaves fragilisant les souverainetés étatiques[162]. De surcroit, cette question est devenue brulante avec l'émergence d'un « devoir de protéger « et d'un « droit

---

[156] DOUZET, Frédérick, « La géopolitique pour comprendre le cyberespace », *Hérodote*, 2014/1-2 (n° 152-153), p. 3-21. https://www.cairn.info/revue-herodote-2014-1-page-3.htm
Dès 1997 la chercheuse Frédérick Douzet écrivait que « Le réseau [Internet] est lui-même l'enjeu de nombreux conflits géopolitiques qui donnent lieu à des stratégies de domination de la part des nations aux intérêts divergents qui cherchent à en contrôler le contenu, le fonctionnement et le développement économique. Il est une arme hautement stratégique pour la sécurité des nations [...] et surtout un instrument extrêmement puissant dans les rivalités de pouvoir entre groupes, minorités, forces politiques, religieuses, économiques, au niveau local comme au niveau mondial. » DOUZET, F. « Internet géopolise le monde », *Hérodote,* n°86-87, 1997, p.222-223

[157] *La souveraineté numérique : dix ans de débats, et après ?*, Annales des mines, n°23, septembre 2023 https://www.annales.org/enjeux-numeriques/2023/en-23-09-23.pdf

[158] GLASZE, G., CATTARUZZA, A., DOUZET, F., DAMMANN, F., BERTRAN, M. G., BOMONT, C., ZANIN, C., "Contested Spatialities of Digital Sovereignty", *Geopolitics*, *28*(2), 2022, p. 919–958. https://doi.org/10.1080/14650045.2022.2050070

[159] CATTARUZZA, Amaël, DANET, Didier, DOUZET, Frédérick, DESFORGES, Alix, LIMONIER, Kevin, et al.. La balkanisation du web : Chance ou risque pour l'Europe? . [Rapport de recherche] Ministère de la défense, 2015

[160] LEMAIRE, Félicien, « propos sur la notion de « souveraineté partagée » ou sur l'apparence de remise en cause du paradigme de la souveraineté », Presses Universitaires de France, *Revue française de droit constitutionnel,* 2012/4 n° 92 p. 821-850

[161] BRAUMAN, Rony, « Sans frontières, mais pas sans passeports », Crash, 20/07/2010 https://msf-crash.org/fr/publications/acteurs-et-pratiques-humanitaires/sans-frontieres-mais-pas-sans-passeports

[162] PANDOLFI, Mariella, CORBET, Alice, « De l'humanitaire imparfait », *Ethnologie française*, 2011/3 (Vol. 41), p. 465-472. https://www.cairn.info/revue-ethnologie-francaise-2011-3-page-465.htm
BACZKO, Adam, DORRONSORO, Gilles, « La souveraineté fragmentée. Intervention internationale et guerre civile en Afghanistan après 2001 », *Sociétés politiques comparées*, n° 50, 2020

d'ingérence » à la fin des années 1990. C'est sous la double impulsion du juriste Mario Bettati et de Bernard Kouchner [163]que s'est cristallisé le droit d'ingérence au sein d'organes onusiens. Il se résume à la reconnaissance de la légitimité d'une intervention au sein d'un État en crise manquant à l'obligation de protection de sa population, d'où la conduite de « guerres humanitaires », principalement à partir du conflit ayant frappé l'ex-Yougoslavie[164]. Les acteurs de la solidarité internationale complémentent alors l'action des militaires, d'où un risque d'une instrumentalisation de l'aide et de perte d'indépendance de cette dernière[165] ainsi qu'un risque de perte d'intégrité de l'espace humanitaire. Pour rappel, Rony Brauman décrit ainsi l'espace humanitaire comme suit : il s'agit d'« *un espace symbolique, hors duquel l'action humanitaire se trouve détachée [de son] fondement éthique et qui se constitue à l'intérieur des repères suivants : accès, dialogue, indépendance, impartialité. «* Protéger ce dernier est essentiel pour les humanitaires afin d'assurer la continuité de l'aide. Or son intégrité serait mise en cause. Et à la fin des années 2000, l'OCHA a alerté sur son rétrécissement. L'organisation met en avant la « confusion des rôles entre organisations militaires et humanitaires [de] la manipulation politique de l'assistance humanitaire [et de] la perception du manque d'indépendance des acteurs humanitaires à l'égard des bailleurs de fonds ou des gouvernements hôtes. »[166] Ce resserrement de l'espace humanitaire est la résultante de différents facteurs. Comme on l'a indiqué, entrent en jeu les risques d'instrumentalisation de l'aide propre aux guerres humanitaires. Mais il faut prendre aussi en compte différents facteurs de difficultés d'accès au terrain, qui sont aussi liées à la multiplication d'attaques sur les humanitaires, directement ciblés, pour le coup par des acteurs non étatiques, parfois des groupes armés. Les difficultés d'accès au terrain peuvent en outre découler de blocages politiques. Cela est clairement le cas à Gaza[167]. Le resserrement de l'espace humanitaire résulte aussi de la volonté par un gouvernement de maintenir un plus grand contrôle de cette

---

[163] BETTATI, Mario, *Le Droit d'ingérence. Mutation de l'ordre international*, Paris*:* Odile Jacob, « Hors collection », 1996, 384 p.

[164] ANDERSSON, Nils, « Le «droit d'ingérence humanitaire», concept de paix ou instrument de guerre », *Recherches Internationales*, n°113, 2019, p. 89-102.

[165] BRAUMAN, Rony, « l'ingérence humanitaire ou le droit du plus fort », *Crash,* 30/06/2015 https://msf-crash.org/fr/publications/acteurs-et-pratiques-humanitaires/lingerence-humanitaire-ou-le-droit-du-plus-fort

WEISSMAN, Fabrice, « Responsabilité de protéger » : le retour à la tradition impériale de l'humanitaire », *Grotius,* 31/08/2010https://grotius.fr/responsabilite-de-proteger-le-retour-a-la-tradition-imperiale-de-l%E2%80%99humanitaire/

« Parce qu'elle lève certains des obstacles qui restreignaient les ambitions onusiennes, la fin de la guerre froide entraîne alors une impressionnante multiplication d'opérations de paix qui, dans un premier temps, laissent espérer la construction d'un nouvel ordre mondial. Avec la chute du Mur puis la désintégration de la Yougoslavie, les Européens, notamment, voient exploser le système de sécurité collective qui reposait sur le principe du respect des souverainetés nationales depuis le traité de Westphalie de 1648. Les changements en cours ouvrent la voie à des interventions "militaro- humanitaires" en Bosnie puis au Kosovo. L'Amérique latine est également concernée quand l'ONU y accompagne les processus de transition démocratique qui entérinent des accords de paix et mettent fin à l'ère des dictatures militaires. En 1991, note Ted Van Baarda, la mission d'observation des Nations Unies au Salvador est par exemple la première à se doter d'un département des droits de l'homme, une pratique aujourd'hui courante. L'Afrique subsaharienne, quant à elle, constitue un champ d'expérimentation novateur. À défaut d'intervenir pour rétablir l'ordre constitutionnel après un coup d'État au Burundi ou l'annulation d'élections par les militaires au Nigeria en 1993, les casques bleus s'y déploient dans des États "neufs", comme en Namibie dès 1990, ou "faillis", comme en Somalie en 1992. »

PEROUSE DE MONTCLOS, Marc Antoine, *Les humanitaires dans la guerre*, Paris: La documentation française, 2012,p.151 https://horizon.documentation.ird.fr/exl-doc/pleins_textes/2022-08/010058366.pdf

[166]"Analysis : humanitarian action under siege", *The New humanitarian*, 18/08/2009 https://reliefweb.int/report/afghanistan/analysis-humanitarian-action-under-siege

MAHE, Anne-Hélène, «Accès humanitaire": une campagne lancée par le CICR contre la réduction de l'espace humanitaire en Afrique »,blog CICR, 06/10/2022, https://blogs.icrc.org/hdtse/2022/10/06/le-cicr-lance-une-campagne-pour-sensibiliser-au-manque-d-acces-humanitaire/

[167]« L'OMS appelle à la protection de l'espace humanitaire à Gaza à la suite d'incidents graves survenus lors d'une mission à haut risque de transfert de patients et de livraison de fournitures médicales », OMS, 12/12/2023 https://www.who.int/fr/news/item/12-12-2023-who-calls-for-protection-of-humanitarian-space-in-gaza-following-serious-incidents-in-high-risk-mission-to-transfer-patients--deliver-health-supplies

HASTING, Lynn, "Statement of the humanitarian coordinator for the occupied palestinian territory",OCHA, 04/12/2023https://www.unocha.org/publications/report/occupied-palestinian-territory/statement-humanitarian-coordinator-occupied-palestinian-territory-lynn-hastings-4-december-2023

dernière[168]. Certains États peuvent vouloir également s'opposer à l'intervention d'ONG, pour des raisons de souveraineté, comme cela a été le cas au Maroc[169]. En réaction, cela peut conduire les ONG à renouer avec des pratiques de sans-frontiérisme, comme le note Philippe Ryffman pour la Syrie[170]. Ajoutons que, plus généralement, le contrôle des ONG se fait aussi en amont. C'est le cas des mesures de contre-terrorisme qui peuvent aller de pair avec un contrôle des financements d'ONG par les bailleurs[171]. On peut mentionner aussi le fait que les atteintes aux libertés associatives se multiplient dans un nombre croissant d'États, et également dans des régimes considérés comme démocratiques[172].

Nous devons à ce stade faire une précision importante : le rétrécissement de l'espace humanitaire n'est pas simplement lié aux États. Du fait de la complexification des crises et du nombre d'acteurs pouvant y intervenir, les ONG doivent interagir avec un nombre croissant d'entités étatiques, acteurs gouvernementaux divers et militaires, d'acteurs privés et de groupes armés non étatiques, etc. Initialement, nous avions décidé de nous focaliser sur les répercussions de l'exercice de leur souveraineté sur la préservation de l'espace humanitaire. Cependant, nous devons bien garder à l'esprit le fait que les frontières entre acteurs étatiques et non étatiques peuvent se brouiller. C'est particulièrement le cas du cyberespace. En effet que les cyberopérations peuvent impliquer des groupes d'acteurs dont les liens avec les États sont fluctuants[173].

Toujours est-il que l'ampleur du resserrement de l'espace humanitaire est discutée. Des membres de MSF ont pu au début des années 2010 être critiques sur ce point. L'augmentation du nombre d'attaques contre des humanitaires serait à re-contextualiser en fonction de

[168] « Avec une vigueur croissante depuis la fin des années 1990, MSF dénonce également les effets délétères d'une "confusion des genres" accentuée par le regain d'interventionnisme militaire post -11 Septembre, le développement de la justice pénale internationale et l'assujettissement des opérations de secours aux stratégies politiques de gestion de crise des Nations unies. Assimilées aux formes militaires, judiciaires et politiques de l'interventionnisme libéral, les ONG seraient en butte à une montée générale de l'hostilité envers les organismes d'aide dans les pays du Sud. Elles feraient face à une réaffirmation de souveraineté des États postcoloniaux bénéficiant du soutien diplomatique et économique de puissances émergentes. » MAGONE, Claire, NEUMAN, Michael, WEISSMAN, Fabrice (dir.) , *Agir à tout prix? Négociation humanitaire : l'expérience de MSF*, Paris : la Découverte, 256 p.

[169] BOBIN, Frédéric, « Le Maroc affiche sa "souveraineté" dans la sélection de l'aide internationale aux victimes du séisme », *Le Monde Afrique,* 15/09/2023 https://www.lemonde.fr/afrique/article/2023/09/15/le-maroc-affiche-sa-souverainete-dans-la-selection-de-l-aide-internationale-aux-victimes-du-seisme_6189466_3212.html

[170]« Aussi bien ces ONG – a fortiori le Mouvement Croix-Rouge ou les agences des Nations unies – ne sont intervenues que dans le cadre d'accords minimaux, et parfois très détaillés, avec des États, des administrations ou des groupes armés : il n'était donc plus question de sans-frontiérisme. Or on constate aujourd'hui que des organisations humanitaires renouent dans une certaine mesure – et c'est notamment le cas de la Syrie que vous évoquiez – avec des pratiques de franchissement de frontières qu'on n'a pas connues depuis très longtemps. Par ailleurs, et je rejoins Boris Michel, les premiers à créer des difficultés d'accès, ce sont les États. C'est particulièrement vrai en Syrie où l'État entend instrumentaliser et contrôler de façon très étroite l'aide humanitaire sur le territoire où il exerce encore son autorité. » PERRIN, Jean-Pierre**,** ABU-SADA, Caroline, OBERREIT, Stephan**,**POTIER, Gilbert, MICHEL, Boris**,** RYFMAN, Philippe, « Les nouvelles frontières de l'humanitaire », *Humanitaire*, 34 | 2013

[171]MCLEAN, Duncan, « Les conséquences humanitaires d'une réaffirmation de la souveraineté de l'État », *Alternatives humanitaires,* n°9, 2018 https://alternatives-humanitaires.org/fr/2018/11/13/les-consequences-humanitaires-dune-reaffirmation-de-la-souverainete-de-letat/

[172]RYFMAN, Philippe, « Extension de la "contre-révolution anti-associative" : diagnostic, enjeux, solutions », *Alternatives humanitaires*, n°20, 2022 https://www.alternatives-humanitaires.org/fr/2022/08/17/extension-de-la-contre-revolution-anti-associative-diagnostic-enjeux-solutions/

PRADIER, Vincent, GRISARD, Roxane, « Le soutien sous contrôle des acteurs de la société civile : le cas des organisations de solidarité internationale françaises et européennes », *Alternatives humanitaires*, n°20, 2022
https://www.alternatives-humanitaires.org/fr/2022/08/16/le-soutien-sous-controle-des-acteurs-de-la-societe-civile-le-cas-des-organisations-de-solidarite-internationale-francaises-et-europeennes/

[173] EGLOFF, Florian, *Semi-sate actors in cybersecurity*, Oxford University press, 2022, 305 p.

l'évolution des formes d'interventions humanitaires [174]. Et au sein de MSF est défendue l'idée qu'il existe toujours une marge de négociation pour permettre un accès au terrain et une aide respectueuse des principes éthiques humanitaires[175]… ainsi que de la souveraineté des États. Et bien sûr, on peut quant à nous se demander si cette marge de négociation existe aussi sur le plan numérique.

L'objet de nos recherches est justement de comprendre comment ces enjeux de souverainetés et d'espace humanitaire se traduisent sur le plan informationnel et numérique. Trois points sont à retenir : les demandes de partage des données que détiennent des ONG par les États ; les formes de surveillance menées dans le cadre de politiques de contre-terrorisme, ou de « cyberopérations ». Et donc une première modalité d'expression des souverainetés étatiques est la volonté de contrôler sa population, son territoire, ainsi que les acteurs y transitant. Pour ce faire, les États tentent de garder la main sur des flux informationnels transitant sur leur territoire. Ce point nous fait d'ailleurs penser aux réflexions d'un sociologue comme Antoine de Rosière ou d'un anthropologue comme James Scott[176]. À leurs yeux, les statistiques constituent pour les États des outils de gouvernance des populations. Dans notre troisième chapitre, on tentera donc de déterminer quel peut être l'intérêt à contrôler ces données pour les États où les ONG opèrent. Il faudra aussi déterminer dans quels cas le partage de données avec des États est perçu comme un risque pour les bénéficiaires en matière de vie privée. Et dans ce cas, comment les ONG y font-elles face ? On verra qu'échanger ou non des données peut faire l'objet de négociations. La marge de manœuvre dont disposent les ONG dépend d'une série de facteurs, comme le statut juridique d'une organisation, de ses liens avec les États, etc. Cela est flagrant pour les organisations internationales comme l'UNHCR ou le CICR qui jouissent de privilèges et immunités. Ces derniers leur permettent de s'opposer aux demandes de données des États. Leur application permettrait en effet la constitution de ce que le délégué à la protection des données du CICR Massimo Marelli qualifie d'« espace humanitaire numérique »[177]. Par voie de conséquence, sa

---

[174]« Reprise par des chercheurs comme Sami Makki, la vulgate des organisations de secours table cependant sur une "multiplication des crises et des situations d'urgence depuis la fin de la guerre froide". De façon prospective, John Borton fait par exemple l'hypothèse d'un rétrécissement de l'espace humanitaire et d'une prolifération de guerres plus meurtrières. De telles analyses ne veulent ainsi pas voir qu'en réalité, ce sont les opérations de secours qui se sont multipliées, plus que les catastrophes. Concernant plus spécifiquement les conflits armés, elles vont encore plus loin, estimant que les guerres auraient fondamentalement changé de nature et seraient donc plus dangereuses pour les volontaires des ONG. » PEROUSE DE MONTCLOS, Marc Antoine, *Les humanitaires dans la guerre*, Paris : La documentation française, 2012, p.130-131 https://horizon.documentation.ird.fr/exl-doc/pleins_textes/2022-08/010058366.pdf

[175]« Contrairement à l'idée véhiculée par le discours victimaire du "rétrécissement de l'espace", qui exonère les acteurs de secours de toute responsabilité dans la conquête et la défense de leur espace de travail, il n'y a pas de périmètre d'action légitime de l'humanitaire, valable en tout temps et en tout lieu, dont la reconnaissance irait de soi une fois le brouillard de la "confusion militaro-humanitaire" dissipé et les humanitaires protégés de toute contamination politique. Il y a en revanche un espace de négociation, de rapports de forces et d'intérêts entre acteurs de l'aide et autorités. La liberté d'action de MSF ne repose pas sur un espace de souveraineté juridico-moral dont il conviendrait de proclamer l'existence pour obtenir sa reconnaissance. Elle est le produit d'un processus de transactions permanent avec les forces politiques et militaires locales et internationales. Son étendue dépend notamment des ambitions de l'association et de sa façon de les justifier, des soutiens diplomatiques et politiques dont elle dispose et de l'intérêt des pouvoirs pour son action. » MAGONE, Claire, NEUMAN, Michael, WEISSMAN, Fabrice (dir.), *Agir à tout prix, négociation humanitaire l'expérience de MSF*, Paris : La Découverte, 2011,256 p.
«Mythes et mystères de l'espace humanitaire», *The New Humanitarian*, 02/05/2012, https://www.thenewhumanitarian.org/fr/actualites/2012/05/02/mythes-et-mysteres-de-l-espace-humanitaire

[176] DESROSIERES, Alain, *La politique des grands nombres, histoire de la raison statistique*, Paris: la Découverte, 2010, 462 p.
SCOTT, James, *L'oeil de l'Etat, moderniser, uniformiser, détruire*, Paris : La Découverte,2021 546 p.

[177]MARTIN, A., SHARMA, G., PETER DE SOUZA, S., TAYLOR, L., VAN EERD, B., MCDONALD, S. M., MARELLI, M., CHEESMAN, M., DIJSTELBLOEM, H., "Digitisation and Sovereignty in Humanitarian Space: Technologies, Territories and Tensions", *Geopolitics*, *28*(3), 2022, p.1362–1397. https://doi.org/10.1080/14650045.2022.204746
MARELLI, Massimo, "Hacking Humanitarians: Defining the Cyber Perimeter and Developing a Cyber Security Strategy for International Humanitarian Organizations in Digital Transformation", *International Review of the Red Cross*, 102 (913), 2020, p.367–387, https://ssrn.com/abstract=3969883

version « virtuelle » permettrait de se prémunir de pressions ou de demandes de données à risque en vertu du principe d'indépendance ainsi que des privilèges et immunités du CICR. Or leur application dans le milieu numérique n'est pas sans difficulté. Pour ce faire, le CICR envisage par exemple de constituer une sorte d'« ambassade numérique » qui serait une forme possible d'espace numérique humanitaire. Cette dernière repose sur les privilèges et immunités accordés au CICR. Mais si ce statut d'exception est discuté, puisqu'il implique de ne pas appliquer le RGPD, pourquoi permettrait-il, pour les juristes de l'organisation, de garantir la confidentialité de l'organisation ? Et quelles difficultés l'organisation rencontre-t-elle dans l'application de ces derniers à l'espace numérique ?

Évoquons maintenant notre deuxième point. On ne doit pas oublier que traditionnellement, il existerait un lien consubstantiel entre souveraineté et guerre. Selon une définition wébérienne de l'État[178], ce dernier serait le seul acteur légitime pouvant employer la violence guerrière pour contraindre d'autres acteurs, dont les États attaquant son territoire. L'acte guerrier serait même constitutif de l'État et renforcerait ce dernier. « War makes states », écrivait ainsi le politiste Charles Tilly[179]. Or ce monopole est contesté du fait de la multiplication de conflits intraétatiques et l'implication d'acteurs privés dans la conduite de la guerre. Certains chercheurs vont jusqu'à parler d'une relative privatisation du fait guerrier[180]. Ce phénomène a également ses facettes digitales. Le processus de numérisation de nos sociétés accompagne et renforce aussi la recomposition des souverainetés, notamment parce qu'il permet l'entrée en scène d'une série d'acteurs non étatiques, des entreprises évidemment, comme les GAFAM, mais aussi d'autres groupes plus informels, comme des hackers. L'implication de cybercombattants dans des conflits contemporains s'inscrit donc dans un long mouvement de contestation du monopole de la violence des États du fait de la multiplication de conflits intraétatiques, et l'implication de groupes armés non étatiques, pouvant être qualifiés pour certains de terroristes, d'où une réaffirmation des souverainetés des Etats par la « guerre contre le terreur »[181].

---

[178] LINHARDT, Dominique, « Le concept de monopole de la violence légitime dans l'œuvre de Max Weber :Une approche de sociologie de la connaissance. Penser les sociétés et les pouvoirs avec Max Weber »,Centre culturel international de Cerisy, Sep 2022, Cerisy-la-Salle, France.

[179] TILLY C., " War Making and State Making as Organized Crime", In: EVANS PB, RUESCHEMEYER D, SKOCPOL T, (eds.), *Bringing the State Back In*. Cambridge University Press, 1985, p.169-191.

[180] BANEGAS, Richard, « De la privatisation de la guerre à la privatisation du peacekeeping ?, Actes du colloque, *Le boom du mercenariat : défi ou fatalité ?*, Novembre 2000, Lyon, France. p.18 - 21.

MAGNON-PUJO, Cyril, « La souveraineté est-elle privatisable ? La régulation des compagnies de sécurité privée comme renégociation des frontières de l'État », *Politix*, 2011/3 (n° 95), p. 129-153. https://www.cairn.info/revue-politix-2011-3-page-129.htm

MAKKI, Sami. « Privatisation de La Sécurité et Transformation de La Guerre. » *Politique Étrangère*, vol. 69, no. 4, 2004, p. 849–61.

Colloque guerre et souveraineté : revisiter un débat canonique en science sociales par l'interdisciplinarité », Programmes war Studies et Chaire grands enjeux stratégiques de l'Université Paris 1 Panthéon-Sorbonne, 7 et 8 juin 2022https://www.youtube.com/watch?v=kAil9FLbhAQ&list=PL0lIMNx8BqSllvaG7g8pHS3arKpCnHwsz&index=1

HASSNER, Pierre, MARCHAL, Roland, *Guerres et sociétés : État et violence après la Guerre froide*, Paris : Karthala éditions, 2003, 616 p.

Cette privatisation vaut aussi pour le volet « cyber » des conflits : « La privatisation de la sécurité nationale représente une évolution manifeste de cette guerre : Microsoft ou Amazon, pour ne parler que d'eux, sont intégrés dans les dispositifs de défense. Ces acteurs ont l'occasion de montrer leur responsabilité au cours d'un conflit armé, mais les implications en termes de souveraineté sont abyssales. » POUPARD Guillaume, « La privatisation de la sécurité nationale, une donnée majeure du volet cyber de la guerre en Ukraine : entretien avec Guillaume Poupard », *Études françaises de renseignement et de cyber*, 2023/1 (N° 1), p. 177-181. https://www.cairn.info/revue-etudes-francaises-de-renseignement-et-de-cyber-2023-1-page-177.htm

[181] BONDITTI Philippe, « (Anti) terrorisme. Mutations des appareils de sécurité et figure de l'ennemi aux États-Unis depuis 1945 », *Critique internationale*, 2013/4 (N° 61), p. 147-168. https://www.cairn.info/revue-critique-internationale-2013-4-page-147.htm

Or cette dernière a eu de nombreuses répercussions sur l'action humanitaire[182]. Il existe en effet une volonté de contrôle des ONG en vertu d'un lien supposé avec des groupes non armés pouvant être qualifiés de terroristes. Les formes de surveillances (numériques ou non) liées à la guerre contre le terrorisme ont été très discutée, voire critiquée en raison des inquiétudes qu'elle soulève en matière de vie privée. On se concentrera pour notre part dans notre cinquième chapitre sur le sujet du contrôle du financement des ONG. On verra que les bailleurs de fonds imposent des opérations de criblage aux personnels d'ONG, voire dans certains cas aux bénéficiaires, afin de vérifier qu'ils ne se trouvent pas sur des listes de terroristes constituées par les États et des organismes onusiens. Les banques conditionnent la gestion de fonds à l'identification de leurs clients, afin de s'assurer qu'ils ne sont pas associés à des organisations criminelles. Et ces institutions traitent, grâce à différents logiciels, dans le cadre de leur obligation de « vigilance raisonnable », une quantité toujours accrue d'informations. Ces opérations touchent particulièrement les programmes de transferts monétaires menés par les ONG humanitaires, ces derniers tendant à être de plus en plus numérisés, d'où des problématiques spécifiques en matière de protection des données. En effet, si les ONG dénoncent les conséquences des sanctions en matière de violation du droit international humanitaire (DIH), et si les ONG tentent de négocier un statut d'exception à leur égard, les différentes mesures de contrôle du financement du terrorisme soulèvent aussi un bon nombre d'enjeux relatifs à la protection de la vie privée des bénéficiaires.

Ensuite, si les ONG clament qu'elles ne sont pas des cibles (« not a target »), et plaident pour un arrêt des enlèvements d'humanitaires et des bombardements d'hôpitaux, ce slogan est maintenant décliné dans une version « modernisée » : les ONG ne sont pas des cibles numériques (« not a digital target »). Ce slogan constitue un appel à stopper les cyberopérations contre les ONG, qui sont largement victimes des affrontements entre Etats agitant l'espace numérique, pouvant être ou non, cela fait l'objet de discussions, être qualifié de cyberconflits[183]. Il existe encore peu de littérature sur les répercussions de ces formes de conflictualités sur la société civile[184], et donc sur les humanitaires[185].

---

[182] LENFANT, François, VAN BROEKHOVEN, Lia, VAN LIERDE, Frank, « Les conséquences de la guerre contre le terrorisme sur le monde des ONG », *Cultures & Conflits*, 76 | hiver 2009,
OPHIR, Adi, « le souverain, l'humanitaire et le terroriste », *Vacarme*, 2006/1 (n° 34), p. 20-25. https://www.cairn.info/revue-vacarme-2006-1-page-20.htm
WEISSMAN, Fabrice, « La criminalisation de l'ennemi et son impact sur l'action humanitaire », MSF crash, 20/12/2010
PEROUSE DE MONTCLOS Marc-Antoine, « Aide internationale et "guerre globale contre le terrorisme" en Afrique. Des défis renouvelés », *Revue internationale des études du développement*, 2020/1 (N° 241), p. 41-63. https://www.cairn.info/revue-internationale-des-etudes-du-developpement-2020-1-page-41.htm
PANTALIANO, Sara, MACKINTHOSH, Kate, ELHAWARY, Samir, METCALFE, Vitoria, "Counter terrorism and humanitarian action, tensions, impact and ways forward", HPG politic, october 2011
DE TORRENTE, Nicolas, "The war on Terror's challenges to humanitarian action", MSF, Septembre 2002 https://www.msf.fr/sites/default/files/2002-09-19-Torrente.pdf
ANTOULY, Julien, "Quels sont les effets de la lutte contre le terrorisme sur l'action humanitaire", *Alternative humanitaire*, n°18, 2021 https://www.alternatives-humanitaires.org/fr/2021/11/12/quels-sont-les-effets-de-la-lutte-contre-le-terrorisme-sur-laction-humanitaire/
[183] NOCETTI, Julien, « Géopolitique de la cyber-conflictualité », *Politique étrangère*, 2018/2 (Été), p. 15-27. https://www.cairn.info/revue-politique-etrangere-2018-2-page-15.htm
DOUZET, Frédérick, GERY, Aude, « Le cyberspace, ça sert, d'abord, à faire la guerre. Prolifération, sécurité et stabilité du cyberespace », *Hérodote*, 2020/2, n° 177-178,p. 329-350
TAILLAT Stéphane, « La conflictualité numérique et la conflictualité internationale », dans : TAILLAT, Stéphane, CATTARUZZA, Amael, DANET, Didier, (éd.), *La Cyberdéfense. Politique de l'espace numérique.* Paris, Armand Colin, « Collection U », 2023, p. 43-56.
[184]HANSEN, Lene, NISSEMBAUM, Helen, "Digital Disaster, Cyber-Security, and the Copenhagen School," *International Studies Quarterly* 53, no. 4, 2009, p. 1155-75
[185] DUNN CAVELTY, Myriam, EGLOFF, Florian, "The politics of cybersecurity : balancing different roles of the state", *St Antony's International Review* 15 no. 1 2019, p. 37-57.

Pour résumer, on s'intéresse donc aux conséquences informationnelles du resserrement de l'espace humanitaire, ainsi qu'à leurs répercussions en matière de vie privée. Par voie de conséquence, si les ONG tentent bien de préserver l'espace humanitaire physique, on peut se demander en toute logique comment les ONG s'efforcent ou non de protéger ce qui pourrait être sa version numérique. Sachant que l'objectif premier de la préservation de l'espace humanitaire est la continuité de l'aide, et le fait de pouvoir avoir accès au terrain. Certaines définitions de l'espace humanitaires mettent de surcroit l'accent sur la protection des bénéficiaires[186]. On peut ainsi citer celle d'Oxfam : « un environnement opérationnel dans lequel le droit des populations à bénéficier d'une protection et d'une assistance est respecté et où les agences d'aide peuvent mener une action humanitaire efficace en répondant à leurs besoins de manière impartiale et indépendante. »[187] Par conséquent, le rétrécissement de l'espace humanitaire irait de pair avec une augmentation de risques pour les civils. Théoriquement, il revient à l'État de garantir leur protection, en temps de paix, comme de conflits[188]. Or, les États peuvent faillir à ces obligations et ne pas porter secours à leurs ressortissants en cas de crise. Tout d'abord parce qu'ils n'en ont plus les capacités. Et cela implique que les ONG appuient l'action de protection des États, la complémentent ou s'y substituent[189]. Ajoutons que malgré leur obligation de protection, les États peuvent aussi être un facteur de risque pour les populations. C'est le cas lorsque des conflits interétatiques ou intraétatiques ont des répercussions sur des civils[190]. Cela peut conduire pour l'État à enfreindre le DIH. Et dans ce cas, on peut parler de « violence d'État ». Cette dernière adopte

---

[186]« In a way, every humanitarian crisis has protection implications. Consequently, all humanitarian actors must take this into account in their activities. These concerns are reflected, for example, in principles such as 'do no harm' or 'mainstreaming protection'. It is up to protection actors to encourage and guide discussions with specialists in other fields on these different concerns, and to propose measures to reduce protection risks. »« D'une certaine façon, toute crise humanitaire a des implications sur le plan de la protection. Par conséquent, tous les acteurs humanitaires doivent en tenir compte dans leurs activités. Ces préoccupations se reflètent par exemple dans des principes tels que « do no harm » (ne pas nuire) ou « mainstreaming protection » (intégrer transversalement les préoccupations de protection dans toutes les activités Il appartient aux acteurs de la protection d'encourager et d'orienter les débats avec les spécialistes d'autres domaines d'action sur ces différentes préoccupations, et de leur proposer des mesures pour réduire les risques sur le plan de la protection. » BRADLEY, M., "All Lives Are Equal but Some Lives Are More Equal than Others: Staff Security and Civilian Protection in the Humanitarian Sector", *Journal of Humanitarian Affairs*, 2019, *1*(2), p.13-22. https://doi.org/10.7227/JHA.013

[187]« an operating environment in which the right of populations to receive protection and assistance is upheld, and aid agencies can carry out effective humanitarian action by responding to their needs in an impartial and independent way." "OI Policy Compendium Note on United Nations Integrated Missions and Humanitarian Assistance", Oxfam, January 2008https://www-cdn.oxfam.org/s3fs-public/file_attachments/story/oi_hum_policy_integrated_missions_0_1.pdf

COLLINSON, Sarah, ELHAWARY, Samir, "Humanitarian space: a review of trends and issues", *ODI HPG Report* 32, April 2012 http://cdn-odi-production.s3.amazonaws.com/media/documents/7643.pdf

[188] SASSOLI, Marco, "State responsibility for violations of international humanitarian law", *IRRC*, June 2002, vol.84, n°846https://www.icrc.org/en/doc/assets/files/other/401_434_sassoli.pdf

[189] « Idéalement, les activités de substitution devraient être complétées par des mesures visant à renforcer la capacité des autorités d'assumer leurs responsabilités en matière de protection. Cela est particulièrement important lorsque les autorités ont la volonté d'agir, mais n'en ont pas les moyens. La substitution totale ne devrait être envisagée que dans des situations extrêmes. Même dans ce cas, les acteurs de la protection devraient réaliser en permanence un travail de sensibilisation et de persuasion pour encourager les autorités officielles à mieux s'acquitter de leurs obligations et de leurs responsabilités en ce qui concerne la protection des populations à risque » "Standards professionnels pour les activités de protection menées par les organisations humanitaires et de défense des droits de l'homme lors de conflits armés et d'autres situations de violence", CICR, Juin 2010 https://www.icrc.org/fr/doc/assets/files/other/icrc_001_0999.pdf

METCALFE-HOUGH, Victoria, "Influencing states' policy and practice on the protection of civilians", *HPG briefing note*, April 2022 https://apo.org.au/sites/default/files/resource-files/2022-04/apo-nid317432.pdf

O'CALLAGHAN, Sorcha, PANTULIANO, Sara, "Protective action, Incorporating civilian protection into humanitarian response", *HPG Report* 26, December 2007 https://odi.cdn.ngo/media/documents/1640.pdf

[190] CASIER, Frédéric, «La préservation d'une action humanitaire impartiale, neutre et indépendante en cas de conflit armé : l'application effective des règles du DIH et des principes humanitaires», Croix-Rouge de Belgique, 2023 https://www.croix-rouge.be/content/uploads/sites/6/2023/09/Article-sur-action-humanitaire-aout-2023-F.Casier.pdf

"Aid Operations under Increasing Threat as State, Non-State Combatants Ignore International Law, Humanitarian Affairs Chief Warns Security Council", United Nations, Meetings coverage and Press releases, SC/13760, April 2019https://press.un.org/en/2019/sc13760.doc.htm

de multiples formes. On pense aux violences policières, à la criminalisation des minorités, des réfugiés, voire à des conflits ethniques ou à des génocides[191].

Or les différentes formes de violence d'État se répercutent sur le plan numérique[192]. Et comme le remarquent les chercheurs Florian Egloff et James Shires : « La transformation et la réinvention de la violence d'État se sont poursuivies à l'ère numérique. L'élargissement du concept de violence, y compris les préjudices affectifs et communautaires, révèle comment les OCC délocalisent la violence d'État par le biais de nouveaux moyens de répression et de manipulation de l'information. »[193] Pour notre part, gardera en tête cette dimension lorsqu'on reviendra sur les échanges de données entre ONG et gouvernements, sur les différentes mesures de contre-terrorisme, ainsi que des cyberopérations impliquant des acteurs étatiques[194].

Toutefois, cette conception de la protection des données axée sur une approche par les risques suppose— dans une certaine mesure — de considérer les bénéficiaires comme des « objets de protection » et non pas des « sujets de droit ». Pourtant, le principe de « dignité » occupe une place importante dans l'architecture éthique humanitaire. Il signifie tout d'abord le fait de ne pas réduire les bénéficiaires à des victimes passives. Cela nécessite de reconnaitre la capacité d'exercice de leurs droits accordés par le RGPD, comme le droit à consentir au traitement de données, le droit d'accès, de rectification et le droit à l'oubli. Prendre en compte ces droits contribuerait à atténuer les rapports de pouvoirs et inégalités propres au technocolonialisme qu'on a évoqué précédemment. Or la notion de dignité constituera le sous-bassement théorique de la troisième et dernière partie de notre thèse. Elle portera en effet sur la possibilité pour des « indésirables » d'exercer les droits accordés par le RGPD en contexte humanitaire. On se distanciera donc des analyses strictement biopolitiques de l'humanitaire, réduisant les bénéficiaires à des « vies nues », des victimes passives dont seule la subsistance compte. Certes, les bénéficiaires restent marqués par des formes de vulnérabilité. Elles peuvent être contextuelles et être causées par les différentes crises que les

---

[191]LINHARDT, Dominique, « Un monopole sous tension : les deux visages de la violence d'État » *Politika*, 2019, ⟨10,260 95/g3js-va 66⟩. ⟨hal-02430940⟩

[192] GOHDES, Anita, *Repression in the digital age : surveillance, censorship, and the dynamics of state violence*, New York : Oxford University Press, 2024, 200p

[193]"The transformation and reinvention of state violence has continued into the digital age. expanded concept of violence, including affective and community harms, reveals how OCCs relocate state violence through new means of repression and information manipulation, without simplifying or exaggerating their complex effect." EGLOFF, Florian, SHIRES, James, « The better angels of our digital nature? Offensive cyber capabilities and state violence", *European journal of international security*, 8, 2023, p. 130-149

[194] "The impact is not limited to the delivery of assistance but extends to protection activities, especially in contexts where groups designated as 'terrorist' have significant influence. Host States and third States' governments tend to prioritize a security and law enforcement approach which has led to denying certain categories of persons protections afforded to them under international humanitarian law, human rights law or refugee law (e.g. family relations of suspected members of groups designated as 'terrorist'; persons detained on terrorism-related charges; communities in or displaced persons from areas controlled by such groups; wounded and sick combatants; etc.)"" L'impact ne se limite pas à la fourniture d'assistance mais s'étend aux activités de protection, en particulier dans les contextes où les groupes désignés comme « terroristes » ont une influence significative. Les États hôtes et les gouvernements des États tiers ont tendance à privilégier une approche sécuritaire et répressive qui a conduit à refuser à certaines catégories de personnes les protections qui leur sont accordées en vertu du droit humanitaire international, du droit des droits de l'homme ou du droit des réfugiés (par exemple, les relations familiales des membres présumés de groupes désignés comme « terroristes » ; les personnes détenues pour des motifs liés au terrorisme ; les communautés vivant dans les zones contrôlées par ces groupes ou les personnes déplacées de ces zones ; les combattants blessés et malades ; etc. » « Impact of sanctions and counterterrorism measures on humanitarian operations", *IASC*, September 2021https://interagencystandingcommittee.org/sites/default/files/migrated/2021-09/IASC%20Guidance%20to%20Humanitarian%20Coordinators%20-%20Impact%20of%20Sanctions%20and%20Counterterrorism%20Measures%20on%20Humanitarian%20Operations.pdf
DAWODY, Hevi, "Terrorism and exclusion from refugee protection" Doctoral thesis, Stockholm University, Public international law, 2024 https://su.diva-portal.org/smash/get/diva2:1841269/FULLTEXT01.pdf

bénéficiaires traversent, ou bien elles peuvent leur être assignées, et liées au fait qu'ils soient catégorisés par les ONG comme tels. Mais, les membres d'ONG s'efforcent aussi de défendre leur dignité, cette notion occupant une place majeure au sein de l'éthique humanitaire. On précisera donc ses différentes facettes, sa place au sein du système normatif humanitaire, mais aussi au sein du droit de la protection des données : garantir la dignité des personnes concernées signifie aussi s'assurer qu'elles puissent garder la maitrise de leurs données. Il existe en effet un lien profond entre cette notion et le principe d'autodétermination informationnelle ainsi que celui de consentement. Or le principe de dignité trouve ses racines dans un héritage philosophique libéral, mettant l'accent sur l'autonomie du sujet, ce qui fait qu'il existe une tension entre ce dernier et la notion de vulnérabilité. On détaillera donc dans notre thèse la façon dont les humanitaires cherchent à dépasser cette tension. Puis dans notre dernier chapitre, on s'intéressera justement à une autre façon de penser la dignité, puisqu'on abordera le travail d'acteurs impliqués dans l'identification des morts en migration. Préserver la dignité des morts, c'est alors s'assurer qu'ils bénéficient d'une « belle mort », ne dérogeant pas aux normes d'un groupe social. Cela signifie entre autre le fait de conserver son identité. Or, un bon nombre de victimes de catastrophes ou de guerre sont des morts anonymes. Et il se trouve que certaines ONG humanitaires se sont donné la difficile mission d'identifier les corps de personnes décédées. Or, on verra que ce travail d'identification s'articule à un certain nombre d'enjeux en matière de protection des données, que ce soit la protection de la vie privée des morts ou bien de celle de leurs proches

## Hypothèse et problématique

Nous avons décrit dans les lignes précédentes un ensemble de risques liés aux NTIC et découlant de dynamiques sectorielles et globales. La suite de la thèse creusera la façon dont ils se concrétisent sur le terrain pour les ONG. Nous tenterons surtout de répondre à notre question centrale. Cette dernière peut être formulée comme suit : comment les humanitaires résolvent-ils les différents dilemmes résultants de la tension entre la numérisation de l'aide, présentée parfois comme une manière d'améliorer son efficience, et le fait qu'elle mette en péril la vie privée des bénéficiaires, voire qu'elle les mette en danger ?

Notre étonnement est d'autant plus grand qu'il nous semble qu'on assisterait à une prise de conscience progressive des dérives liées au numérique humanitaire, voire que différents acteurs du secteur s'investissent dans des actions visant à atténuer ces dernières. Or ce dernier constat prend le contrepied d'une partie de la littérature critique qui axe son analyse de la numérisation de l'aide sur la notion de surveillance et sur la dialectique entre « care » et « contrôle ». On y fera largement référence, il ne s'agit pas de minimiser et de nier les formes

de dominations, voire de violences symboliques, traversant l'humanitaire. Mais un bon nombre de ce type d'approche nous semble mettre en grande partie de côté la façon dont certains humanitaires s'inquiètent des tensions propres au numérique. En effet, de prime abord, il nous semble que la protection des données a mobilisé un certain nombre d'acteurs dans l'humanitaire. Des conférences ont été organisées sur ce sujet, la vie privée a nourri des discussions au sein de forums et des arènes propres à la solidarité internationale. Dans nos entretiens, nos enquêtés ont pu nous faire part de leurs préoccupations et de leurs attachements au droit à la vie privée. Il s'agissait de délégués d'ONG, mais aussi d'autres acteurs impliqués dans le travail des données. Nous avons pu en effet interroger des « information manager officier », des ingénieurs travaillant pour des ONG, des chargés de mission opérationnels, des médecins, des médecins légistes, voire des bénévoles d'ONG. En bref, ces différents acteurs s'alarment des répercussions du numérique sur les bénéficiaires, certains d'entre eux tentent même d'agir pour les atténuer. Cela constitue certes une obligation légale, notamment liée à l'application du RGPD. Mais prendre en compte la vie privée des bénéficiaires semble également faire sens pour nos enquêtés, au-delà du fait que leurs discours et pratiques peuvent être réduits à des formes de légitimation des dérives du numérique humanitaire. Cette affirmation repose sur un certain nombre de suppositions qu'on peut détailler.

Comme on l'a dit, elle repose sur l'idée que dans l'humanitaire des acteurs n'ignorent pas des répercussions potentielles du numérique sur les bénéficiaires. Il s'agit de préciser la façon dont se manifeste cette « prise de conscience ». Le cyberespace nourrit un bon nombre de récit, dystopiques, reposant sur l'exploitation de menaces imprévisibles, peu anticipables, mais une part de nos enquêtés, notamment les DPO et/ou les ingénieurs, sont plutôt impliqués dans la constitution d'un savoir sur ces dernières, et ils tentent de mettre en place des mesures de gestion de risque[195]. Ceci nécessite d'avoir un certain degré de connaissance à la fois du droit de la protection des données et du fonctionnement technique des dispositifs numériques.

Il s'agit aussi de disposer d'outils techniques (des NTIC respectant le principe de privacy by design, des blockchains, des clouds souverains, etc.) et d'outils juridiques (des analyses d'impacts d'atteinte à la vie privée par exemple). Cela suppose aussi pour les déployer l'existence d'un certain capital en termes de ressources financières ou humaines. En fin de compte, on peut se demander dans quelle mesure il existerait une professionnalisation des acteurs se consacrant à la gestion du risque numérique et du traitement de données humanitaires.

De surcroit, si l'on part du principe qu'un des principaux outils à leur disposition est le RGPD, cela implique aussi d'accorder du crédit au fait que le Règlement puisse constituer un outil efficace de régulation du numérique. Le RGPD apporterait une réponse aux défis causés par la numérisation de nos sociétés. Et ce texte de loi pourrait répondre aux enjeux sectoriels propres à l'humanitaire. Du moins, les DPO se seraient approprié cet outil juridique pour l'acclimater aux spécificités du milieu de la solidarité internationale. Le texte de droit serait alors suffisamment flexible pour répondre aux spécificités du secteur humanitaire [196] tout en

[195] KERMISCH, Céline, *Le concept de risque : de l'épistémologie à l'éthique*, Tec&Doc Lavoisier, 2011, 96 p.
[196] CARBONIER, Jean, *Flexible droit : pour une sociologie du droit sans rigueur*, Paris : LGDJ, 2001, p.493

étant contraignant et pouvant atténuer efficacement les différents risques liés à la numérisation de l'aide.

En outre, il découle de ces dernières lignes que les risques numériques qu'on a identifiés sont problématisés, cadrés en tant qu'atteintes aux principes du droit de la protection des données. En effet, cette affirmation repose sur l'idée qu'un fait social lorsqu'il acquiert une certaine « existence » pour des acteurs fait l'objet de formulation, de traduction, ou de « transcodage » pour reprendre le terme de Pierre Lascoumes. Ce dernier désigne différentes opérations, à savoir l'insertion d'enjeux émergents (les risques numériques par exemple), dans des systèmes d'action, mais aussi le recyclage d'idées et de pratiques antérieures en des formes neuves qui constituent des contenants pour la réception. Par exemple, la formule « do no digital harm » « recycle le principe humanitaire « ne pas nuire » dans une version faisant sens dans un espace numérique.

Par conséquent, on abordera un bon nombre de textes de droit, qu'il soit question de droit dur ou souple, mais on n'adoptera pas une approche strictement juridique. En effet, on évoquera différentes difficultés liées à la mise en œuvre du RGPD, mais on s'intéressera aussi à la manière dont le droit à la protection des données est relié, ou non, à un système de représentations. Pour les différents acteurs impliqués dans la gestion des données, il ne s'agit pas que d'opérations techniques. Collecter ou traiter des données implique le fait de se représenter la manière dont ces opérations touchent les bénéficiaires, la façon dont des traitements de données sont producteurs d'inégalités et de risques. En somme, au-delà de l'obligation juridique, nous nous intéresserons à une série de normes et de valeurs de ce qui est juste ou non, sûr ou non, légitime ou non de faire avec des données[197].

Donc nous avons donné un aperçu très surplombant et théorique des risques numériques, en les reliant à des dynamiques bien spécifiques. Or il est aussi important de comprendre comment des acteurs les perçoivent et les formulent, quels sont les discours à leur sujet, quelles en sont leurs représentations.

Pour commencer, on peut supposer que cette prise de conscience des risques numériques contribue à transformer la façon dont les humanitaires se représentent des outils techniques, et qu'ils se distancient d'une conception instrumentale de la technologie. Du moins, il s'agirait de ne plus considérer le numérique comme un outil neutre pouvant servir une finalité propre, visant à « améliorer » l'aide. Cela suppose de nuancer la définition que donne Patrick Vink du numérique humanitaire, qu'il décrit comme « l'utilisation de la technologie pour *améliorer* la qualité des efforts de prévention, d'atténuation, de préparation, de réaction, de récupération et de reconstruction. »[198] Cela implique de nuancer l'idée que le secteur humanitaire serait strictement technosolutionniste ou, pour reprendre ce terme, technophile. Il serait plus pluriel et il existerait un certain nombre de tensions entre des acteurs liés à des espaces d'innovations et des acteurs ayant un positionnement plus distancé, comme les délégués à la protection des

[197] TAYLOR, L.,"What is data justice? The case for connecting digital rights and freedoms globally", 2017, *Big Data & Society*, *4*(2). https://doi.org/10.1177/2053951717736335

[198] « the use of technology to improve the quality of prevention, mitigation, preparedness, response, recovery and rebuilding efforts", VINCK Patrick, "Humanitarian Technology, World Disasters Report", *International Federation of Red Cross and Red Crescent Societies*, 2013, www.ifrc.org/PageFiles/134658/WDR%202013%20complete.
pdf

données. Mais on ne se limitera pas à ces derniers, comme on le verra. Cela suppose aussi qu'on mette l'accent sur des tensions entre des acteurs, pouvant critiquer des « effets pervers » liés à la numérisation, et des dynamiques jouant à une autre échelle, l'adoption d'un bon nombre de dispositifs technologiques pourrait être liée à des dynamiques structurelles touchant plus largement le secteur (quantification de l'aide, « redevabilité bailleur », rapprochement avec le secteur privé, politiques sécuritaires, etc.).

Il faut aussi préciser l'objet que protège le droit de la protection des données et l'ensemble de valeurs que sous-tend ce droit pour les humanitaires. D'où le fait de déconstruire l'idée que la protection des données est nécessairement équivalent au droit à la vie privée. Pour rappel, la relation entre ces deux types de droit est objet à interprétation, et bien que très proches, ils ne se confondent pas nécessairement. L'objectif du droit de la protection des données peut varier selon son périmètre d'application, selon le type de donnée qu'il s'agit de protéger (des données sensibles ou non), selon le sens associé à la nature « personnelle » des données, ce point faisant l'objet de controverse comme l'a montré Julien Rossi[199]. Ajoutons que la notion de vie privée est plus large et comprend une facette informationnelle, mais elle englobe aussi la protection de l'intimité corporelle et de la vie familiale. En outre, le droit de la protection des données et le droit à la vie privée peuvent être associés à une série de valeurs. Pour certains auteurs, il constitue une précondition à la liberté d'expression, et donc d'une société démocratique. On a là une conception fonctionnaliste de la vie privée, dans le sens où elle permet d'activer d'autres droits. Qu'en est-il des humanitaires ? Comment formulent-ils la nécessité de protéger les bénéficiaires face aux différents risques numériques ?

Pour notre part, on fait l'hypothèse que les humanitaires associent les risques numériques à un problème de protection des bénéficiaires et des civils. Les humanitaires se sont tout d'abord donné comme mission la protection des personnes face aux ravages concrets causés par des catastrophes et des guerres. Protéger sa vie privée signifie préserver son image et son intimité, soit une composante « abstraite », mais essentielle à l'identité d'une personne. Alors qu'une part de l'activité des humanitaires reste concentrée sur l'allocation de biens matériels (médicaments, nourriture, soutien financier, etc.). D'ailleurs, les actions de protection ont pour finalité de « prévenir et alléger en toutes circonstances les souffrances des hommes ; de protéger la vie et la santé et de faire respecter la personne humaine de façon impartiale. »[200] Les activités de protection impliquent de prendre en compte deux dimensions : une dimension physique, matérielle, puisqu'il est question de souffrance, et une dimension immatérielle puisqu'il est question de « respect ». Par conséquent, considérer la protection des données comme une activité de protection humanitaire signifierait tout d'abord que les atteintes aux

[199] « il faut préciser ce qu'il s'agit de protéger lorsqu'il est question de protection des données : il semblerait qu'on parle de protéger la vie privée d'un individu. Rien n'est moins sûr. En bref, certaines conceptions de la protection des données mettent l'accent sur la façon de caractériser les données, sensibles ou non sensibles. D'autres mettent l'accent sur la façon de contrôler l'accès ou non aux données (en dehors de leurs sensibilités) et de protéger la vie privée des individus » ROSSI, Julien, « Protection des données personnelles et droit à la vie privée: enquête sur la notion controversée de "donnée à caractère personnel" », thèse, Science de l'information et de l'information, Université Technologique de Compiègne, 2020

[200] Politique du comité permanent interinstitutions sur la protection dans le cadre de l'action humanitaire, iasc, 2018 https://interagencystandingcommittee.org/sites/default/files/migrated/2018-10/iasc_protection_policy_french_logo_final.pdf

principes du droit tel que le RGPD causeraient de la douleur, et/ou qu'elles porteraient atteinte à la vie et à la santé des bénéficiaires. Cela suppose que les humanitaires puissent par exemple lier des risques numériques et violence d'État par exemple, comme on l'a évoqué plus haut. L'accent est alors mis sur les répercussions concrètes et physiques liées au non-respect du droit de la protection des données. Cette lecture nous semble spécifique à l'humanitaire. En tout cas, la doctrine des autorités de protection de données n'envisage pas (à notre connaissance) ce type de répercussions. La CNIL ou le Comité européen à la protection des données se concentrent en effet sur le cas de discriminations ou d'atteinte aux droits et aux libertés. Il s'agit d'autres droits fondamentaux tels que la liberté d'expression, la liberté de pensée, la liberté de circulation, la prohibition de discrimination, le droit à la liberté, à la conscience et à la religion.

Cependant, nous nous arrêtons pas à cette hypothèse. Le fait de protéger les données des bénéficiaires serait aussi associé pour les humanitaires à la nécessité de protéger leur vie privée, ainsi que leur dignité. Cela repose sur la possibilité pour les bénéficiaires de contrôler dans une certaine mesure l'accès à ses données, afin de préserver leur intimité. Comme on l'a déjà indiqué, on se départit d'une lecture strictement biopolitique de l'aide, du moins de son interprétation selon laquelle l'humanitaire serait avant tout préoccupé par la survie biologique des bénéficiaires et les réduiraient à être des victimes passives. Cela ne signifie pas gommer les rapports de pouvoir traversant l'humanitaire pour autant. Ces derniers ont été objectivés par la recherche (qu'ils soient ou non dus à des legs coloniaux). Mais les humanitaires tentent de les atténuer (en défendant par exemple la localisation de l'aide). On peut en dire de même concernant la protection des données, puisqu'on suppose que les humanitaires tentent de garantir différents droits aux bénéficiaires (entre autres en matière de consentement).

## Méthodologie – terrain

On mettra à l'épreuve et l'on discutera ces différentes hypothèses. Mais il nous reste maintenant à préciser comment on est venue à travailler sur la protection des données dans l'humanitaire, à circonscrire notre terrain et notre matériel empirique qui vont servir à appuyer notre démonstration.

La construction d'un objet de recherche est liée à un parcours individuel (quand bien même il repose grandement sur l'apport d'échanges et de rencontres scientifiques et extra-académiques). Il nous parait donc nécessaire de commencer par évoquer brièvement notre cheminement personnel. Notre mémoire de première année de Master en science politique peut être considéré comme un point de départ. Ce premier travail a porté sur les liens entre travail social et NTIC. Il a mis l'accent en premier lieu sur la problématique de la « managérialisation » de ce secteur, et dans ce cadre nous avons pu rencontrer des personnes impliquées dans l'innovation sociale. Nous avons en quelques sorte continué d'explorer lors de notre seconde année de master cette thématique en nous intéressant à des lieux spécifiquement destinés à l'innovation dans l'humanitaire, soit des fablabs. Nous sommes donc parties en Grèce, en tant que bénévole au sein du fablab humanitaire d'Habibi works, situé près d'un camp de réfugiés.

Cette expérience représente un de nos premiers contacts avec le secteur de la solidarité internationale. Nous ajoutons qu'à titre personnel, nous avons été bénévole entre 2016 et 2023 à Entraides Citoyennes, une association d'aide aux personnes sans-abris, ainsi qu'à Utopia 56, une organisation de défense des exilés. C'est avec cette dernière que nous avons participé à des actions d'assistance au Centre « Premier accueil Paris Nord » en 2017, à la Chapelle, essentiellement des distributions alimentaires. Puis, plus récemment, nous avons accompagné, toujours avec Utopia 56, des familles d'exilés dans des hébergements citoyens. De surcroit, nous avons ponctuellement travaillé durant l'été 2019 au siège d'une ONG humanitaire (Solidarités International) en tant que chargée de communication numérique. Enfin, nous avons pu aussi échanger de façon régulière et informelle avec des proches ayant effectué au sein de MSF des missions « post-conflits » dans le Caucase. L'ensemble de ces expériences nous a donné un premier aperçu du travail humanitaire. Mais surtout, elles nous ont permis d'aborder nos enquêtés avec une meilleure compréhension de leurs savoirs implicites. Sachant que nous avons complété nos connaissances de ce milieu par la lecture de publications destinées aux professionnels de l'aide, à savoir des articles de presse de revues comme The New humanitarian, Alternatives humanitaires, et de publications de centre de réflexions comme le Groupe Urgence Réhabilitation et Développement (URD), le centre de réflexion sur l'action et les savoirs humanitaires de MSF (CRASH).

Parallèlement, nous avons commencé à élaborer notre projet de recherche de thèse. La construction de notre objet a été progressive et s'est faite par ajustements successifs. Nous souhaitions rester dans la lignée générale de nos mémoires de master, et approfondir le sujet du numérique dans l'humanitaire ou dans le domaine médico-social. Pour tout dire, au départ, nous avions choisi de travailler sur des dossiers médicaux destinés aux réfugiés sous l'angle de la protection des données de santé.

Notre intérêt pour la problématique de la vie privée a été nourri par l'actualité. Il se trouve que notre entrée dans l'étude des NTIC a coïncidé avec une phase spécifique de leur histoire. La fin des années 2010 a été en effet marquée par un renforcement de ce qui peut constituer une « perception "désenchantée" du numérique »[201]. Cette dernière s'est cristallisée lors de différentes controverses nées de la médiatisation de certaines affaires, comme Cambridge Analytica en 2018, ou les « Facebook Files » en 2021. Et surtout, l'entrée en vigueur du RGPD a contribué à mettre sur le devant de la scène les enjeux de protection des données. Et il se trouve que les dossiers médicaux destinés aux exilés nous paraissaient être un objet de recherche intéressant en raison de la sensibilité des données de santé. Point d'importance, les dossiers médicaux faisait alors écho courant 2019 aux débats relatifs à la base de donnée du Data health Hub.

En bref, on pensait d'abord travailler sur des dossiers de santé, à savoir des objets très différents selon le mode d'organisation des données, selon que leur échelle d'usage soit locale, à l'échelle d'un hôpital, d'un camp de réfugié, ou régionale, voire nationale, selon les modalités d'accès et de contrôle des données, selon que ces dernières soient ouvertes ou non à leurs usagers. Il existe des dossiers médicaux utilisé par des agences Onusiennes ou des Organisations internationales :

[201] ALEXANDRE Olivier, BEUSCART Jean-Samuel, BROCA Sébastien, « Une sociohistoire des critiques numériques », *Réseaux*, 2022/1 (N° 231), p. 9-37. https://www.cairn.info/revue-reseaux-2022-1-page-9.htm

- L'UNHCR a par exemple développé un « carnet de consultation patient (Patient consultation Booklet).
- La Commission européenne a soutenu un projet de dossier médical à destination de réfugié, intitulé CARE.
- L'UNRAW a mis en place depuis 2011 des programmes en e-health, et utilise des dossiers médicaux numériques dans le camp.
Des start-up ont pu se lancer dans la création de dossiers médicaux à destination d'exilés. Par exemple Iryo a conçu une application permettant une gestion directe par les réfugiés eux-mêmes de leurs données de santé via leur smartphone.

Au tout début de nos recherches, nous avons souhaité réinscrire ces cas d'étude dans le contexte plus général du numérique humanitaire. Mais au fil du temps, nous avons noté qu'il y avait peu de littérature francophone sur ce sujet. Et surtout, lors de cette première revue de littérature (effectuée durant l'automne 2019), nous avons alors remarqué qu'un sujet était peu étudié : le RGPD et les délégués à la protection des données des ONG. Comme on l'a dit plus haut, les risques liés au numérique en matière de vie privée étaient évoqués par plusieurs auteurs, mais sans prendre en compte la façon dont les humanitaires tentaient d'y remédier. Une bonne part de la littérature était proche d'un prisme de lecture axé sur la dialectique entre « care » et « contrôle ». En outre, une bonne part des travaux se sont attachés à faire entendre le témoignage d'exilés et d'humanitaires et décrire les usages numériques de travailleurs humanitaires sur le terrain. C'est le cas de Léa Macias par exemple, ou de Margie Cheesman. Elles ont eu recours à une méthodologie d'observation participante, se traduisant par des séjours , plus ou moins prolongés, dans des camps de réfugiés en Jordanie. Pour notre part, nous avons progressivement choisi de laisser de côté notre objet de recherche initial, les dossiers médicaux. Et nous nous sommes concentrées au fur et à mesure de la thèse sur le sujet plus général de la vie privée dans l'humanitaire, et plus particulièrement sur la profession de délégués à la protection des données. Ce choix implique que nous avons choisi une autre méthodologie d'enquête. En effet, les DPO n'ont pas un contact permanent avec le « terrain », ils travaillent habituellement aux sièges d'ONG. Or nous n'avons pas pu mener d'observation participante au sein d'une structure. Par conséquent, notre terrain empirique est en partie constitué d'entretiens.

Joindre les DPO a été relativement simple : il nous a suffi d'utiliser les adresses de type « dpo@org » qui étaient communiquées sur les sites Internet des organisations. Cela dit, le taux de réponse a varié selon les DPO. Un facteur clef a été le peu de reculs de nos enquêtés. Ces derniers n'avaient que trois ou quatre ans d'expérience, voire à peine un an. Par conséquent, certains DPO n'ont pas donné suite à nos demandes d'entretiens, craignant de ne pas avoir assez d'informations pour nos recherches. D'autres ont accepté, au contraire, souhaitant mettre en avant un rôle pour le moment peu documenté en sciences sociales. D'autres enquêtés ont considéré que la réalisation d'un entretien leur permettait d'avoir un retour réflexif sur des pratiques pour eux encore émergentes. D'autres ont investi l'entretien comme un lieu de témoignage, voire de dénonciation, critiquant le manque de mise en œuvre des principes du RGPD.

Mais très vite, nous avons réalisé que nous ne pouvions passer qu'un nombre « limité » d'entretiens. En effet, n'ayant pas effectué d'observation participante au sein d'une ONG, et n'ayant pas tranché pour une démarche monographique, nous avons élargi dans un premier

temps notre terrain d'enquête au niveau européen (soit l'échelle d'applicabilité du RGPD). Mais il est apparu que seules les grandes ONG avaient nommé un DPO. Or le secteur humanitaire étant très centralisé, cela ne représente alors qu'un nombre réduit de personnes. En fin de compte, nous avons pu passer 23 entretiens avec des DPO. Par conséquent, nous avons choisi d'adopter une « focale » plus large. Le choix de cet angle d'approche s'est fait de façon progressive. Nous avons peu à peu décidé de mener des entretiens avec des personnes travaillant dans l'humanitaire et susceptibles d'être aux prises avec des enjeux de vie privée sans être pour autant des professionnels de la protection des données. Notre objet de recherche ne s'est donc pas restreint au rôle des DPO dans la mise en œuvre du RGPD, d'autant qu'il nous est vite apparu que les enjeux de vie privée et de protection des données débordaient le RGPD, et ce pour plusieurs raisons. Tout d'abord, plusieurs facettes du numérique humanitaire se situent à la frontière du RGPD. Le CICR ou l'UNHCR, des organisations internationales, n'appliquent pas le RGPD ( en raison de leurs immunités et privilèges). En outre, une part des opérations des ONG échappent au RGPD ( en bref la portée extraterritoriale du règlement porte à interprétation). Mais surtout, les humanitaires interviennent dans des terrains de conflits, notamment des zones conflictuelles liés à des groupes armés qualifiés de terroristes, et elles sont aussi concernées par la numérisation des conflits, notamment par toute une série de cyber-opérations qui les concerne aussi. Or le RGPD ne s'applique pas à des sujets liés à sécurité nationale, ou des contextes sécuritaires (autre cadre juridique ou bien une suspension de ce dernier). Dernier point, il faut savoir que le RGPD ne s'applique pas aux données des morts, les ONG sont occupées à sauver les vivants, mais interviennent aussi dans le travail des morts, et notamment l'identification des morts, qui pose de gros enjeux de protection des données.

Pour compenser les limites d'application du RGPD, les ONG et OI humanitaires ont produit une grosse quantité de droit souple, qui s'inspire en grosse partie du RGPD, mais qui est aussi dans certains cas des formes de traduction du droit international humanitaire (DIH) et de principes éthiques propre au milieu. Or tout ceci pour en venir au fait, que les acteurs produisant ce cadre éthique et qui interprètent la façon le DIH s'applique à l'espace numérique ne sont pas nécessairement des DPO. Par exemple, une bonne part du cadre normatif est produit par les juristes travaillant pour le CICR, qui est garant du DIH. Cela est flagrant pour tout ce qui concerne la dimension cyber des conflits qui est encadré par le droit international humanitaire. Nous ne les avons pas directement interrogé, mais leur production doctrinaire a consisté aussi une bonne partie de la matière de la thèse. Elle prend la forme de guidelines, de droit souple, mais aussi de façon plus générale d'une série de traces numériques, soit des billets de blog, des interventions dans des conférences, des rapports de réunions, des déclarations dans des arènes multilatérales, etc. Soit un ensemble assez divers de documents et traces qui ont constitué un terrain numérique et nourri une bonne partie de notre thèse.

En fin de compte, nous avons interrogé des ingénieurs engagés au sein d'ONG, qu'ils soient impliqués dans le développement de dossiers médicaux ou que ce soient des membres du service informatique de ces structures, ou qu'ils appartiennent à des organisations spécialisées dans la connectivité de crise. Nous avons aussi contacté des personnes affiliées au poste de chargé de gestion de l'information et prenant part à la gestion et à la coordination des opérations de recueil des données et des statistiques d'ONG. Leur tâche va du choix de logiciel de collecte d'information d'une organisation à la création et consolidation de bases de données. Nous avons aussi joint des personnes impliquées dans le travail de collecte

d'information d'une ONG, sans qu'elles soient nécessairement « professionnalisées » dans cette tâche[202]. Il s'agissait aussi des personnes directement en contact avec le « terrain », soit des bénévoles d'associations, des travailleurs sociaux ou des médecins, à savoir des personnels employés au sein d'ONG humanitaires sur des programmes de santé, mais aussi des médecins impliqués dans la gestion de dossiers médicaux, ou plus spécifiquement des médecins légistes.

Nous disposons donc en tout de 96 entretiens d'une durée de 30 minutes à 3 heures, menés par visioconférence ou par téléphone, à l'exception faite de trois d'entre eux, ayant eu lieu en présentiel. En somme, nous avons donc interrogé des DPO d'ONG humanitaire (23 entretiens), des information management officer (6 entretiens), des personnes au profil d'ingénieurs employées dans des ONG ou développant des logiciels de traitement de données médicales destinés à des ONG humanitaires (16 entretiens). On a également interrogé des personnes en contact direct avec les bénéficiaires, et traitant des données au jour le jour sans être professionnalisées sur la gestion d'information. Il s'agit soit de bénévoles d'association, (4) des médecins impliqués dans la coordination de programmes de santé d'ONG humanitaires ou dans des services médicaux destinés aux exilés (39), ou encore de médecins légistes traitant des données d'identification de migrants morts lors de leur traversée (8).

Nos entretiens avec des DPO ont servi de matière centrale de la thèse. Nous les avons réemployés de façon extensive dans la première partie, et surtout dans son second chapitre sur la régulation de l'innovation. Ils appuient aussi une bonne part des développements du chapitre 3 portant sur les échanges de données avec les acteurs étatiques. Nous y avons fait référence de façon plus ponctuelle dans le chapitre sur les cyberattaques. Et enfin, ils occupent une place importante dans le chapitre 6 portant sur le consentement. Le fait de passer par des entretiens était nécessaire pour aborder le travail des DPO, en raison du manque de source sur le sujet. On a aussi pu s'appuyer sur des rapports d'ONG et des conférences. Mais la plupart du temps, ces sources se concentrent sur un aspect particulier de la profession : les enjeux liés au consentement, ou sur la place de la biométrie dans l'humanitaire. En tout cas, certains sujets étaient moins couverts dans la production publique disponible sur Internet. On pense aux méthodologies de gestion de risque, et aux analyses d'impact en matière de protection de données, ainsi que les approches de type « privacy by design ».

Le chapitre 8, sur l'identification des morts, constitue un terrain à part, tout en étant relié logiquement au reste de la thèse. Il sert de prolongement à nos réflexions sur la notion de dignité dans l'humanitaire et la protection des données. Contrairement aux chapitres 5 et 7, il repose sur une série d'entretiens. Il a nécessité de contacter des acteurs spécifiques, comme des médecins légistes, des membres d'ONG impliqués dans l'identification des morts. Il s'agit d'un groupe quelque peu à part au sein de l'humanitaire, mais ses acteurs sont fortement liés, d'où un effet boule de neige particulièrement efficace, qui nous a permis rapidement de rentrer en contact avec des personnes ayant accepté de répondre à nos questions.

[202] MACIAS, Léa, « Professionnalisation de l'humanitaire et production de données dans le camp de réfugiés de Zaatari en Jordanie », *Carnet de recherche hypothèse, conflits et migrations*, 21/02/2018 https://lajeh.hypotheses.org/987

Nos échanges avec les enquêtés se sont faits en majeure partie par visioconférence, via Microsoft Team, Zoom, ou via Jitsi. Ce choix a été contraint par le fait qu'une partie des entretiens ont été réalisés avec des personnes ne résidant pas en France. Ajoutons que ces entretiens ont eu lieu en partie durant le confinement. La situation était exceptionnelle. Toutefois, l'utilisation de logiciel de visioconférence est usuelle au sein d'ONG, en raison du fort degré d'internationalisation des acteurs de l'aide. Le fait d'utiliser des dispositifs de visioconférence a toutefois eu deux conséquences. Nous avons pu observer que cette modalité d'interaction tend à « lisser » les échanges, à induire une plus grande distance. Les entretiens menés en présentiel ont été moins cadrés sur le plan temporel (ils ont dépassé la durée d'une heure de façon plus systématique). Ils ont été en partie plus informels, dans le sens qu'ils ont donné lieu à des écarts plus grands avec la grille d'entretien initiale.

Deuxième point, nous nous sommes demandé si le choix du logiciel a pu avoir des conséquences sur le contenu de l'entretien en fonction de leur sensibilité. Toujours est-il que le choix du logiciel de visioconférence constitue à ce titre une indication du rapport que l'acteur entretient avec le droit à la vie privée. Pour notre part, nous avons pu proposer, dans certains cas, d'utiliser le logiciel Jitsy[203]. Quant aux enquêtés, la plupart du temps, les DPO utilisaient de façon commune le logiciel employé par l'ONG, bien souvent Skype, ou Microsoft Team. Il y eut une exception. Sur 96 entretiens, seul un DPO nous a imposé d'emblée d'échanger via Signal, pour des raisons de confidentialité. Il faut dire que nous-mêmes nous étions déjà interrogées sur la potentielle sensibilité de notre terrain, et sur les conséquences que cela peut avoir en matière de méthodologie de recherche. Or le fait de qualifier un terrain « sensible » englobe des réalités très diverses. Cela peut relever de ce qui est de l'ordre de l'intime (entre autres du sexuel), du tabou social, ou ce qui est couvert par le secret professionnel (médical, bancaire, journalistique), par le secret des affaires, ou par le secret d'État ou le secret défense, ou ce qui relève de la marginalité (domaine des pratiques illicites, trafiquants de drogue, cybercriminels, etc.), ou bien des sujets relatifs à des populations vulnérables, voire persécutées, et préférant rester dans l'« ombre ». Ajoutons que le sens de ce terme est aussi juridique et fait référence, dans le RGPD, à la catégorie de données sensibles (soit des données de santé, relatives à la sexualité, ou à des convictions religieuses ou des opinions politiques)[204].

Une bonne partie de nos recherches ne semblent pas relever du secret. Nous avons en effet interrogé des DPO sur des pratiques — relevant parfois de tâches de travail routinières (Analyse d'impact, contrats, rédaction de clauses de confidentialités, etc.). Cependant, des facettes plus spécifiques de notre sujet ont pu être qualifiées de sensibles aux yeux de nos enquêtés. Ce qualificatif a pu être utilisé pour décrire des activités liées à différentes formes de surveillance touchant les ONG, quelles se manifestent par le partage de liste de bénéficiaires d'ONG aux gouvernements, ou de mesures de contreterrorisme ou de cyberopérations. Par exemple, communiquer de façon détaillée sur les cyberattaques implique potentiellement de « divulguer » une faille de sécurité de la part des ONG. Cela peut conduire à « révéler » des vulnérabilités sur lesquelles les organisations ne souhaitent pas rendre compte. Cela a aussi des implications géopolitiques que l'ONG ne désire pas mettre en

[203] https://www.frontlinedefenders.org/fr/resource-publication/jitsi-meet-simple-and-secure-video-conferencing-platform

[204] DAHO, Grégory, GUITTET, Emmanuel-Pierre,POMAREDE, Julien, « Les territoires du secret : confidentialité et enquête dans les mondes pluriels de la sécurité », *Cultures & Conflits*, 118 | été 2020,. http://journals.openedition.org/conflits/21827

avant. Par exemple, le CICR reste discret sur la nature de l'attaquant de la cyberopération de janvier 2022 pour ne pas « politiser » le sujet et conserver une posture de neutralité.

Cela dit, très vite, nous nous sommes rendu compte que le caractère sensible d'un fait comprend aussi une grande part d'interprétation du niveau de risque lui étant associé. Pour certains DPO, le fait de partager des données anonymisées de bénéficiaires à un gouvernement local était anodin. Pour d'autres DPO, même anonymisées, les échanges d'informations consistaient en soit une prise de risque et tout partage de données avec un État était alors considéré comme un sujet « sensible ».

Toujours est-il que si un enquêté a pu estimer qu'un fait peut être caractérisé comme tel, cela a pu avoir des conséquences sur la qualité et la nature de l'information communiquée. Dans certains cas, des enquêtés ont pu indiquer qu'ils ne pouvaient pas nous communiquer un détail (nom de gouvernement, nom de groupe armé). Dans d'autres cas, des DPO ont pu au contraire nous faire part de leur absence de connaissance concrète des risques encourus concernant tel ou tel fait. Nous n'avons évidemment pas de quoi vérifier s'il s'agissait de cas d'omission afin de garder une information confidentielle ou non. À vrai dire, il nous importe plutôt de recueillir la façon dont les enquêtés formulent ou perçoivent un phénomène et le cadre en matière de problématique relative à des enjeux de vie privée ou non. Enfin, des DPO ont pu évoquer des scénarios fictifs que toute personne travaillant sur la protection des données dans l'humanitaire peut avoir à l'esprit. On pense à des échanges de données entrainant la persécution, l'arrestation, voire la mort de tel ou tel bénéficiaire. Ou bien il a pu être fait références à quelques cas avérés, bien connus au sein de l'humanitaire et documentés par des ONG de défense de droits de l'homme ou par des journalistes. Des cas n'ayant rien de secret donc. On en a déjà mentionné en ouverture de l'introduction : il s'agit du partenariat avec Palantir du WFP, des échanges de données entre le HCR et le gouvernement birman, l'arrêt de distribution alimentaire au Yémen par le World Food Program en raison d'un refus de collecte de données biométrique par des groupes liés aux Houthis.

Ajoutons enfin qu'une dimension bien particulière de notre thèse nous parait être particulièrement sensible, en raison du contexte politique plus général dans lequel elle s'inscrit. Il s'agit du contrôle du financement des ONG dans le cadre de mesures de contre-terrorisme. Sa sensibilité est renforcée par le climat politique actuel et le conflit israélo-palestinien. Il nous semble important de signaler le fait que nous avons décidé d'écrire sur le sujet du terrorisme avant les attaques du 7 octobre 2023. Ces dernières vont indubitablement avoir des répercussions profondes. Mais nous n'avons pas pu les prendre en compte dans nos recherches en raison d'un manque de recul. Nous ne disposons tout simplement pas de sources aussi récente. Pour préciser, notre chapitre y étant consacré ne repose pas sur des entretiens. Nous avons décidé de couvrir ce sujet malgré tout dans le sens où il permet de réfléchir sur les limites du RGPD concernant son application à des enjeux régaliens et sécuritaires. Le fait que ce sujet ait été mis à l'agenda politique lors du vote de la loi relative à la préservation de l'espace humanitaire de 2021 nous a grandement aidées. Il a fait l'objet de mobilisations, qui ont laissé des traces consultables en ligne. Ce sont des documents témoignant de prises de positions ou de communications de coalitions d'acteurs (sous forme de tribunes). Le chapitre y étant consacré est fondé en majeure partie de ressources accessibles en ligne : comptes rendus, prises de position d'ONG et d'humanitaires (sous forme

de tribunes par exemple), audits, rapports de centre de recherche, base de données des organes politiques (Assemblée nationale, gouvernement fédéral américain). Ces documents nous ont permis de documenter ce qui nous intéressait le plus : la façon dont a pu être cadré le sujet. Nous nous intéressions alors aux enjeux de vie privée et non pas à la « réalité » du sujet du financement potentiel de groupes qualifiés de terroristes par les ONG. Ce sujet aurait été nettement plus sensible et il aurait demandé une méthodologie différente.

Toujours est-il que s'est évidemment posée de façon plus générale la question de l'anonymisation des entretiens et la protection des données de notre recherche[205]. Nous avons indiqué le statut professionnel de l'enquêté. Or, il n'y a généralement qu'un ou deux DPO par organisation. Pour conserver un certain degré de pseudonymat, nous avons décidé de ne pas mentionner le nom de l'ONG. Mais nous avons hésité à préciser des détails importants pour la compréhension du sujet, comme la formation initiale du DPO (juriste ou ingénieur), mais le risque de ré-identification nous a paru trop grand. Nous avons cependant choisi de conserver le statut juridique de la structure (ONG ou organisation internationale), cette indication étant nécessaire pour mieux comprendre certains sujets liés aux immunités et privilèges. Nous avons conscience que cela renforce la possibilité de ré-identifier l'organisation, surtout concernant le CICR, qui a une posture bien spécifique dans le champ et que nous traitons dans certaines parties à part. L'organisation a cependant une dizaine de personnes affiliées au service de protection des données, ce qui maintient donc un certain pseudonymat.

Ajoutons que nous avons aussi recouru à de la littérature grise (rapports d'institutions et articles de presse par exemple) et sans faire du renseignement en source ouverte (OSINT), nous avons exploité un « terrain numérique ». Plus précisément, un premier type de source nous a permis de compléter des entretiens ou de mieux cibler ces derniers. Il recoupe différents espaces d'expression où les acteurs communiquent des prises de position ou réflexions sur un sujet donné. Ce sont des articles de blogs, des interviews, des conférences, de publications sur les réseaux sociaux. Nous avons consulté régulièrement les blogs du CICR, « Humanitarian Law & Policy du CICR,[206] le blog de Linda Raftree, [207] d'Amos Doornbos[208]. Nous avons aussi collecté des échanges ayant lieu sur des listes de diffusion, dont celle du collectif « responsible data », rattaché à l'organisation de défense des droits en ligne The Engine Room.

D'un autre côté, la littérature grise est centrale au moins pour trois chapitres de la thèse. Par exemple, le premier chapitre retrace une thématique déjà explorée par la littérature scientifique anglophone, à savoir la notion d'expérimentation et le secteur humanitaire comme laboratoire technologique. Nous avons complété cette littérature par des recherches personnelles, en nous référant à des rapports d'organisations et des articles de presse, et surtout en creusant trois cas d'études spécifiques (la biométrie, les drones et les données massives). Ensuite, deux autres chapitres ont été construits à partir de la littérature grise. On

[205] ROSSI Julien, BIGOT Jean-Édouard, « Traces numériques et recherche scientifique au prisme du droit des données personnelles », *Les Enjeux de l'information et de la communication*, 2018/2 (N° 19/2), p. 161-177. https://www.cairn.info/revue-les-enjeux-de-l-information-et-de-la-communication-2018-2-page-161.htm
[206] https://lindaraftree.com/
[207] https://blogs.icrc.org/law-and-policy/
[208] https://thisisamos.com/

pense au chapitre 4 portant sur les mesures de lutte contre le financement du terrorisme. Notre chapitre 5 portant sur les cyberopérations touchant les ONG humanitaires a nécessité une méthodologie spécifique, que nous détaillerons dans le chapitre consacré à ce sujet, par souci de lisibilité. Enfin, nous avons eu aussi recours à de la littérature grise pour écrire le chapitre 7 sur les blockchains. Il existe en effet peu de projets relatifs à ces dernières, complexifiant ainsi l'accès à des sources de première main.

Nous nous sommes donc fondée de façon extensive sur des rapports publiés par les ONG. D'ailleurs il faut noter que les ONG produisent elles même une bonne quantité de documents équivalents à du droit souple, mais aussi des rapports portant sur des facettes opérationnelles de leur action, parfois écrits par des chercheurs. D'ailleurs, les limites entre humanitaires et monde académique sont en partie poreuses ; même si des points de friction existent (entre savoirs fondamentaux, savoirs institutionnels, neutres et indépendants, et savoir opérationnels, voire militants). De fait, certains chercheurs se situent à la frontière entre les deux secteurs, cela est par exemple le cas de Larissa Fast, ou Kristin Sandvik[209]. Mais le secteur de la solidarité internationale peut aussi être lui-même producteur de connaissances. Le secteur est caractérisé par une forte réflexivité. Cela se traduit par l'existence de centres de réflexions spécialisés, plus ou moins ancrés dans le secteur humanitaire. On pense à la fondation de la Croix-Rouge ou au Centre de Réflexion sur l'Action et les Savoirs Humanitaires (Crash), rattaché à MSF. La réflexivité y est devenue réflexe et la critique sur les pratiques humanitaires y est institutionnalisée, comme le remarque encore Elsa Rambaud[210]. Ajoutons que nous nous sommes référées aussi aux travaux du Centre For humanitarian Action, soit un autre lieu d'élaboration de connaissance, qui nourrit plus directement la politique de solidarité internationale allemande, mais qui est présenté comme indépendant et reste financé et soutenu par un consortium d'ONG humanitaires[211]. En revanche, l'Overseas development institute (ODI) et l'Humanitarian pratice Network, sont présentés comme des centres de recherches indépendants, mais ils nous semblent plus directement liés au ministère des Affaires étrangères britannique, qui est un de ses plus grands bailleurs[212]. Enfin, différentes organisations se sont spécialisées sur le sujet du numérique humanitaire. Elles sont caractérisées par une finalité fortement opérationnelle et ont vocation à diffuser des savoirs et des compétences plus directement techniques au sein du secteur. On pense à CartONG, Enginee Room, et au Cyberpeace institute.

Enfin, nous précisons qu'en raison de l'échelle temporelle de la thèse allant de 2010 à 2024, il a été nécessaire de jouer sur plusieurs temporalités. Nous avons dû effectuer un travail de veille, afin de collecter des publications de littératures grises venant d'être publiées. Mais nous avons aussi pris en compte le temps plus long, ce qui pose la question de la pérennité des sources d'informations en ligne. Mais certaines institutions ont leur propre politique

[209] RIDDE, Valéry, « Chercheurs et acteurs humanitaires: passer de la méfiance à l'efficience », *Alternatives Humanitaires*, 2021, n° 17 https://www.alternatives-humanitaires.org/fr/2021/07/19/chercheurs-et-acteurs-humanitaires-passer-de-la-mefiance-a-lefficience/

[210] RAMBAUD Elsa, « L'organisation sociale de la critique à Médecins sans frontières », *Revue française de science politique*, 2009/4 (Vol. 59), p. 723-756.https://www.cairn.info/revue-francaise-de-science-politique-2009-4-page-723.htm

[211] Ce centre de réflexion a un modèle de financement diversifié, comprenant des soutiens matériels du ministère affaire étrangères allemand, mais aussi de partenaires humanitaires. Elle est chapeauté par différentes ONG allemandes comme MSF Allemagne, Caritas, la Croix Rouge et l'ONG caritative, Diakonie. https://www.chaberlin.org/en/about-cha/

[212] Ajoutons que son président actuel, Suma Chakrabarti, est un homme politique britannique, ayant eu de fortes responsabilités au DFID.

d'archivage. Il se trouve que le secteur humanitaire dispose de sa propre base de données ReliefWeb[213], remontant à 1996. Différentes organisations ont aussi leur propre politique de gestion et de publicisation de rapports, comme le HCR ou encore le CICR. Cela nous a été utile pour retracer la mise à l'agenda de certains sujets, que ce soit les cyberopérations ou la constitution d'un cadre éthique en médecine légale.

Une autre source d'information s'est révélée être des conférences en ligne, le sujet étant contemporain, il a correspondu à un moment d'échange intensif entre acteurs du terrain, qui se sont retrouvés dans des arènes onusiennes. Cela étant, comme nous l'a indiqué un enquêté, il s'agit bien souvent d'acteurs appartenant aux plus gros acteurs du secteur humanitaire, à savoir le mouvement de la croix rouge ainsi que le réseau onusien. Nous avons aussi noté que le nombre de conférences impliquant les acteurs du champ humanitaire nous a semblé décroitre à partir de fin 2023 et début 2024. Mais il est trop tôt pour établir des conclusions sur ce fait. Toujours est-il que les conférences peuvent également être le lieu de réseautage, observation des modalités de socialisation d'acteurs, ou occasion d'échanges informels ou de prise de contact pour des entretiens. Cependant, en ce qui nous concerne : un bon nombre de conférences ont eu lieu à l'étranger (en Suisse, mais aussi aux USA). Toujours est-il que sur la période de 5 ans qu'a duré notre thèse, nous avons totalisé environ 150 conférences sur le numérique humanitaires et sur des problématiques connexes (protection des données, souveraineté numérique). Nous avons noté quelques points sur ces acteurs. Ils n'étaient pas nécessairement de délégués à la protection des données. Il s'agissait aussi de membres de l'OCHA, d'information manager officer, de consultant, d'universitaires. Certains de ces acteurs avaient une proximité plus grande avec le monde des droits de l'homme en ligne. Nous avons assisté aux conférences « Rightscon », organisées par l'organisation de défense des droits de l'homme en ligne, Access Now. Nous avons suivi en ligne les éditions de 2020, 2021, 2022, 2023. On a assisté aux conférences bruxelloises CPDP Computers, privacy & data protection (CPDP), plus spécifiquement l'édition de 2020 en présentiel, suivi de conférences archivées sur leur chaine YouTube ; aux conférences de Cartong en 2020 et 2022 ; et de l'humanitarian networks & partnership week en 2022,2023. Enfin, nous avons évidemment consulté le cycle de conférences dédiées au numérique humanitaire organisé par le CICR, le Digitarium[214].

Nous précisons que pour traiter l'ensemble de ces données collectées sur l'Internet nous n'avons pas eu recours à des méthodologies computationnelles. Cela est aussi valable pour les sources journalistiques. On a toutefois effectué une première collecte d'articles au fil de l'eau, puis on a au cours de la thèse commencé à envisager d'utiliser un logiciel de textométrie (Iramuteq) et effectué un travail plus systématique en recensant environ 1288 références entre 2000 et avril 2022. Il s'agissait de la presse anglophone (destiné à un public international ou une presse britannique nationale) et francophone (France et Suisse). On a constitué trois catégories de presse : la presse grand public, avec des journaux dits de « référence » (Le Monde, Libération, Figaro ; le Time, The Guardian ; le Temps) ; la presse spécialisée, relative au numérique (avec des revues comme Wired, ou Usbek et Rica en France), la presse relative à l'humanitaire, avec The New humanitarian et Devex. The New Humanitarian était originalement le réseau « IRIN », une agence de presse délivrant des informations à

[213]ReliefWeb, Wikipedia, 22/07/2022 https://fr.wikipedia.org/wiki/ReliefWeb
[214] https://www.icrc.org/en/digitharium

destination d'acteurs humanitaires couvrant des crises et conflits, également de pays peu en dehors de l'attention médiatique[215]. Devex est d'autre part une plateforme intégrant des offres d'emploi, espaces de réseautage, et service de presse.

Cette collecte nous a permis d'avoir un aperçu de la progression de la numérisation humanitaire, et confirmer que l'année 2010 constitue une année de rupture, le nombre de publications ayant cru drastiquement à partir de cette date. Cela a justifié donc notre bornage chronologique. Mais pour des raison de construction d'objet et d'investissement nécessaire à l'adoption de ce type de méthodologie, nous n'avons en fin de compte pas utilisé ce type de méthodologie computationnelle, et nous n'avons pas inclus la représentation et les discours sur le numérique et des enjeux de protection des données de l'humanitaire véhiculés par la presse.

Toujours est-il que la constitution du corpus nous a permis cependant de mettre en place une méthode de collecte d'article et de veille que nous avons exploitée de façon plus qualitative le long de notre recherche. Ces données médiatiques ont complété nos entretiens puisqu'elle était parfois citée des acteurs de notre terrain (en ce qui concerne la presse spécialisée). Elle a apporté une matière complémentaire à nos entretiens, mais sa lecture a aussi permis d'impulser le travail de recherche. Nous tenons à préciser que deux chapitres de notre thèse ont été directement inspirés par le travail de journalistes. Ainsi c'est la lecture de l'enquête de Taina Tenoven sur l'identification des morts en migration qui nous a donné envie de prolonger ses investigations en les axant sur le droit à la protection des données. Les journalistes de Mediapart et Disclose nous ont aussi permis de découvrir le sujet du criblage des bénéficiaires dans le cadre de mesure de contre-terrorisme, que nous avons complété ensuite dans notre chapitre 4.

### Annonce de plan

Les chapitres de la thèse mettront à l'épreuve nos différentes hypothèses, et permettront de les nuancer. Notre première partie portera donc sur la possibilité de réguler l'innovation humanitaire. En effet, le rapprochement entre le secteur privé et humanitaire facilite l'exportation de récits technophiles, via différents acteurs et espaces et laboratoires d'innovation. L'innovation est en effet favorisé par le fait que l'humanitaire a une longue tradition d'expérimentation. Cette dernière relève en partie d'une forme de technocolonialisme et ce chapitre se réfère donc fortement aux travaux de Nick Couldry et à la notion de colonialité. Toutefois, le secteur s'est doté d'un cadre éthique visant à encadrer les usages numériques et surtout notre deuxième chapitre part de l'hypothèse que le RGPD pourrait contribuer à réguler l'innovation humanitaire et atténuer les rapports de pouvoir propres au technocolonialisme. Tout d'abord, on reviendra sur la mise à l'agenda de la protection des données dans l'humanitaire. On se concentrera ensuite sur l'émergence d'une profession particulière, les délégués à la protection des données. Et on examinera l'usage des

[215] Réseaux d'information régionaux intégrés,Wikipedia 29/04/2024 https://fr.wikipedia.org/wiki/R%C3%A9seaux_d%27information_r%C3%A9gionaux_int%C3%A9gr%C3%A9s

outils de gestion de risques propre au RGPD : les analyses d'impact relatives à la protection des données, et les clauses de confidentialité avec les prestataires techniques. Sachant que l'on verra au cours de notre thèse que le RGPD n'est pas dépourvu de limites. Ce dernier repose en effet sur une démarche de « compliance » mettant l'accent sur la responsabilisation des acteurs, et ce alors que les ressources allouées à la protection des données des ONG restent modestes.

Notre seconde partie sera consacrée aux dynamiques associées aux souverainetés étatiques qu'on a évoquées plus haut. Notre troisième chapitre portera alors sur les circulations de données entre États et ONG. Il reviendra sur leur encadrement, et sur les différentes négociations entre acteurs étatiques et humanitaires y étant relatives. On se demandera notamment dans quelle mesure l'accès au terrain peut se faire en contrepartie à l'accès à des informations détenues par les ONG. Ces dernières sont plus ou moins en position de force face à ces demandes selon leur statut. Les Organisations internationales semblent par exemple être mieux placées en raison de leurs privilèges et immunités. On reviendra sur les cas spécifiques de l'UNHCR et du CICR, ainsi que le défi que pose à l'application des privilèges et immunités la numérisation des opérations et plus spécifiquement l'adoption de l'informatique en nuage.

Dans un second temps, on prendra en compte le fait que le processus de numérisation de nos sociétés accompagne et renforce un phénomène au long cours de recompositions des souverainetés, que ce soit la guerre contre le terrorisme ou les cyberopérations. Notre quatrième chapitre concernera donc les conséquences des mesures de « la guerre contre la terreur » sur l'aide et des mesures de sanction contre le financement du terrorisme. Le sujet semble, a priori, moins connu. Et pourtant, les humanitaires sont également affectés par ces dernières et tentent de négocier un statut d'exception. On reviendra donc sur les arguments qu'elles mobilisent et sur les contournements que les humanitaires trouvent aux mesures de contrôle du financement du terrorisme, qui soulèvent un certain nombre de questions en matière de protection de données. Dans notre chapitre 5, on s'intéressera plus spécifiquement à la façon dont le CICR a mis à l'agenda la protection des civils face aux risques numériques. De par son mandat, le CICR se limite à la protection des civils face aux cyberopérations survenant lors de conflits armés. Et surtout, le CICR se fonde majoritairement sur le droit international humanitaire (DIH) pour protéger les civils et les bénéficiaires des répercussions de ces dernières, notamment en raison du fait que l'application du RGPD en temps de conflit reste discutée. Cette approche n'est pas sans limites, entre autres parce que, comme on le verra, le DIH ne couvrirait pas l'ensemble des cyberopérations. Il reste à savoir si cette limite peut être interprétée (ou non) comme un manque en matière de protection des civils et des bénéficiaires de l'aide, et quels arguments et outils juridiques peuvent être mobilisés pour assurer la défense de ces derniers face aux cyberopérations touchant les organisations humanitaires. Pour notre part, on se référera entre autres au travail du juriste Asaf Lubin. Ce dernier se réfère en effet au principe de dignité (qui est au cœur du droit

international humanitaire) pour appuyer la défense de la vie privée des parties prenantes de conflits contemporains (et donc aussi de civils et de bénéficiaires d'ONG)[216].

Et donc c'est cette notion qui servira de fondement à notre troisième et dernière partie. On prendra le temps de revenir sur les soubassements philosophiques du concept de dignité qui est étroitement associé à celui d'autonomie et d'autodétermination informationnelle. Or, il existe aussi une tension entre injonction à l'autonomie et catégorisation des bénéficiaires comme personnes vulnérables.

On s'intéressera dans le chapitre 5 au recueillement du consentement de personnes estimées vulnérables par les humanitaires. Quant au chapitre 6, il porte sur des projets d'outillage de l'autodétermination informationnelle. En bref, nous étudierons la façon dont des ONG recourent à des blockchains afin de garantir aux bénéficiaires une plus grande maitrise de leurs données. Pour finir, on a jusqu'alors considéré que le concept de dignité reposait sur l'idée d'autonomie des personnes concernées.

Notre chapitre 8 nous permettra de changer d'angle d'approche en traitant la façon dont cette notion fait sens pour les acteurs impliqués dans l'identification des morts en migration. Rendre une dignité à ces morts anonymes passerait pour ces derniers par le fait de leur rendre un nom, et une appartenance sociale. Néanmoins, on verra que ce processus d'identification rentre en tension avec des principes relatifs au droit de la protection des données.

## Partie I — Le droit de la protection des données comme modalité de régulation du laboratoire technologique humanitaire : RGPD et technocolonialisme

### Introduction de partie

Christophe Fabian, directeur du service innovation d'UNICEF, déclare ainsi que « Changer la façon dont l'UNICEF s'acquitte de sa mission d'aide aux enfants les plus vulnérables du monde signifie rechercher et expérimenter de nouvelles technologies. (…)UNICEF doit « penser comme des entreprises et […] travailler avec des start-ups »[217]. Cette déclaration illustre la diffusion de pratiques et de discours managériaux ainsi qu'un impératif d'innovation au sein du secteur humanitaire. Il s'agit de tirer du meilleur des technologies pour allouer une aide la plus efficace et de meilleure qualité. Mais plutôt que d'innovation, il serait plus juste pour certains chercheurs de parler d'expérimentation. L'humanitaire servirait de laboratoire permettant de tester des technologies certes innovantes comme des dispositifs biométriques, des drones, des blockchains, etc., mais surtout peu stabilisées et éprouvées. Or

[216] LUBIN, Asaf, "The Rights to Privacy and Data Protection Under International Humanitarian Law and Human Rights Law, in: KOLB, Robert, GAGGIOLI, Gloria, KILIBARDA, Pavle, (eds), *Research Handbook on Human Rights and Humanitarian Law: Further Reflections and Perspectives*, Cheltenham : Edward Elgar, 2022, p.463-492

[217] "the work of UNICEF Innovation is essentially about connecting the needs of humans to profit. That is connecting 50 million refugees on the move because of violence with businesses to 'create stronger businesses and help humanity'. Changing the way UNICEF does its business of helping the world's most vulnerable children means pursuing and experimenting with new technology: 'we think that some of the best solutions for kids come from startups and from the space of technology', as Fabian has explained it. UNICEF needs to 'think like businesses and . . . work with startups' FEJERSKOV, Adam, The Global lab : inequality, technology, and the experimental movement, Oxford University Press, 2022, p.48

l'expérimentation constitue ainsi une facette de la notion de « technocolonialisme » forgée par Mirca Madianou, qui lui permet de théoriser la façon dont la numérisation vient réactiver le passé colonial de l'humanitaire. Le technocolonialisme aurait pour Mirca Madianou une triple caractéristique : sa dimension extractive, expérimentale, et son lien avec des technologies de surveillance.

Le numérique humanitaire serait caractérisé par sa dimension extractive. Le déploiement de nouvelles technologies permettrait non seulement de rendre l'aide plus efficace, mais serait producteur de valeur, qui profiterait, selon la chercheuse, aux humanitaires plutôt qu'aux bénéficiaires. Mirca Madianou prend l'exemple des données recueillies via des applications de chatbot destinées aux bénéficiaires. Pour la chercheuse, elles serviraient surtout pour l'ONG à remplir des rapports d'audits en vue de bénéficier de financement de bailleurs. Léa Macias a également démontré comment les résultats d'audits n'étaient pas communiqués aux bénéficiaires. Ces derniers sont donc dépossédés de leurs propres données. Et comme elle le déclare : « C'est de cette dépossession que Couldry et Mejias parlent à travers leur concept de « data colonisalism». La mise en données du camp, et plus largement des activités dites « humanitaires », participe d'une dépossession des données collectées « au Sud », qui sont manipulées, analysées et médiatisées au « Nord », dans des centres de pouvoir que sont les villes comme Genève ou New York. »[218]

Ses réflexions peuvent être rapprochées des travaux de Linnet Taylor, qui mobilise la notion de « data justice ». Cette dernière travaille sur l'ensemble des inégalités et des rapports de pouvoirs associés à la datafication de nos sociétés. En réaction aux formes d'extraction informationnelle, elle défend la nécessité de garantir le partage des bénéfices rattachés aux traitements de données, et une forme d'autonomie dans l'usage des données. Elle déclare ainsi que : « la liberté de contrôler les conditions de son engagement dans les marchés de données est une composante essentielle de tout cadre de justice en matière de données, car elle sous-tend le pouvoir de comprendre et de déterminer sa propre visibilité. »[219]

Ensuite, la deuxième caractéristique propre au technocolonialisme est son lien à des systèmes de classification et de surveillance renforçant des formes de discriminations. Mirka Madianou évoque ici le cas de la biométrie et de son utilisation coloniale. Ici on peut se référer à une série de travaux sur ce sujet, sur la place de la surveillance dans le système colonial, notamment à l'égard d'esclaves, conduits par Simone Browne ou encore Anita Allen [220].

Enfin, une deuxième caractéristique du « technocolonialisme » est sa nature expérimentale. Katja Jacobsen réactualise ce cadre d'analyse en revenant sur l'adoption expérimentale d'un dispositif inédit biométrique de scan d'iris, à la frontière pakistano-afghane. L'entreprise

---

[218] MACIAS, Léa « Usages expérimentaux des nouvelles technologies par l'action humanitaire : un data colonialisme ? », *Hommes & migrations*, 1337 | 2022, http://journals.openedition.org/hommesmigrations/13907

[219] TAYLOR, Linnet," What is data justice? The case for connecting digital rights and freedoms globally", *Big Data & Society*, VL 4, 2017.
"The freedom to control the terms of one's engagement with data markets is an essential component of any data justice framework because it underpins the power to understand and determine one's own visibility. Arguments for the importance of people's autonomy with regard to technology can be found in postcolonial theory, since the way in which data is processed and analysed within national and global data markets positions individuals as subalterns (Spivak, 1988) in relation to those who process their data. They are unable to define for themselves how their data are used, to whom they are resold or the kinds of profiles and interventions those data can enable."

[220] ALLEN, Anita L., « Dismantling the "Black Opticon": Privacy, Race Equity, and Online Data-Protection Reform » *Faculty Scholarship*, 2022, 2803. https://scholarship.law.upenn.edu/faculty_scholarship/2803

Irisguard y a testé en 2002 ses technologies sur des populations vulnérables, sans leur consentement, avant que ses produits soient commercialisés sur les marchés européens. Notre premier chapitre approfondira cette dimension du numérique humanitaire en la reliant au rapprochement opérant entre secteur de la solidarité internationale et secteur privé. On prendra exemple sur plusieurs cas concrets symptomatiques de techniques de gouvernance de population. En l'occurrence on reviendra sur l'expérimentation de dispositifs biométriques, de drones et de données massives, en lien avec l'analyse de mobilités et de flux de population. L'exceptionnalité du régime de suspension du droit en moment de crise humanitaire peut être toutefois interrogée. Pour certains auteurs, c'est plus largement que les entreprises bénéficient d'une dérégulation juridique du secteur du numérique, plus particulièrement étatsunien[221].

Cependant, certains auteurs notent un infléchissement de la dérégulation de l'économie numérique, avec une série de lois notamment européenne visant à contraindre le modèle des GAFAM (RGPD, Digital Markets Act, IA Act, etc.). D'autant que ces dernières essaimeraient à l'échelle internationale du fait du « Brussel Effect ». Le RGPD participe donc de ce mouvement et impose aux organisations une série de mesures d'encadrement. Revenir sur ce règlement consistera en un contrepoint aux analyses de Mirca Madianou, qui n'évoque pas dans le détail ce texte de loi. Notre idée de départ est qu'en raison de l'entrée en vigueur du RGPD, on ne peut plus souscrire à la thèse de l'humanitaire comme laboratoire technologique. Il nous reste à mettre à l'épreuve cette idée lors des lignes qui vont suivre. La partie sera constituée en deux chapitres. Tout d'abord, après être revenue sur la diffusion de l'impératif d'innovation, en lien avec le rapprochement entre le secteur privé et l'humanitaire, on expliquera pourquoi l'humanitaire a pu constituer un laboratoire, en convoquant des cas d'étude concrets ( biométrie, données massive, drone). Puis dans un second chapitre, on verra dans quelle mesure le RGPD participe d'un mouvement de régulation des pratiques numériques. Or pour ce faire, il repose sur une approche par la « compliance » et une méthode de gestion de risque, qui n'est pas sans limites. On explicitera cette dernière et la manière dont elle repose sur une responsabilisation des acteurs et une délégation du contrôle de l'innovation. Et ce alors que le secteur humanitaire manque de moyens humains et financiers relatifs à la protection des données.

## Chapitre 01 — Économie politique du numérique humanitaire : entre innovation et expérimentation

### Introduction de chapitre

[221]SMYRNAIOS, Nikos, *Les gafam contre l'internet. Une économie politique du numérique*, Bry-sur-Marne, ina, 2017
COELHO, Ophélie, *Géopolitique du numérique, l'impérialisme à pas de géants*, Ivry-sur-Seine, Les éditons de l'atelier, 257 p.

Pour le chercheur Tom Scott Smith, il existerait une proximité entre les valeurs défendues par les membres de la Silicon Valley et les partisans d'approches innovantes dans l'humanitaire[222]. Ils partageraient une même foi dans la technologie comme porteuse de solutions pour régler les maux de l'humanité, misère, guerre, catastrophe, etc. Cette proximité s'inscrirait dans un rapprochement plus global entre ONG et secteur privé. Pour ouvrir cette partie, on présentera ce mouvement en deux temps. Un premier moment sera consacré à l'action philanthropique. On décrira ses formes contemporaines en revenant sur les évolutions de l'action philanthropique des membres de la Silicon Valley. Néanmoins, comme on l'a annoncé en introduction, nous ne nous restreignons pas à ces acteurs, car il est nécessaire d'explorer plus largement les multiples interactions pouvant lier entreprises du numérique et ONG : responsabilité sociale d'entreprise, action de type *pro-bono*, sous-traitance, etc. Comme annoncé, le cœur de ce chapitre portera la diffusion au sein de l'humanitaire d'un impératif d'innovation qui va de pair avec sa numérisation et son rapprochement avec le secteur privé. Or des chercheuses comme Kristin Sandvik ou Mirca Madianou préfèrent plutôt parler d'expérimentation que d'innovation. Pour asseoir leur démonstration, ces deux chercheuses se réfèrent à une littérature d'inspiration foucaldienne, consacrée à l'histoire des expérimentations en médecine, dont un aperçu de l'usage de cette notion dans l'humanitaire sera donné dans la seconde partie du chapitre. Puis on discutera la thèse de Mirca Madianou. Pour ce faire, on s'appuiera sur des cas concrets relevant d'une forme de technocolonialisme. Il s'agit de cas caractérisés par une dimension expérimentale et/ou extractive et constituant des formes de gouvernance de population, comme la biométrie, aux drones, aux projets de données massives en lien avec des initiatives qualifiées de « data for good ».

## Section 1 — Secteur privé et humanitaire

La numérisation du secteur de la solidarité internationale renforce le rapprochement préexistant entre entreprises et ONG. Le développement de l'humanitaire a en effet accompagné les différentes évolutions du capitalisme [223] . La diffusion de logiques entrepreneuriales au sein du secteur a été longuement documentée. De nombreuses études ont critiqué l'adoption d'une approche par les résultats, les méthodes du nouveau management public, les formes d'évaluation via des indicateurs quantitatifs[224]. Il faut dire que

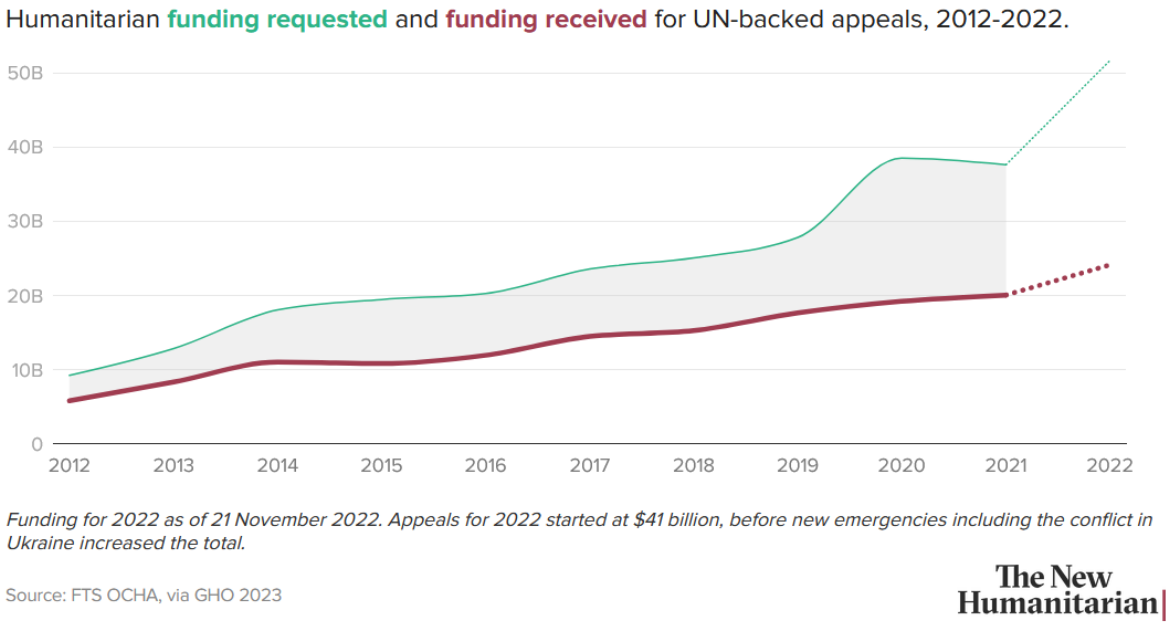
---

[222] "Face à de nouvelles menaces, à des crises de plus grande ampleur et à des déficits de financement et de capacité, l'innovation est présentée comme une question de survie. Sans innovation", lit-on dans un document d'information pour le Sommet humanitaire mondial, "la communauté humanitaire deviendra soit inutile ou trop rigide pour fonctionner efficacement". "With new threats, crises on a bigger scale and shortfalls in funding and capacity, innovation is presented as a matter of survival. 'Without innovation', reads a back-ground paper for the World Humanitarian Summit, 'the humanitarian community will either become irrelevant or too rigid to function effectively."
SCOTT SMITH, Tom, « Humanitarian neophilia: the 'innovation turn' and its implications », *Third World Quarterly*, 37:12,2016 p.2229-2251, DOI: 10.1080/01436597.2016.1176856

[223] comme le rappelle Michael Barnett « L'humanitarisme est donc une manière libérale de comprendre, de catégoriser les problèmes et de les gérer par la suite en imposant des systèmes rationalisés et efficaces visant à garantir et à accroître la vie productive et les possibilités du marché libéral. » Humanitarianism, therefore, is a liberal way of understanding, categorizing problems and subsequently managing them through the imposition of rationalized and efficient systems aimed at securing and increasing productive life and the possibilities of the liberal market." BARNETT, Michael, "Neoliberalism, Philanthropy, and Humanitarianism", in MITCHELL, Katharyne, PALLISTER-WILKINS, Polly, *The Routledge International Handbook of Critical Philanthropy and Humanitarianism,* London: Routledge,2023, 332 p.
DUFFIELD, Mark,"The resilience of the ruins: towards a critique of digital humanitarianism", *Resilience*, 4:3, 2016, p.147-165.
HILHORST, D. "Classical humanitarianism and resilience humanitarianism: making sense of two brands of humanitarian action". *Int J Humanitarian Action* 3, 15, 2018. https://doi.org/10.1186/s41018-018-0043-6

[224] CAZENAVE, Bruno, MORALES, Jeremy, "Against new humanitarian management: Prefigurative accounting in the humanitarian field", *Critical Perspectives on Accounting*, Volume 99, 2024
KRAUSE, Monika,*The good project: humanitarian releif NGOs and the fragmentation of reason*", University of Chicago Press, 2014, 240 p.

ce rapprochement s'inscrit dans un mouvement de fond traversant l'humanitaire depuis les années 1990. Il correspond à la mise en avant de la nécessité d'améliorer la redevabilité du secteur, en réponse à une crise de légitimité de l'aide, à la suite de l'intervention humanitaire désastreuse au Rwanda[225]. Et être redevable de son action, cela signifie également être efficient et innovant, d'autant que les besoins augmentent et le manque de financement se creuse[226]. On assisterait même pour certains acteurs à un « essoufflement du modèle financier » de l'humanitaire.



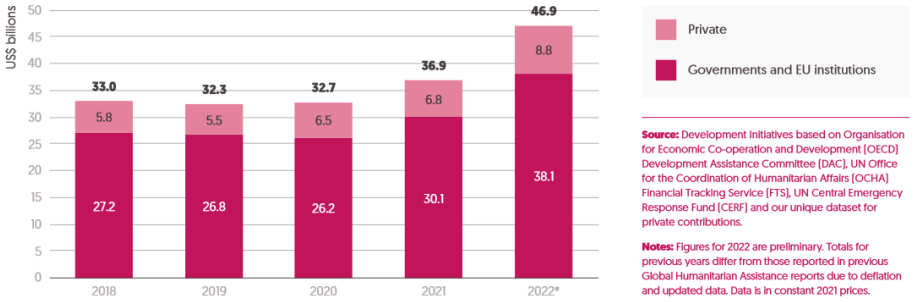

**BESOIN EN FINANCEMENTS ET FINANCEMENTS REÇUS POUR LES CAMPAGNES DE FONDS SOUTENUES PAR LES NATIONS UNIES[227]**

[225] RIEFF, DAVID. "In Rwanda : The Crisis of Humanitarianism." *Salmagundi*, no. 188/189, 2015, p. 417–29. http://www.jstor.org/stable/43942314.
DONNADIEU, Ludovic, « Associations et bailleurs de fonds publics internationaux : concilier les objectifs de redevabilité et d'efficience des projets de solidarité », *Alternatives Humanitaires*, n°24, 2023
https://www.alternatives-humanitaires.org/fr/2023/11/20/associations-et-bailleurs-de-fonds-publics-internationaux-concilier-les-objectifs-de-redevabilite-et-defficience-des-projets-de-solidarite/
GLASMAN, Joel, *Humanitarianism and the Quantification of human needs, minimal humanity*, London, Routledge, Taylor & Francis Group, 274 p.
[226]SCHOEMAKER, Emrys "Digital transformation and the transformation of humanitarian response", Global Policy Journal, Blog, 22/08/2024, https://www.globalpolicyjournal.com/blog/22/08/2024/digital-transformation-and-future-humanitarian-response

[227] LOY, Irwin, ALEXANDER, Jessica, « Key takeaways from the UN's record-breaking tally for 2023 humanitarian needs », *The New humanitarian*, 01/12/2022 https://www.thenewhumanitarian.org/news/2022/12/01/financing-appeals-OCHA-global-humanitarian-overview

De façon plus globale, le montant des financements accordé aurait connu une augmentation notable en 2022, mais sans parvenir à satisfaire les besoins et étant en partie due à un effet de concentration sur la crise ukrainnienne[228].

**Figure 1.3**
International humanitarian assistance from public and private donors grew by over a quarter in 2022
Total international humanitarian assistance, 2018–2022




**Source:** Development Initiatives based on Organisation for Economic Co-operation and Development (OECD) Development Assistance Committee (DAC), UN Office for the Coordination of Humanitarian Affairs (OCHA) Financial Tracking Service (FTS), UN Central Emergency Response Fund (CERF) and our unique dataset for private contributions.

**Notes:** Figures for 2022 are preliminary. Totals for previous years differ from those reported in previous Global Humanitarian Assistance reports due to deflation and updated data. Data is in constant 2021 prices.

## EVOLUTION DES FINANCEMENTS HUMANITAIRES PUBLICS ET PRIVES DE 2018 A 2022[229]

Ainsi, Pierre Micheletti, administrateur de SOS Méditerranée et président d'honneur d'ACF, tire la sonnette d'alarme : « Le modèle de financement visant à répondre à l'ensemble de ces situations est chroniquement et largement déficitaire, car incapable de réunir les 52 milliards de dollars estimés nécessaires en 2022 par les Nations unies. Avec l'aide des ONG, 47 milliards de dollars auront finalement été mobilisés cette année-là, ce qui correspond à une augmentation des dépenses de 27 % depuis 2021. À court terme, l'objectif est donc de sécuriser des dépenses annuelles autour de 50 milliards de dollars et de sauver un système de financement à bout de souffle, sans oublier pour autant la nécessité concomitante d'améliorer la fiabilité de l'analyse des besoins financiers comme l'efficience des organisations de secours. »[230]

Plusieurs facteurs expliquent le manque de financement depuis 2020 environ : le choc économique résultant de la pandémie de Covid19, l'invasion de l'Ukraine par la Russie qui a contribué à l'augmentation de pénuries alimentaires, tout en créant un effet de concentration

---

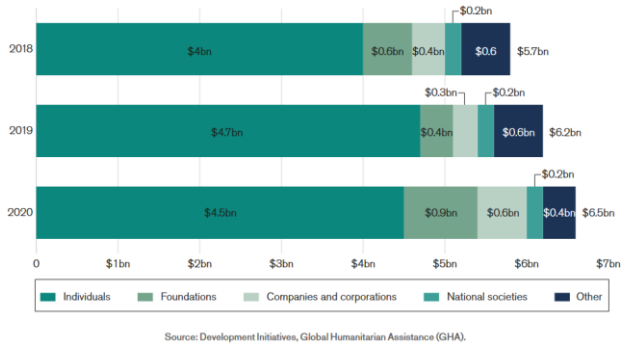
[228] "there is no universal obligation or system for reporting expenditure on international, or indeed domestic, humanitarian assistance. The main reporting platforms for international humanitarian assistance are the Organisation for Economic Co-operation and Development (OECD) Development Assistance Committee (DAC) and the Financial Tracking Service (FTS) of the UN Office for the Coordination of Humanitarian Affairs (OCHA). Increasingly, data on humanitarian activities is also published according to the International Aid Transparency Initiative Standard.1 OECD DAC members are obligated to report their humanitarian assistance to the DAC systems as part of their official development assistance (ODA), in accordance with definitions set out by the DAC.2 Some other governments and most major multilateral organisations, including several of the largest private philanthropic foundations, also voluntarily report to the DAC." "il n'existe pas d'obligation ou de système universel de notification des dépenses liées à l'aide humanitaire internationale, ni même nationale. Les principales plates-formes de notification de l'aide humanitaire internationale sont le Comité d'aide au développement (CAD) de l'Organisation de coopération et de développement économiques (OCDE) et le Service de suivi financier (FTS) du Bureau de la coordination des affaires humanitaires des Nations unies (OCHA). De plus en plus, les données sur les activités humanitaires sont également publiées conformément à la norme de l'Initiative internationale pour la transparence de l'aide.1 Les membres du CAD de l'OCDE sont tenus de déclarer leur aide humanitaire aux systèmes du CAD dans le cadre de leur aide publique au développement (APD), conformément aux définitions établies par le CAD.2 Certains autres gouvernements et la plupart des grandes organisations multilatérales, y compris plusieurs des plus grandes fondations philanthropiques privées, déclarent également volontairement leur aide au CAD. »Development initiatiative, "global humanitarian assistance report 2023", "Global humanitarian assistance report 2023"Development initiatives, 2023https://devinit-prod-static.ams3.cdn.digitaloceanspaces.com/media/documents/GHA2023_Digital_v9.pdf

[229] "Global humanitarian assistance report 2023", Development initiatiative https://devinit-prod-static.ams3.cdn.digitaloceanspaces.com/media/documents/GHA2023_Digital_v9.pdf

[230] MICHELETTI, Pierre, "Il faut un nouveau pacte mondial pour financer l'aide humanitaire internationale", Revue HEM, 05/10/2023, https://www.urd.org/fr/revue_humanitaires/il-faut-un-nouveau-pacte-mondial-pour-financer-laide-humanitaire-internationale/#_ftn16

des financements (en partie privés), ainsi que l'impact du réchauffement climatique, se traduisant par une fréquence accrue de catastrophes et une aggravation de la famine dans le monde, comme l'atteste la sécheresse actuelle frappant la Corne de l'Afrique[231].

Parallèlement, certains bailleurs gouvernementaux ont pu réduire leurs fonds destinés à l'aide humanitaire[232]. Le DFID a baissé ses financements de 0,7 % à 0,5 % du PIB britannique[233], l'Australie et l'Italie de même, la Suède, gros bailleur, a baissé de 15 % son budget alloué à l'aide [234]. Seule la Commission européenne a augmenté son budget de 900 millions à 1,4 milliard d'euros. Notons également que le DFID a fusionné avec le ministère des Affaires étrangères. Cette fusion va de pair avec une baisse de personnels et de financements [235]. Cependant, dans l'ensemble, les financements de bailleurs étatiques restent majoritaires, mais les apports monétaires du secteur privé tendent à augmenter d'année en année, ces derniers englobent aussi les financements de particuliers, qui sont encore en tête, mais les fondations et les entreprises tendent à gagner en importance, comme le montrent les graphiques suivants :




**REPARTITION DES FINANCEMENTS PAR CATEGORIES DE DONATEURS PRIVES [236]**

[231] « La crise de la faim dans la Corne de l'Afrique est loin d'être terminée », WFP, 23/05/2023https://fr.wfp.org/communiques-de-presse/la-crise-de-la-faim-dans-la-corne-de-lafrique-est-loin-detre-terminee

[232] VAN RIJ, Armida, "Beyond the UN: Closing the humanitarian funding gap", *Chathamhouse*, 08/07/2021
LOY,Irwin, « Emergency aid leaders and donors met in Geneva. Here's what happened", *The New humanitarian*, 26/06/2023
https://www.thenewhumanitarian.org/news/2023/06/26/ECOSOC-Emergency-aid-leaders-donors-Geneva#:~:text=of%20the%20phrase%2C%20%E2%80%9C-,You%20can%E2%80%99t%20humanitarian%20your%20way%20out%20of%20this,-%E2%80%9D.

[233] LOFT, Philip, BRIEN, Philip, "UK aid : spending reductions since 2020 and outlook from 2023*", House of commons library*, 30/10/2023
https://researchbriefings.files.parliament.uk/documents/CBP-9224/CBP-9224.pdf

[234] Le Figaro, AFP, « Suède: le nouveau gouvernement fait des coupes drastiques dans l'aide internationale », 8/11/2022, https://www.lefigaro.fr/flash-eco/suede-le-nouveau-gouvernement-fait-des-coupes-drastiques-dans-l-aide-internationale-20221108

[235] WORLEY, William, "Dispute erupts at UK Labour Party conference over restoring DFID", *Devex,* 27 /09/2022https://www.devex.com/news/dispute-erupts-at-uk-labour-party-conference-over-restoring-dfid-104082

[236]« funding for humanitarian response is also raised through national societies at country level, including the Red Cross National Societies. Funding from national societies has remained consistent throughout the past five years at US$0.2 billion. While the exact breakdown is not known, donors to national societies include the private sector, foundations and individual. » , « Le financement de la réponse humanitaire est également assuré par les sociétés nationales au niveau des pays, y compris les sociétés nationales de la Croix-Rouge. Le financement des sociétés nationales est resté constant au cours des cinq dernières années, à hauteur de 0,2 milliard de dollars. Bien que la répartition exacte ne soit pas connue, les donateurs des sociétés nationales comprennent le secteur privé, les fondations et les particuliers. »
Development initiatiative, "global humanitarian assistance report 2022" https://devinit-prod-static.ams3.cdn.digitaloceanspaces.com/media/documents/GHA2022_Digital_v8_DknWCsU.pdf

Les partenariats avec le secteur privé sont alors présentés comme une solution pour pallier le manque de financement des bailleurs gouvernementaux[237]. Cela dit, l'émergence d'une formalisation des partenariats publics/privés au sein du secteur remonte au début des années 2000. Notons la publication en 2008 par l'OCHA de principes directeurs sur ce sujet. Au sein d'ONG ont été ouvertes des unités consacrées à ce type de partenariat[238]. Et au-delà d'un moyen de combler le manque de financement, la coopération avec le secteur privé semble, pour certains acteurs du secteur, constituer une solution pour atteindre les Objectifs de développement durable. L'objectif numéro 17 adopté en 2015 formule en effet explicitement cette nécessité.

Les liens entre le monde de l'entreprise et les ONG prennent plusieurs formes : fourniture de biens ou de services, via des campagnes de collecte de don, via la redistribution de revenus commerciaux, partenariats plus durables, sous-traitance de logistiques ou autre fourniture, tutorat, action pro-bono[239], « *impact investments* », etc. [240]. Dans le cadre d'un mouvement de « moralisation du capitalisme » [241] sont créées des unités de responsabilité sociale d'entreprises et se multiplient de grandes fondations, inscrivant leur action philanthropique dans l'économie globalisée[242]. La philanthropie aurait pris un nouveau visage, que décrivent Charles Bosvieux-Onyekwelu et Valérie Boussard[243]. Le capitalisme « éthique » contemporain ne serait plus l'œuvre d'un individu ou d'une famille, mais d'une entreprise et de « professionnel.les de la vertu ». Les fondations sont touchées par une logique de professionnalisation et par un export de la logique entrepreneuriale en leur sein (on parle de « venture philanthropie »). Les critiques à l'égard de la philanthropie restent cependant inchangées : manque de transparence, passage de la solidarité à la charité, participation à l'affaiblissement de l'État social et contournement des impôts, etc. L'action philanthropique

---

[237] « Renforcer la coopération humanitaire-développement, créer des partenariats public-privé afin de combiner subventions humanitaires, fonds de développement et participation du secteur privé est une voie possible qui permettrait d'établir un mécanisme de financement alternatif pour les crises de longue durée. » MICHELETTI, Pierre, « Il faut un nouveau pacte mondial pour financer l'aide humanitaire internationale », Revue HEM, 05/10/2023, https://www.urd.org/fr/revue_humanitaires/il-faut-un-nouveau-pacte-mondial-pour-financer-laide-humanitaire-internationale/#_ftn16

Ainsi Cyndi McCain directrice exécutive du WFP a déclaré lors d'une réunion au Conseil de Sécurité de l'ONU que : « des choix déchirants et réduire les rations alimentaires pour des millions de personnes vulnérables », avant d'engager d'autres coupes nécessaires. « C'est la nouvelle réalité de la communauté humanitaire, notre nouvelle normalité », a-t-elle déploré. « Et nous en subirons les retombées dans les années à venir ». Plutôt que de se résigner à « l'impuissance face à cette souffrance humaine », la cheffe du PAM a préconisé un meilleur recours au secteur privé, un facteur de croissance économique qui « au cours des 200 dernières années à en grande partie contribué au progrès réalisés dans la réduction de la pauvreté dans le monde ». ONU info, « Il faut repenser le partenariat entre les entreprises privées et l'aide humanitaire, propose le PAM », 14/09/2023 https://news.un.org/fr/story/2023/09/1138582

[238] ALY Heba, "What future for private sector involvement in humanitarianism?", *The New humanitarian*, 23/08/2013 https://www.thenewhumanitarian.org/analysis/2013/08/26/what-future-private-sector-involvement-humanitarianism

[239] Pro bono : l'externalisation des employés, le bénévolat et le mentorat dans les domaines du marketing, des ressources humaines, de la technologie et de la finance.

[240]« Panorama des financements accessibles aux ONG françaises », décembre 2022, Coordination Sud https://www.coordinationsud.org/wp-content/uploads/CSUD-Panorama-des-financements-0123-1.pdf

[241] HOURS, Bernard, « La naturalisation morale du capitalisme », *L'Homme & la société*, n° 216, 2022, p.23

BOSVIEUX-ONYEKWELU Charles, BOUSSARD Valérie, « Moraliser le capitalisme ou capitaliser sur la morale ? », *Actes de la recherche en sciences sociales*, 2022/1 (N° 241), p. 4-15. https://www.cairn.info/revue-actes-de-la-recherche-en-sciences-sociales-2022-1-page-4.htm

LASSUS Renaud, « Chapitre 2. Repenser le capitalisme », dans : LASSUS, Renaud (dir.), *Renouveau de la démocratie en Amérique,* Paris, Odile Jacob, « Hors collection », 2020, p. 107-140. https://www.cairn.info/renouveau-de-la-democratie-en-amerique--9782738152701-page-107.htm

[242] DEZALAY Yves, « Les courtiers de l'international. Héritiers cosmopolites, mercenaires de l'impérialisme et missionnaires de l'universel », *Actes de la recherche en sciences sociales*, 2004/1-2 (n° 151-152), p. 4-35. https://www.cairn.info/revue-actes-de-la-recherche-en-sciences-sociales-2004-1-page-4.htm

[243] MOROZOV, Evgeny, » A l'ère numérique, le capitalisme compatissant », *Le Monde diplomatique*, 02/07/2016,https://blog.mondediplo.net/2016-07-02-A-l-ere-numerique-le-capitalisme-compatissant

serait au service d'une stratégie d'accaparement de marché et en fin de compte servirait de légitimation de l'économie capitaliste et comme instrument de reproduction des élites [244]. Au-delà du gain d'image et réputationnel, la motivation des entreprises serait nourrie par la nécessité de trouver de nouveaux marchés pour soutenir l'économie nationale. Plutôt qu'un intérêt ponctuel d'entreprises considérant l'humanitaire un débouché potentiel. Michael Barnett rappelle qu'il existe un lien fort entre crise (catastrophe naturelle ou guerre) et capitalisme, et se réfère à Naomi Klein, et à ses théories du choc[245], ou Mark Telling et Kathleen Dill[246]. De façon plus générale, les acteurs humanitaires restent partagés quant à ces transformations sectorielles, pouvant porter atteinte aux systèmes de valeurs propres au champ de la solidarité internationale[247]. Plusieurs risques sont pointés : une rationalisation excessive, une perte d'indépendance et de neutralité, voire une instrumentalisation de l'aide, ainsi qu'un risque de perte de réputation et de confiance par des bénéficiaires.

## Section 2 — Secteur privé et numérique humanitaire

Avant d'approfondir notre réflexion sur le rôle et l'implication d'entreprises du secteur technologique dans la numérisation de l'humanitaire, il est nécessaire de brosser un premier tableau général de l'usage des NTIC par les ONG.

Pour rappel, c'est au courant des années 1990 que la numérisation du secteur s'amorce, quand bien même elle reste encore embryonnaire. Certaines ONG restaient alors réticentes à l'égard de l'adoption de nouveaux types d'outils, comme nous le raconte un humanitaire :

« *On avait déjà en 1999 des outils informatiques pour toute notre bureautique, le support opérationnel de nos missions. Seulement, Paris, je veux dire la direction des programmes ne voulait pas nous donner de logiciel de gestion, voilà. C'est intéressant de voir ça, parce que nous… pour nous… on gérait énormément de médicament, sur une grande population, avec énormément d'item, dans une zone de 10 000 habitants, à distribuer dans de nombreux points, et donc du coup c'était très compliqué de gérer un tel flux de médicament, une telle gestion… avec des fiches quoi, parce que [Nom de l'organisation] nous demandait de faire ça avec des fiches papier quoi. (…) C'était un frein à la technologie dans l'humanitaire, ils ne souhaitaient pas une gestion informatisé, numérisée, par principe presque. Pour éviter… c'était en lien avec*

[244] MITCHELL, Katharyne, PALLISTER-WILKINS, Polly, "Monopoly Philanthropy and the Humanitarian New World Order", in : MITCHELL, Katharyne, PALLISTER-WILKINS, Polly, *The Routledge International Handbook of Critical Philanthropy and Humanitarianism*, Routledge,2023, 332 p.

[245] BARNETT, Michael, "Neoliberalism, Philanthropy, and Humanitarianism", in Katharyne Mitchell, Polly Pallister-Wilkins *The Routledge International Handbook of Critical Philanthropy and Humanitarianism Routledge*,2023, 332 p.

[246] PELLING, M., DILL, K., "Disaster politics: tipping points for change in the adaptation of sociopolitical regimes", *Progress in Human Geography*, *34*(1), 2010, p. 21-37. https://doi.org/10.1177/0309132509105004

[247] "there is a culture clash. Humanitarians see themselves as virtuous, value-driven, and ready to sacrifice for others, and they perceive those in the corporate world as the inverse. Because humanity is part of the sacred and money is part of the profane, corporate involvement in humanitarianism potentially pollutes their sacred space."
BARNETT, Michael, "Neoliberalism, Philanthropy, and Humanitarianism", in MITCHELL, Katharyne, PALLISTER-WILKINS, Polly, *The Routledge International Handbook of Critical Philanthropy and Humanitarianism,* London: Routledge,2023, 332 p.

*l'opposition à une professionnalisation des équipes, une gestion plus corporate en fait, des missions. Mais ce n'était pas forcément en lien avec le budget, il y avait de l'argent*. » [248]

Toujours est-il que c'est l'émergence de la téléphonie mobile qui accompagne les premiers pas de la numérisation du secteur. Dans certains pays en voie de développement, notamment en Afrique, il est en effet plus commun d'utiliser des téléphones mobiles — souvent « low cost » et peu sécurisés[249] — que des ordinateurs individuels. Et à côté de grandes activités, rentières et extraverties, que sont les mines et le pétrole, le secteur de la téléphonie mobile est celui qui attire le plus d'investissements étrangers depuis plus d'une décennie. Et les flux d'investissements directs étrangers (IDE) dans le secteur africain des télécommunications auraient, d'après la chercheuse Annie Cheneau-Loquay, à peine souffert de l'éclatement de la bulle internet en 2001.

Pour ces grands groupes internationaux faisant face à une saturation de leurs marchés et à une concurrence exacerbée qui pèse sur les prix et les marges, l'Afrique reste une source de croissance très importante [250] . Ainsi, les grands opérateurs de télécommunication accompagnent en partie la vague de libéralisation des économies africaines, imposées par le FMI dans les années 1990[251].

Au sein de l'action humanitaire, la téléphonie a connu plusieurs applications plus spécifiquement dans le cadre de programmes de santé [252], de réduction de risques de catastrophe ou encore de transferts monétaires. C'est durant cette période que des ONG comme le WFP et l'UNHCR commencent à mettre en avant l'intérêt de programmes de transferts financiers sur mobile. Pour rappel, la Global System for Mobile Communications Mobile money Transfer Initiative a été fondée en 2006. Et le programme kenyan M-PESA (chapeauté par Vodafone et Safaricom au Kenya) date de 2007[253], de surcroit cette même année est nouée une alliance entre les compagnies téléphoniques MTN Uganda, Ericsson, la Global System for Mobile Communications (GSMA) [254] et l'UNHCR. Il s'agit là d'une des premières collaborations entre des opérateurs mobiles et des ONG pour améliorer la

---

[248] Entretien n°95, ONG5, infirmier engagé dans une ONG humanitaire, 26/07/2024

[249] Privacy international, "Buying a smart phone on the cheap? Privacy might be the price you have to pay", 20/09/2019
ODANGA, Madung, AGOSTI, Claudio, ROMANO, Salvatore, "Light on Safety, how TikTok lite sacrifices user protections in the Global majority", Mozilla Foundation, 2024https://privacyinternational.org/long-read/3226/buying-smart-phone-cheap-privacy-might-be-price-you-have-pay https://foundation.mozilla.org/en/campaigns/light-on-safety/ Rapport de Mozilla foundation sur la version "allégée" de Tik Tok, qui serait adapté aux conditions d'usage de pays dits du Sud (smartphones peu puissants, connectivité limitée), mais que serait d'après l'organisation moins sécurisée.

[250] LABEY, Antoine, « Téléphonie mobile: un succès africain », *Inaglobal*, 11/07/2011,https://larevuedesmedias.ina.fr/telephonie-mobile-un-succes-africain
CHENEAU-LOQUAY, Annie, « La révolution des TIC : du téléphone à Internet », *Bulletin de l'Association de géographes français*, 2010, 1, p.15.
CHENEAU-LOQUAY, Annie, LENOBLE-BART, Annie (dir.), *Les médias africains à l'heure du numérique*, L'Harmattan, Netsuds, n° 5, septembre 2010, 133 p.

[251] CHENEAU-LOQUAY, Annie, « L'Afrique au seuil de la révolution des télécomunnications, les grandes tendances de la diffusion des TIC », *Afrique Contemporaine*, 2010/2 (n° 234) p. 93-112

[252] AL DAHDAH, Marine, « Les géants du numérique au chevet de l'Afrique. Le téléphone portable comme nouvel outil de santé globale », *Politique africaine*, 2019/4 (n° 156), p.101-1019, https://www.cairn.info/revue-politique-africaine-2019-4-page-101.htm
AL DAHDAH, Marine, « Between Philanthropy and Big Business: The Rise of mHealth in the Global Health Market », *Development and change*, Volume 53, issue 2, 2022, p. 376-395.

[253] HUTTON BOESER FLOOR GROOTENHUIS, Shawn Boeser, " A Review of Cash Transfer Programming and the CALP Network 2005–2015 and Beyond, 2014", Calp Network. https://www.calpnetwork.org/publication/a-review-of-cash-transfer-programming-and-the-cash-learning-partnership-calp-2005-2015-and-beyond/

[254]La GSMA est une association internationale représentant les intérêts de plus de 750 opérateurs et constructeurs de téléphonie mobile https://www.gsma.com/

connexion d'un camp de réfugiés. En 2008, le WFP, l'United Nations foundation et le Vodafone Group foundation ont annoncé un partenariat visant à développer les services de téléphonie en situation d'urgence[255]. En 2011 le groupe GSMA a établi un partenariat avec l'OCHA. Enfin, en mars 2015, une charte de la connectivité humanitaire est publiée par GSMA, cette dernière a été signée par une centaine d'opérateurs mobiles[256]. La crise migratoire de 2015 renforce la place du mobile dans l'économie numérique humanitaire, d'où la multiplication de partenariats entre l'UNHCR et le GSMA en guise de réponse à ce phénomène[257]. La connectivité et le droit à l'information sont de façon grandissante considérés comme un droit et un besoin pour les bénéficiaires[258].

Ajoutons que les années 2000 voient émerger un autre volet du numérique humanitaire : la cartographie. En effet, à partir de la fin des années 1990 commencent à se démocratiser des logiciels de cartographie, des Systèmes d'information géographique[259], comme ArcGIS. Cette période correspond aussi à l'émergence de l'usage d'imagerie satellitaire par des ONG. Ce rôle de l'imagerie est sans nul doute favorisé par la libéralisation par l'administration américaine du secteur géospatial. Auparavant réservées aux militaires, les images satellites sont en partie déclassifiées au milieu des années 1990 et peuvent être commercialisées[260]. Le secteur spatial était dominé par des agences spatiales étatiques et interétatiques (NASA, ESA, CNES, etc.), des organisations internationales, dont certaines (Intelsat, Eutelsat) sont touchées par un mouvement de privatisation au tournant des années 2000. Mais depuis peu, de nouveaux entrants tentent de s'y faire une place, dont les GAFAM ou une compagnie comme celle d'Elon

---

[255] Vodafone fundation, "Vodafone joins UN Foundation and World Food Programme Goal: to improve communications during humanitarian crises", 2008. https://www.finchandbeak.com/194/vodafone-joins-foundation-and-world-food.htm

[256] https://www.gsma.com/mobilefordevelopment/mobile-for-humanitarian-innovation/humanitarian-connectivity-charter/

[257] GSMA Mobile for humanitarian innovation, "The digital worlds of displacement-affected communities, a cross-context study of how people affected by displacement use mobile phone", October 2022
https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2022/10/DigitalWorldsDAC_R2_WEB.pdf
GSMA, « Evolution des besoins et de l'usage de la connectivité dans les contextes humanitaires », April 2023
https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2023/05/Overview_FRENCH.pdf

[258] « Les populations touchées ont commencé à considérer l'amélioration de l'accès à l'information permise par la connectivité internet, les smartphones et d'autres TIC et infrastructures comme un besoin humanitaire primaire qui est, dans certains cas, plus important pour eux que l'accès aux formes traditionnelles d'assistance telles que la nourriture, l'eau et les abris. Le fait que les populations touchées perçoivent les TIC et les mises à jour de données en temps quasi réel comme des conditions préalables à l'accès aux services marque un tournant important dans l'histoire de l'aide humanitaire. », "Affected populations have begun to identify the enhanced access to information enabled by internet connectivity, smartphones, and other ICTs and infrastructure as a primary humanitarian need that is, in some cases, more important to them than access to traditional forms of assistance such as food, water, and shelter. The phenomena of ICTs and near real-time data updates being perceived by affected populations as necessary prerequisites for accessing services is a significant turning point in the history of humanitarian assistance."
GREENWOOD, Faine, HOWARTH, Caitlin, POOLE ESCUDERO, Danielle, RAYMOND Nathaniel A., and SCARNECCHIA, Daniel, "The Signal Code: A Human Rights Approach to Information During Crisis", 2017, p.1.
https://hhi.harvard.edu/sites/hwpi.harvard.edu/files/humanitarianinitiative/files/signalcode_final.pdf?m=1607469621

[259] « Cartographie humanitaire : nos représentations en question », *Revue humanitaire, enjeux, pratiques, débats*, 32, 2012 https://journals.openedition.org/humanitaire/1289

[260] « Au milieu des années 1990, dans le cadre de la déréglementation, de la privatisation et de la mondialisation des systèmes d'infrastructures critiques (Collier et Lakoff 2006), l'administration Clinton a introduit plusieurs réformes géospatiales cruciales qui ont permis la privatisation et la commercialisation rapides des technologies et des ensembles de données militaires (Verjee 2005). (...) L'année suivante, Clinton a déclassifié les capteurs d'imagerie militaires et autorisé les entreprises privées américaines à lancer et à exploiter des satellites commerciaux à haute résolution. » "In the mid-1990s, as part of the wider de- regulation, privatisation and globalisation of critical infrastructure systems (Collier and Lakoff 2006), the Clinton administration introduced several crucial geospatial reforms that allowed the rapid privatisation and commercialisation of military technologies and data-sets (Verjee 2005). (…) The following year, Clinton declassified military imaging sensors and authorised private US firms to launch and operate commercial high- resolution satellites." DUFFIELD, Mark, "Disaster-Resilience in the Network Age Access-Denial and the Rise of Cyber- Humanitarianism", *Danish Institute for International Studies*, 2013. http://www.jstor.com/stable/resrep13344
BLOM, M, SENNEQUIER, N., « L'espace privatisé : les transitions originales au secteur privé de l'opération de satellites », *Annales des Mines*, 2000. https://www.annales.org/ri/2000/11-2000/blom10-15.pdf
COURDIER, Anne-Sylvie, MANCIAUX, Sébastien, « NewSpace, la nouvelle économie des activités spatiales : enjeux juridiques et éthiques », *LexisNexis*, vol.60, 2023, 220 p.

Musk, Starlink, dédiée la connectivité satellitaire. Or les réseaux de télécommunications employés par les humanitaires reposent en partie sur le maillage satellitaire. Et Elon Musk a pu ainsi mettre en avant son assistance lors de plusieurs crises[261], avec en contrepartie une dépendance naissante d'ONG vis-à-vis de cette compagnie pour assurer leur connectivité[262].

Pour revenir à notre premier sujet sur l'imagerie, en 2000 est conduit au sein de l'unité d'information géographique de l'UNHCR, le projet « Environmental monitoring of Refugee camps Using High Resolution Satellite Image »[263]. Son objectif était de cartographier des camps au Kosovo, au Népal et au Kenya. En 2004, un projet alliant UNOSAT et l'UNHCR permet de repérer les points d'eau afin d'optimiser la localisation des camps[264]. À partir de 2006, Amnesty International commence à se servir d'image satellitaire pour documenter des violations des droits de l'homme[265]. Et parallèlement en 2010 a débuté le Satellite Sentinel Project visant à documenter des crimes de guerre au Sud-Soudan[266]. L'entreprise DigitalGlobe a fourni les images satellites, qui ont été analysées par des spécialistes d'imagerie satellite d'UNOSAT, et par des experts en Droits de l'Homme de l'Harvard Humanitarian Initiative[267]. Le chercheur Nathaniel Raymond en fait partie. Notons qu'il s'est par la suite investi sur les enjeux de protection des données[268].

Enfin, la cartographie de crise a pris un autre tournant en 2010, lors du tremblement de terre haïtien. Des cartographes volontaires ont en effet collecté des données à partir de nombreuses publications postées sur les réseaux sociaux par les victimes de la catastrophe. Ces données ont ensuite aidé à constituer des cartes informant sur les besoins des populations[269]. Cette opération a été coordonnée par Ushaidi, une organisation proposant l'usage de logiciels de cartographie, d'abord impliquée dans la documentation de violences

---

[261] https://www.starlink.com/connecting-the-unconnected
MERAT, Victor, "Elon Musk va offrir une connexion Internet aux organisations humanitaires à Gaza, grâce à Starlink", *Le Figaro*, 28/10/2023 https://www.lefigaro.fr/international/guerre-israel-hamas-musk-appele-a-installer-starlink-au-dessus-de-gaza-prive-d-internet-20231028

[262] MARKS, Simon, "Musk urged to keep starkink active in Sudan for life-saving aid", *Bloomberg*, 13/05/2024 https://www.bloomberg.com/news/articles/2024-05-13/aid-groups-plead-with-elon-musk-to-keep-starlink-on-in-sudan

[263] JOHANNESSEN, Ola, BJORGO, E., ROST, Torbjörn, BOUCHARDY, J.Y., BABIKER, Mohamed, ANDERSEN, Gidske, PAULSEN, S., HAGLUND, A. , ORDENEZ, C. , SANDVEN, Stein. "Environmental monitoring of refugee camps using high-resolution satellite images (EnviRef)", Final Report, 2001.

[264] CLARK, Jennifer, "Une nouvelle technologie prometteuse pour la recherche d'eau au Tchad", UNHCR, 30/07/2004 https://www.unhcr.org/fr-fr/actualites/articles-et-reportages/une-nouvelle-technologie-prometteuse-pour-la-recherche-deau-au

[265] SCOTT, Edwards, KOETTL, Christoph Koettl. "Amnesty international presents ... looking to the sky: monitoring human rights through remote sensing." *Harvard International Review*, vol. 32, no. 4, 2011, pp. 66
AAAS, Human Rights applications of remote sensing, case studies from the geospatial technologies and human rights project, 2014, https://www.aaas.org/sites/default/files/2019-09/Human_Rights_Applications_of_Remote_Sensing_Revised.pdf

[266] WANG,B.Y., RAYMOND, N., GOULD, G., BAKER, I., "Problems from Hell, Solution in the Heavens?: Identifying Obstacles and Opportunities for Employing Geospatial Technologies to Document and Mitigate Mass Atrocities", *Stability: International Journal of Security and Development*, 2013, 2(3) https://doi.org/10.5334/sta.cn
RAYMOND, Nathaniel, et al. "While We Watched: Assessing the Impact of the Satellite Sentinel Project." *Georgetown Journal of International Affairs*, 2013, vol. 14, no. 2, p. 185–91. http://www.jstor.org/stable/43134425.
RAYMOND, Nathaniel A.; CARD, Brittany L.; BAKER, ISAAC, L. "A New Forensics: Developing Standard Remote Sensing Methodologies to Detect and Document Mass Atrocities," *Genocide Studies and Prevention: An International Journal*: Vol. 8: Iss. 3, 2013, p. 33-48.

[267] En 2007, l'Initiative humanitaire de Harvard (HHI) avait été lancée en 2007, il s'agit d'un programme sur la cartographie de crise et l'alerte précoce, dont le but était d'étudier l'application potentielle des NTIC à la réponse humanitaire.

[268] YUMMO WANG Ben,RAYMOND, Nathaniel,GOULD Gabrielle, BAKER Isaac, « Problems from Hell, Solution in the Heavens?: Identifying Obstacles and Opportunities for Employing Geospatial Technologies to Document and Mitigate Mass Atrocities », *Stability: International Journal of Security & Development*, 2(3): 53, p. 1-18, DOI: http://dx.doi.org/10.5334/sta.cn

[269] Patrick Meier relate que plus de 2 millions de Tweets avec le mot « Haiti » ou « croix rouge » ont été publiés dans les 48heures suivant le tremblement de terre, un numéro d'urgence a été mis en place par la compagnie locale, Digicel, qui a envoyé un message d'information à ses abonnés (1,4 millions de personnes). Ces derniers étaient informés de l'opération de cartographie, et un numéro d'urgence, le 4636 permettait de faire remonter des appels d'urgence pour les équipes de « search and rescue » MEIER Patrick, "New information technologies and their impact on the humanitarian sector », *International Review of the Red Cross*, Vol. 93, N° 884,2011, p. 1239-1263.
MEIER, Patrick, *Digital humanitarians : how big data is changing the face of humanitarian response*, London : Routledge, 2015, 259 p.

postélectorales au Kenya en 2008. Son action a fait l'objet d'une couverture médiatique très enthousiaste, qui a loué la nature décentralisée des organisations de volontaires reposant sur l'« intelligence collective », mais leur action dépendant de réseaux comme Twitter et Facebook soulève un certain nombre de questions en matière de protection des données.

Pour résumer, le numérique humanitaire voit donc le jour conjointement à la libéralisation des économies et le développement de partenariats avec des entreprises télécommunications ou spécialisées dans la gestion et la vente d'images satellitaires. Ceci a une conséquente : pour le chercheur Ryan Burns, la numérisation de l'humanitaire va de pair avec un renforcement de l'influence du privé dans le secteur humanitaire. Il décrit ce qui constitue pour lui une forme de cercle vicieux. Tout d'abord, du fait de politiques d'austérité, l'humanitaire manque de financements, le numérique apparait alors comme une solution, en permettant plus d'efficacité, de traçabilité des fonds [270]. Mais l'adoption d'outils technologiques — en accordant une place accrue aux entreprises privées et aux GAFAM — participerait de la managérialisation de l'aide et intensifierait dans le même mouvement l'influence de pratiques et de discours propres aux entreprises [271]. Pour résumer, selon Tom Scott Smith, la numérisation de l'aide s'inscrit dans un triple mouvement. Cette dernière permettrait une mesure, voulue objective, des besoins et permettrait d'assurer une aide souhaitée impartiale[272]. Mais elle participerait de la standardisation de l'aide et irait de pair avec un rapprochement entre ONG et entreprises. À ce stade, il est nécessaire de préciser comment s'opère ce rapprochement. De multiples liens peuvent en effet nouer entreprises et secteur de la solidarité humanitaire : action philanthropique, responsabilité sociale d'entreprise, action de type pro bono, sous-traitance, etc.

## § 1 — Silicon Valley et humanitaire : entre philanthrocapitalisme et longtermisme

Pour commencer, on reviendra sur le rôle de l'action philanthropique dans la numérisation de l'aide et sur l'implication d'acteurs du secteur privé. Notre première section sera donc tout d'abord concentrée sur les GAFAM ainsi que les firmes américaines. Cette modalité d'action est en effet caractéristique de l'écosystème opérant au sein de la Silicon Valley en raison de la tradition américaine de la redistribution privée, et de l'intensité des critiques ciblant les

[270] BURNS, R. "Digital Humanitarianism and the Geospatial Web: Emerging Modes of Mapping and the Transformation of Humanitarian Practices", Doctoral Thesis, Geography, University of Washington, 2015, http://hdl.handle.net/1773/33947
BURNS, Ryan, "New frontiers of philanthro-capitalism : digital technologies and humanitariansm", *Antipode*, vol 51, issue 4, Septembre 2019.
MOROZOV, Evgeny, « À l'ère numérique, le capitalisme compatissant », *Le Monde diplomatique*, 02/07/ 2016,https://blog.mondediplo.net/2016-07-02-A-l-ere-numerique-le-capitalisme-compatissant

[271] SCHLAPFER, Isabelle, "Humanitarian technologies as sociotechnical imaginaries, how multi-national companies impact on the idea of humanitarian action through technologies", Doctoral thesis, School of Arts, Languages and Cultures, University of Manchester, 2020, https://pure.manchester.ac.uk/ws/portalfiles/portal/216123131/FULL_TEXT.PDF
DAHDAH, Al, M., QUET, M.," Between Tech and Trade, the Digital Turn in Development Policies", *Development,*2020, 63, p. 219–225 https://doi.org/10.1057/s41301-020-00272-y
LEFEVRE, Sylvain , LANGEVIN, Marie, « Mastercard, sa fondation et l'inclusion financière : une entreprise philanthropique ? », *Revue française de sociologie*, 2020/4 (Vol. 61), p. 587-615, https://www.cairn.info/revue-francaise-de-sociologie-2020-4-page-587.htm

[272] GLASMAN, Joel, « L'invention de l'impartialité: historique d'un principe humanitaire, entre raison juridique, stratégique et algorithmique », CRASH, MSF, 18/11/2020 https://msf-crash.org/fr/linvention-de-limpartialite-histoire-dun-principe-humanitaire-entre-raisons-juridique-strategique

GAFAM, engendrant un besoin de blanchiment de leur image[273]. La figure de Bill Gates en est un exemple paradigmatique. Sa fondation a fait l'objet de nombreuses enquêtes médiatiques[274] ainsi que de publications universitaires. Mais on dispose de peu d'études quantitatives portant de façon plus générale sur l'action philanthropique de la Silicon Valley. On peut citer le rapport des chercheuses Cortés Culwell et McLeod Grant qui en 2016 faisaient le constat d'une augmentation significative des montants des dons philanthropiques en provenance de la Silicon Valley[275]. Selon les chiffres de l'enquête, les fondations privées auraient crû de 47 % entre 2005 et 2015. Un chiffre de progression qui serait le double de celui de la Californie ou des États-Unis de manière plus générale. En 2015, 1 146 fondations étaient enregistrées à San Mateo et Santa Clara, qui géraient donc 31,6 milliards de fonds [276]. Enfin, 72 % des fondations détenaient 10 millions de dollars de fonds en 2015.

Mais comme on l'a dit à part cette enquête quantitative, il existe peu de données sur les comportements philanthropiques des entrepreneurs du web. On en est réduit donc à égrener les donations de sommes de plusieurs millions de dollars[277].

La Fondation Bill et Melinda Gates domine donc le paysage philanthropique, mais ne doit pas éclipser d'autres fondations. Mark Zuckerberg s'est également investi dans l'action philanthropique. Ses premiers pas sont plutôt classiques : à partir de 2010, il fait une série de dons, notamment dans le secteur éducatif[278] ; en 2015, il fonde la Chan Zuckerberg initiative. Cette fondation porte le nom de sa femme, pédiatre de formation. Elle se concentre sur la recherche médicale et dans l'éducation. On peut également citer le projet FreeBasics : son objectif est de favoriser la connectivité des pays en voie de développement. Enfin Facebook s'implique également — comme on le verra — dans la philanthropie informationnelle via le programme « data for good »[279].

Quant à Google, sa branche philanthropique, ouverte en 2005, se nomme simplement « Google.org ». Et Lary Page avait alors annoncé qu'un pour cent des profits de Google serait dédié à la philanthropie. Mais en 2011, un article du New York Times laissait entendre que les ambitions de Google.org avaient été revues à la baisse. Elles seraient davantage axées sur les problèmes d'ingénierie que le personnel de Google était le mieux à même de résoudre. Depuis lors, l'entreprise semble avoir retrouvé ses marques en s'engageant dans une démarche plus proche de la philanthropie d'entreprise traditionnelle [280]. Ajoutons cependant que Larry Page

---

[273] SMYRNAIOS, Nikos, « La nouvelle bourgeoisie issue de la Silicon Valley », *La Pensée*, 2022, 1 (409), p.31-42
SMYRNAIOS, Nikos, « L'idéologie cynique de la Silicon Valley », *NECTART*, 2023/1 (N° 16), p. 144-153. https://www.cairn.info/revue-nectart-2023-1-page-144.htm

[274] MCGOEY, Linsey, *No Such Thing as a Free Gift: The Gates Foundation and the Price of Philanthropy*, Verso Books, 2014, 304 p.
ASTRUC, Lionel, *L'art de la fausse générosité : la fondation Bill et Melinda Gates*, Actes Sud, 2019, 128 p.

[275] CULWELL CORTES, Alexa, MCLEOD GRANT, Heather, "The giving code, SIlicon Valley nonprofits and philanthropy", *Open/impact*, 2016 https://openimpact.io/wp-content/uploads/2022/05/GivingCode_full_download_102516.pdf

[276] CULWELL CORTES, Alexa, MCLEOD GRANT, Heather, ibid.

[277] BOYER, Clémence, « Ces nouveaux milliardaires philanthropes de la Silicon Valley », *Challenge's,* 15/02/2015https://www.challenges.fr/high-tech/ces-trentenaires-milliardaires-et-nouveaux-donateurs-de-la-silicon-valley_63250

[278] MAC, Ryan, » Mark Zuckerberg finds giving spirit, donates $500 million to Silicon Valley community foundation", *Forbes*, 18/12/2012 https://www.forbes.com/sites/ryanmac/2012/12/18/mark-zuckerberg-finds-giving-spirit-pledges-nearly-500-million-to-silicon-valley-education/?sh=7e37302c4393

[279] VALLELY, Paul, *Philanthropy, from Aristotle to Zuckerberg*, Bloomsbury Publishing, 2020, 768 p.

[280] « En 2011, un article du New York Times laissait entendre que les ambitions de Google.org avaient été revues à la baisse et qu'elles étaient davantage axées sur les problèmes d'ingénierie que le personnel de Google était le mieux à même de résoudre. Depuis, l'entreprise semble

a fait des déclarations plutôt ambiguës sur ce sujet : lors d'une conférence TEDX, il a ainsi affirmé qu'il préférerait faire don de sa fortune à Musk plutôt qu'à des ONG[281].

Au-delà des GAFAM, GSMA, une organisation représentant les intérêts d'entreprises mobiles propose via son programme M4H des bourses pour des projets de téléphonie mobile humanitaire. Mastercard a ainsi versé via sa fondation 1,3 milliard de dons en 2021, et 670 millions à l'ONU[282]. Plus récemment, on aurait assisté à un pic — a priori sans précédent — d'actions philanthropiques durant le Covid19. Les dons concernaient plusieurs domaines — santé globale, éducation, etc. Et à la date du 17 avril 2020, ils atteignaient déjà 7,8 milliards de dollars [283]. À titre comparatif, les flux philanthropiques afférants à l'épidémie d'Ebola de 2014 en Afrique de l'Ouest se chiffraient à 363 millions de dollars sur 6 mois[284]. La Fondation Bill & Melinda Gates représente une part non négligeable des dons, investis dans la recherche de vaccins en finançant par exemple la « Global Alliance for Vaccines and Immunization » (Gavi) [285]. Mais d'autres acteurs de la Silicon Valley ont également mis la main à la poche : en avril 2020, Jeff Bezos avait fait une don de 100 millions de dollars ; en avril 2020, la Michael et Susan Dell foundation avait fait une don de 100 millions en support du Covid 19 ; et Jack Dorsey — le fondateur de Tweeter — a fait un don d'un milliard de dollars [286].

La guerre ukrainienne a représenté un autre moment important en matière de partenariat entre ONG et firmes numériques[287]. Il faut préciser que le soutien américain à l'Ukraine passe de manière plus générale par un appui numérique, en matière d'assistance technique, de fourniture de cloud au gouvernement, d'expertise dans le domaine de la cybersécurité[288]. Et donc également par un appui aux ONG humanitaires, du fait des liens préalables entre le secteur numérique américain et l'Ukraine.

---

avoir retrouvé ses marques en s'engageant dans une démarche plus proche de la philanthropie d'entreprise traditionnelle. Le cas de Google montre à quel point il peut être difficile, même pour des entreprises immensément riches et talentueuses, d'avoir un impact significatif sur le développement mondial". » "A New York Times piece in 2011 suggested that Google.org's ambitions had been scaled way back and were focused more on engineering problems that Google's people were best suited to solving. Since then, the company appears to have found its footing by engaging in something closer to traditional corporate philanthropy. The Google case shows just how hard it can be, even for immensely wealthy and talented companies, to make a significant impact in global development."
KUMAR, Raj, *The Business of changing the world, how billionaires, tech disrupters, and social entrepreneurs are transforming the global aid industry*, Beacon Press, 2019, 256 p.

[281] TEDblog, "Computing is still to clunky: Charlie Rose and Larry Page in conversation", 19/03/2014 https://blog.ted.com/computing-is-still-too-clunky-charlie-rose-and-larry-page-in-conversation/

[282] OECD Library, Mastercard foundation, https://www.oecd-ilibrary.org/sites/9b4d5022-en/index.html?itemId=/content/component/9b4d5022-en

[283] GRABOIS, Andrew, « Global philanthropic response to coronavirus pandemic exceeds $6 billion », *Candid*, 13/11/2020 https://blog.candid.org/post/global-philanthropic-response-to-coronavirus-pandemic-exceeds-6-billion/

[284] PARKS, Dan, "Coronavirus giving tops $1 billion worldwide", *The Chronicle of philanthropy,* 05/03/2020 https://www.philanthropy.com/article/coronavirus-giving-tops-1-billion-worldwide/

[285] LE SAINT, Rozenn, « Recherche contre le Covid-19: la place de Bill Gates et des VIP interroge », *Mediapart*, 28/07/2020 https://www.mediapart.fr/journal/international/280720/recherche-contre-le-covid-19-la-place-de-bill-gates-et-des-vip-interroge

[286] PATIL, Lara, "Disaster philanthropy: Exploring the power and influence of for-profit philanthropy in education development during pandemic times", *International Journal of Educational Development*, Volume 81, 2021.

[287] For many of the companies, including Facebook, Google, Twitter, the war is an opportunity to rehabilitate their reputations after facing questions in recent years over privacy, market dominance and how they spread toxic and divisive content. They have a chance to show they can use their technology for good in a way not seen since the Arab Spring in 2011, when social media connected activists and was cheered as an instrument for democracy.
SATARIANO, Adam, FRENKEL, Sheera, « Ukraine war tests the power of tech giants », *New York Time*, 28/02/2022 https://www.nytimes.com/2022/02/28/technology/ukraine-russia-social-media.html

[288] GUIFFARD, Jonathan, « L'Ukraine, un allié essentiel à la protection du territoire numérique américain », *Hérodote*, 2023/3-4 (N° 190-191), p. 63-77. https://www-cairn-info.ezproxy.utc.fr/revue-herodote-2023-3-page-63.htm

Microsoft

Fin 2022, Microsoft a porté assistance au gouvernement ukrainien en proposant des services de Cloud. La firme a aussi fait une donation de 10 millions de dollars pour des organisations humanitaires sur 430 millions de donations. A été mise en place une équipe d'assistance dédiée à la crise (Microsoft disaster response team) pour allouer de l'aide technique pour des ONG[289].

Google

Google. org (la branche philanthropique de l'entreprise) a fait une donation de 15 millions de dollars, entre autres pour des organisations venant en aide aux réfugiés en Pologne, Slovaquie, Roumanie et Hongrie.

Ont été mises en place des applications d'alerte aux bombardements[290] et d'assistance à la recherche de renseignements concernant les réfugiés. Enfin, sur Google Maps des informations sur des centres d'aide aux réfugiés ont été ajoutées[291].

Amazon

Même Amazon, qui n'est guère investi sur le plan philanthropique[292], a participé à l'effort de guerre[293]. 35 millions de dollars auraient été dédiés à la crise humanitaire ukrainienne.

Amazon a pu livrer 200 000 kits d'hygiène pour des réfugiés, en partenariat avec la firme Clean The world. Des équipes d'Amazon ont créé des hubs logistiques en Europe de l'Est, dans différents pays frontaliers, pour faciliter l'effort logistique humanitaire et distribuer notamment les dons d'Amazon (kit d'hygiène, couvertures, vêtements, etc.) [294].

Un système de traçage des fournitures médicales a été mis en place : » XCH, fournisseur d'outils logiciels d'analyse de contexte et de gestion des incidents pour soutenir les prestataires de soins de santé en temps de crise, a relevé le défi. Avec le soutien d'Amazon Web Services (AWS), XCH a lancé le système d'aide et d'assistance humanitaire ukrainien (…) afin de faciliter les communications nécessaires pour fournir aux intervenants d'urgence des données en temps réel pour la gestion de l'approvisionnement. » [295].

---

[289] BEAUTY, Thalia, Associated Press, "Microsoft tops the list of largest private donors to Ukraine with $430 million - but Google also made the cut", *Fortune*, 23/02/2023, https://fortune.com/europe/2023/02/23/ukraine-war-top-private-donors-microsoft-google/
SMITH, Brad, "Extending our vital technology support for Ukraine" *blog Microsoft*, 11/03/2022
https://blogs.microsoft.com/on-the-issues/2022/11/03/our-tech-support-ukraine/
SMITH, Brad, « Digital technology and the war in Ukraine », *blog Microsoft*, 28/02/2022.
https://blogs.microsoft.com/on-the-issues/2022/02/28/ukraine-russia-digital-war-cyberattacks/

[290] OUEST France, « Guerre en Ukraine. Google lance un système d'alerte aux bombardements pour les Ukrainiens », 14/03/2022
https://www.ouest-france.fr/monde/guerre-en-ukraine/guerre-en-ukraine-google-lance-un-systeme-d-alerte-aux-bombardements-pour-les-ukrainiens-7673976
HIDALGO, Clara, « Guerre en Ukraine: des applications pour prévenir des bombardements russes », *Le Figaro*, 21/10/2022
https://www.lefigaro.fr/international/guerre-en-ukraine-des-applications-pour-prevenir-des-bombardements-russes-20221021

[291] WALKER, Kent, « Notre soutien à l'Ukraine », 10/03/2022
https://blog.google/intl/fr-fr/nouvelles-de-lentreprise/chez-google/notre-soutien-a-l-ukraine/

[292] BEZAT, Jean-Michel, « Philanthropie: « L'engagement de Jeff Bezos, l'un des patrons les plus critiqués des Etats-Unis, est nouveau », *Le Monde,* 16/11/2022 https://www.lemonde.fr/economie/article/2022/11/16/philanthropie-l-engagement-de-jeff-bezos-l-un-des-patrons-les-plus-critiques-des-etats-unis-est-nouveau_6150122_3234.html

[293] "Innovation on the frontline: the impact of technology in Ukraine's humanitarian response", 24/02/2023, https://techtotherescue.prowly.com/231267-innovation-on-the-front-line-the-impact-of-technology-in-ukraines-humanitarian-response
"How tech is supporting Ukraine", US Chamber of Commerce, technology engagement center, 2022 https://americaninnovators.com/news/how-tech-is-supporting-ukraine/

[294] "Amazon launches new humanitarian aid hub in Slovakia to help relief organizations provide faster support to Ukrainian Refugees", AboutAmazon, 22/03/22 https://www.aboutamazon.com/news/operations/amazon-launches-new-humanitarian-aid-hub-in-slovakia-to-help-relief-organizations-provide-faster-support-to-ukrainian-refugees
"How Amazon is assisting in Ukraine", Aboutamazon, 21/06/2023 https://www.aboutamazon.com/news/community/amazons-assistance-in-ukraine

[295] « XCH—a provider of situational awareness and incident management software tools to support health care providers in times of crisis—stepped up to the challenge. With the support of Amazon Web Services (AWS), XCH launched the Ukrainian Humanitarian Aid and Assistance System (UHAAS) to facilitate the communications required to provide emergency responders with real-time data for supply management. "

A été fourni du soutien informatique et de l'assistance technique, en matière de cybersécurité pour des organisations humanitaires, des espaces de stockage de type cloud ont été alloués, ainsi que des dispositifs de connectivité d'urgence et des applications d'information aux réfugiés ont été développé[296].

L'équipe juridique d'Amazon a créé des supports d'information légale destinés à des réfugiés. Ces guides contenaient des indications administratives sur la façon d'obtenir des permis de travail, de trouver des logements, de l'assistance médicale et psychologique, etc.

Facebook

Le programme « data for good » a permis de produire des cartes destinées à Direct Relief pour mieux cibler les communautés et leur apporter une assistance médicale en fonction de leur localisation. Ces informations ont été également utilisées par UNICEF et MSF.

WhatsApp a mis en place une ligne de secours en coopération avec l'OMS.

A été créé un « centre de santé mentale » (*emotional health center*) sur Facebook, regroupant des informations sur ce sujet (gestion de stress, post-trauma, soutien psychologique des enfants durant le conflit). D'autres points d'information, appelés « Community Help », ont relayé des informations de la Croix rouge ou d'organismes de l'ONU portant sur la façon d'obtenir de l'aide d'association et d'organisations humanitaires en Ukraine.

Les équipes de Facebook ont par exemple travaillé en collaboration avec UNICEF et Child Mind Institute pour poster des guides sur Instagram sur la manière de prendre en charge les enfants durant des crises.

Les opérations de collecte de dons ont été facilitées en accordant plus de visibilité à des ONG et à leurs pages de collecte de fonds.

Et enfin, plus classiquement ont été effectués des dons financiers : 15 millions de dollars pour l'Ukraine et les pays voisins, incluant 5 millions de donations directes à des organismes onusiens et à des ONG, comme International Medical Corps, et Internews, ainsi qu'UNICEF. Les 10 millions restants sont destinés aux opérations de collecte de fonds et à la diffusion d'informations humanitaires[297].

Airbnb

Comme a pu le documenter le journaliste Thibault Prevost : « Le 8 mars, la plateforme d'hébergement de particuliers annonce un partenariat avec l'Organisation internationale pour les migrations (OIM)[298]. L'objectif : héberger gratuitement 100 000 Ukrainiens *« à court terme »,* en Pologne, Moldavie, Roumanie, Hongrie et Slovaquie[299]. L'opération sera financée par Airbnb.org, l'ONG d'Airbnb dédiée à l'hébergement d'urgence créée en janvier 2021 et dotée depuis juin d'un fonds de soutien, le Refugee Fund, de 25 millions de dollars[300]. Une semaine plus tard, Airbnb partage un premier bilan : ses fondateurs ont rajouté dix millions de dollars au fonds, 69 000 donateurs ont donné 6,3 millions de dollars

"AWS-Powered app helps healthcare workers track supplies in Ukraine", AboutAmazon, 12/05/2022 https://www.aboutamazon.com/news/aws/aws-powered-app-helps-healthcare-workers-track-supplies-in-ukraine

XCH est une plateforme américaine de gestion de crise

http://xchlive.org/software/

[296] "Amazon continues donating to help Ukrainian refugees", 22/11/2022 https://www.aboutamazon.com/news/community/amazon-continues-donating-to-help-ukrainian-refugees

[297] « Meta's ongoing efforts regarding Russia's invasion of Ukraine », 26/02/2022. https://about.fb.com/news/2022/02/metas-ongoing-efforts-regarding-russias-invasion-of-ukraine/

[298] JENKINS, Cameron, "AIRBNB teaming up with United Nations on shelter for Ukraine refugees", *The Hill*, 03/09/2022 https://thehill.com/policy/international/europe/597464-airbnb-teaming-up-with-united-nations-on-shelter-for-ukraine/

[299] Support for refugees fleeing Ukraine, 28/02/2022 https://news.airbnb.com/help-ukraine/

[300] Airbnb.org launches $25 million fund to support refugees and asylum seekers, 17/06/2021https://news.airbnb.com/refugee-fund/

supplémentaires[301], et plus de 16 700 personnes se sont inscrites [302]sur la version ONG du site pour proposer leurs maisons *« gratuitement ou à tarif réduit. »* [303]

Ainsi, il existerait — dans une certaine mesure — une pression morale au don dans la Silicon Valley. L'acte philanthropique serait constitutif de l'éthos local[304]. Il existe évidemment des exceptions. Jef Bezos n'a ainsi pendant longtemps pas participé à ce mouvement de riches donateurs. Steve Job ne s'est pas investi dans l'action philanthropique. Il a ouvert une fondation en 1986, qu'il a fermée un an après[305]. Ils dérogent ainsi à la « tradition » américaine de l'action philanthropique. Toutefois, l'action des acteurs de la Silicon Valley se situe aussi en rupture avec cet héritage. Comme l'affirme Sean Parker, le créateur milliardaire du service de partage de fichiers musicaux Napster et président fondateur de Facebook, il s'agit de « hacker » la philanthropie [306]. Les articles de journaux relaient cette image d'une philanthropie renouvelée [307]. Premièrement, elle reposerait sur une forme de « technosolutionnisme ». Développer un logiciel — un produit numérique — serait en soi un acte philanthropique, contribuant au bien être humain. Équiper les individus de smartphones, concourir à augmenter la couverture internet — et lancer des projets comme FreeBasic ou Acquila pour Facebook ou Loon pour Google — serait faire preuve de charité[308]. De surcroit, cela suppose appliquer l'esprit managérial à la philanthropie. Ceci serait propre au « philanthrocapitalisme », terme forgé par Matthew Bishop — ex-rédacteur en chef de The Economist — et Michael Green — économiste, haut responsable de l'action internationale

[301] A $10 million matching donation to support refugees fleeing Ukraine, 15/03/2022 https://news.airbnb.com/a-10-million-matching-donation-to-support-refugees-fleeing-ukraine/

[302] "Save the Children Sweden partners with Airbnb.org to provide free housing to refugees fleeing Ukraine",23/03/2022 https://news.airbnb.com/save-the-children-sweden-partners-with-airbnb-org-to-provide-free-housing-in-sweden-to-refugees-fleeing-ukraine-as-part-of-a-safe-start/

[303] PREVOST, Thibault, « Ukraine : Airbnb, votre nouvelle ONG préférée », *Arrêt sur images, Clic gauche*, 27/03/2022. https://www.arretsurimages.net/chroniques/clic-gauche/ukraine-airbnb-votre-nouvelle-ong-preferee

[304] "not being a tech philanthropist can raise serious questions about your status as a Valley god."
APPLEYARD, Bryan, "The charity algorithm : how Silicon Valley philanthropy turned sour", *The Newstatesman*, 16/01/2019. https://www.newstatesman.com/science-tech/2019/01/the-charity-algorithm-how-silicon-valley-philanthropy-turned-sour

[305] SCHLEIFER, Theodore, "Laurene Powell Jobs's charitable group is going to give away almost all of its money", *Vox*, 28/02/2020 https://www.vox.com/recode/2020/2/28/21157049/laurene-powell-jobs-philanthropy-children
ROSS SORKIN, Andrew, "The Mystery of Steve Job's Public Giving", *The New York Times*, 29/08/2011 https://archive.nytimes.com/dealbook.nytimes.com/2011/08/29/the-mystery-of-steve-jobss-public-giving/
WFP, "WFP's plan to support 42 million people on the brink of famine", 03/11/2021.
https://www.wfp.org/stories/wfps-plan-support-42-million-people-brink-famine

[306] « Ces innovateurs de l'internet devraient maintenant utiliser les talents de " disrupteurs " qui les ont rendus riches pour transformer le monde de la philanthropie, selon Sean Parker, le créateur milliardaire du service de partage de fichiers musicaux Napster et président fondateur de Facebook. Il a même inventé un terme pour cela : la "philanthropie hacker". » "These internet innovators should now use the 'disrupter' talents that made them rich to transform the world of philanthropy, argues Sean Parker, the billionaire creator of the music file-sharing service Napster and founding president of Facebook. He has even coined a term for it: 'hacker philanthropy'."
VALLELY, Paul, *Philanthropy, from Aristotle to Zuckerberg*, Bloomsbury Publishing, 2020, 768 p.
CULWELL CORTES, Alexa, MCLEOD GRANT, Heather, "The giving code, Sillicon Valley nonprofits and philanthropy", *Open/impact*, 2016 https://openimpact.io/wp-content/uploads/2022/05/GivingCode_full_download_102516.pdf
to create a "cancer moonshot," taking a decidedly disruptive approach to the medical industry: he's incentivizing top researchers and scientists in the cancer field to share their data and collaborate to find new insights in a way that they have never done before. "

[307] The Economist, "How a tide of tech money is transforming charity", 09/02/2023https://www.economist.com/international/2023/02/09/how-a-tide-of-tech-money-is-transforming-charity
SEMUELS, Alana, "How Silicon Valley has disrupted philanthropy", *The Atlantic*, 25/07/2018 https://www.theatlantic.com/technology/archive/2018/07/how-silicon-valley-has-disrupted-philanthropy/565997/
MANNING, P., BAKER, N. T., STOKESS, P., "The ethical challenge of Big Tech's "disruptive philanthropy"", *International Studies of Management & Organisation,* 50(3), 2020, 271-290
Financial Times, "Zuckerberg disrupts Silicon Valley philanthropy", 03/12/2015 https://www.ft.com/content/0bd8d7c3-0909-41b2-9b76-0bebbaec6082

[308] APPLEYARD, Bryan, "The charity algorithm : how Silicon Valley philanthropy turned sour", *The Newstatesman*, 16/01/2019. https://www.newstatesman.com/science-tech/2019/01/the-charity-algorithm-how-silicon-valley-philanthropy-turned-sour

britannique[309]. Marc Abélès a pu aussi parler de « venture philanthropie »[310]. L'effort de philanthropie serait [311] caractérisé par l'application des méthodes du secteur privé à cette dernière, qui doit être rationnalisée et "optimisée". En outre, la philanthropie ne consisterait pas simplement en des actions ponctuelles, mais en une mise en scène de la figure de l'entrepreneur visionnaire, qui va « solutionner » le problème par une innovation plutôt que par un seul investissement financier. En somme, la philanthropie n'est plus une activité parallèle. Le philanthrope doit adopter un positionnement stratégique, créer de la valeur économique et de la valeur sociale.

Et par conséquent, le philanthrocapitalisme n'implique pas seulement de promouvoir une cause spécifique. Soutenir une entreprise peut être considérée comme un acte philanthropique. D'où la volonté de supporter de futurs entrepreneurs[312]. Cette conception de la philanthropie découlerait du libéralisme d'Adam Smith et de sa conception de l'entreprise comme étant « naturellement » productrice de bénéfice et de bien-être pour la société. Et certaines fondations peuvent faire des dons à des entreprises. La Fondation Gates octroie un montant croissant de dons à des entreprises privées : Vodafone et Mastercard, deux firmes jouant un rôle important dans le secteur humanitaire, principalement en soutenant des programmes de cash transfert.

On a commencé à voir qu'est défendue l'idée que la philanthropie des acteurs de la Silicon Valley serait — dans une certaine mesure — marquée par des traits spécifiques. Elle est souhaitée plus professionnalisée, plus attentive aux résultats et doit pouvoir être évaluée. Certes, il s'agit plutôt de continuité que de réelle rupture avec la philanthropie traditionnelle. Et sans doute la volonté de quantifier l'acte du don s'inscrit dans l'idéologie néolibérale[313]. Mais la philanthropie américaine a récemment adopté un visage présenté comme nouveau, celui de l'altruisme efficace.

---

[309] BISHOP, Matthew, GREEN, Michael, *Philanthrocapitalism, how the rich can save the world*, A.&C Black, 2008, 304 p.

[310] ABELES Marc, « Nouvelles approches du don dans la silicon valley », *Revue du MAUSS*, 2003/1 (nº 21), p. 179-197. DOI : 10.3917/rdm.021.0179. URL : https://www.cairn.info/revue-du-mauss-2003-1-page-179.htm

[311]« cet intérêt pour les résultats et les mesures n'est pas exclusif à la philanthropie de la Silicon Valley - il est peut-être simplement plus marqué ici. De nombreuses organisations nationales axées sur l'évaluation des organisations à but non lucratif répondent à la nouvelle demande de données des donateurs en créant des initiatives visant à aider les organisations à but non lucratif à être plus claires sur leurs indicateurs et à suivre leurs résultats », "this focus on outcomes and metrics is not exclusive to Silicon Valley philanthropy—it is perhaps just heightened here. Many national organizations focused on nonprofit ratings are responding to new donor demand for data by creating initiatives to help nonprofits be clearer about their metrics and track their outcomes"CULWELL CORTES, Alexa, MCLEOD GRANT, Heather, "The giving code, SIlicon Valley nonprofits and philanthropy", Open/impact, 2016 https://openimpact.io/wp-content/uploads/2022/05/GivingCode_full_download_102516.pdf

[312] « Si les jeunes sont malades et mal nourris, leur corps et leur cerveau ne se développeront jamais complètement. S'ils ne reçoivent pas une bonne éducation, leur esprit restera en sommeil. S'ils n'ont pas accès aux opportunités économiques, ils ne pourront pas atteindre leurs objectifs", a déclaré M. Gates, selon les remarques préparées publiées sur son blog, Gates Notes. Les jeunes peuvent apporter des solutions innovantes aux problèmes de la région - plus que les personnes plus âgées - "parce qu'ils ne sont pas enfermés dans les limites du passé", a déclaré M. Gates. Il a fait allusion à sa propre expérience et à celle d'autres grands acteurs de la technologie pour illustrer le pouvoir des jeunes esprits. »,"If young people are sick and malnourished, their bodies and their brains will never fully develop. If they are not educated well, their minds will lie dormant. If they do not have access to economic opportunities, they will not be able to achieve their goals," Gates said, according to prepared remarks posted to his blog, Gates Notes. Young people can provide innovative solutions to the region's problems — more than older people — "because they are not locked in by the limits of the past," Gates said. He alluded to his own experience and that of other big players in tech to illustrate the power of young minds."
SIRTORI-CORTINA, Daniela, "Bill Gates: To boost Africa, Invest in its Youth", *Forbes*, 18/07/2016 https://www.forbes.com/sites/danielasirtori/2016/07/18/bill-gates-to-fix-africa-invest-in-its-youth/?sh=5cd3c41e3574
CHENEY,Catherine, "Exclusive: Eric and Wendy Schmidt commit $1B to support young talent", *Devex*, 13/11/2019 https://www.devex.com/news/exclusive-eric-and-wendy-schmidt-commit-1b-to-support-young-talent-95994

[313] DIDIER, Emmanuel, BRUNO, Isabelle*, Benchmarking, l'Etat sous pression statistique*, Paris: éditions la Découverte, Zones, 2013, 250 p.

Ce mouvement est représenté entre autres par William MackAskill et Toby Ord, deux philosophes en éthique rattachés à l'université d'Oxford. Ces derniers ont construit un cadre théorique visant à orienter l'action philanthropique et à définir la façon de s'engager pour le bien commun[314]. L'action charitable est en effet caractérisée par le principe de maximisation et d'efficacité — dans la lignée de l'éthique utilitariste[315]. Et la façon d'agir le plus efficacement est de pouvoir donner le plus possible et donc gagner le plus possible, en travaillant non pas dans l'action humanitaire, mais dans d'autres secteurs plus rémunérateurs[316].

Un deuxième aspect de ce système de pensée est l'efficience du don. Les approches utilitaristes reposent sur des stratégies de maximisation du bien : l'objectif est de faire le maximum de bien avec le minimum de moyen[317]. Le fait de sélectionner une cause, et d'être efficace dans l'action menée est a priori défendable. D'ailleurs, le principe de triage et de redevabilité est — bien que critiqué — déjà présent dans l'action humanitaire[318]. A priori, la logique égalitariste prévalente au sein de l'aide va de pair avec un refus des pratiques de triage, au regard de l'inconditionnalité de l'aide et du respect de la vie humaine. Mais dans les faits, ces pratiques sont courantes. Le chercheur Alex de Waal évoque même la dureté des choix des ONG, contraintes de hiérarchiser les vies à sauver face à l'impossibilité de les sauver toutes, du fait de contraintes de moyens, financiers et logistiques[319].

Mais d'un point de vue éthique, il existe une incompatibilité profonde entre la logique humanitaire et l'altruisme efficace. L'un est conséquentialiste - l'action est évaluée par son résultat, l'autre est ontologique- l'action est évaluée en fonction de son intentionnalité[320].

---

[314] SRINIVASAN, Amia, "Stop the Robot Apocalypse", *London Review of book,* Vol.37, n° 18, 2015

[315] Au-delà de l'utilitarisme « classique » de Bentham, William Mackaskill s'inspire directement de Peter Singer, un philosophe éthique — c'est la lecture d'un de ses articles, Famine, affluence and morality qui aurait été fondateur de son système de pensée singulier. Selon Peter Singer, l'acte charitable le plus grand doit être pensé sans empathie de façon rationnelle, ce calcul implique de ne pas simplement prendre en compte ce qui nous affecte directement, mais d'inclure dans nos actions les drames plus lointains, — malgré leur distance — dans l'évaluation éthique d'une action. Ainsi, pour Peter Singer donner à une association qui réalise les rêves d'enfants gravement malades américains n'est pas un acte efficace, les enfants sont condamnés à mourir, il parait alors préférable de faire un don pour des une association qui lutte contre la malaria en Afrique, à somme égale, cela permettrait de sauver trois enfants.
SINGER, Peter, "Famine, affluence, and morality", Philosoph and public affairs, vol.1, n°3, 1972, p.229-243

[316]TODD, Benajamin, MacAskill, William, "Is it ever Ok to take a harmful Job in order to do more good? An in-depth analysis", June 2017, https://80000hours.org/articles/harmful-career/

[317] William MacAskill se réfère à différentes métriques de l'efficacité, notamment le « Quality Adjusted life years », soit la mesure des années de bonne qualité de vie. Le rapport entre l'investissement (en argent, en temps) et le résultat sur en matière de santé (ou d'autre critère) de la vie d'un individu. Ce rapport doit être le plus équilibré possible afin d'être considéré comme une action efficace. Les Qaly s'inscrivent dans la médecine de la preuve, d'abord testée dans le système de santé britannique, il permet d'évaluer le rapport cout/efficacité des médicament, s'inscrivant dans la politique de privatisation du système sanitaire britannique

[318] « Les décideurs politiques, les prestataires de soins de santé et les distributeurs d'aide étrangère - tous ces organismes décident régulièrement de ce qu'il faut faire en pesant les intérêts des différentes parties les unes par rapport aux autres. Dans une salle d'urgence, les infirmières chargées du triage évaluent les patients qui arrivent : Elles traitent immédiatement ceux dont la vie est en danger, font attendre ceux dont l'état est modéré et renvoient chez eux ceux qui souffrent d'affections mineures. Elles agissent ainsi pour que les médecins ne perdent pas un temps précieux à soigner des toux et des rhumes alors qu'ils pourraient s'occuper de crises cardiaques". " Policymakers, healthcare providers, and distributors of foreign aid—all these bodies regularly decide what to do by weighing the interests of different parties against each other. In the emergency room, nurses in triage assess incoming patients: They treat those with life-threatening conditions immediately, make those with moderate conditions wait, and send those with minor ailments home. The reason they do this is so that doctors don't use up valuable time treating coughs and colds when they could be treating heart attacks."
MACASKILL, W. "What Charity Navigator Gets Wrong About Effective Altruism". *Stanford Social Innovation Review*. 2013, https://doi.org/10.48558/71AW-PN62
William Macaskill oublie simplement de préciser que la question du « triage » des malades est une question hautement débattue, qui ne peut être simplifiée à l'extrême comme il le fait.
LACHENAL Guillaume, LEFEVE Céline, NGUYEN Vinh-Kim, « Le triage en médecine, une routine d'exception », *Les Cahiers du Centre Georges Canguilhem*, 2014/1 (N° 6), p. 1-25, https://www.cairn.info/revue-les-cahiers-du-centre-georges-canguilhem-2014-1-page-1.htm

[319] DE WAAL, Alex," The humanitarians' tragedy: escapable and inescapable cruelties", *Disasters*, 2010, vol. 34, p. S130-S137.

[320] KLEIN-KELL, Nathalie, "More humanitarian accountability, less humanitarian access? Alternative ideas on accountability for protection activities in conflict settings", *international Review of the Red Cross*, 2018, 100 (1-2-3),p. 287–313.

Une organisation phare de l'altruisme efficace, l'Open Philanthropy, n'a qu'un programme de don à destination d'une ONG américaine, l'International Rescue Committee. Il en est de même pour les listes d'organisations qu'il est recommandé de soutenir : MSF ou le CICR n'en font pas partie. Et William MacAskill a pu critiquer l'action d'urgence, du fait de son incapacité supposée à mettre un terme à la pauvreté ou à des problèmes globaux[321].

Ajoutons que l'altruisme efficace n'est pas qu'un simple système de pensée. Ce mouvement est structuré autour d'organisations et des fonds financiers qui gèrent des ressources non négligeables. Ces dernières visent à orienter les financements privés selon les principes de l'altruisme efficace. La plus importante est peut-être l'Open Philanthropy, dirigée par le co-fondateur de Facebook : Dustin Aaron Moskovitz [322] . Les critères de don d'Open Philanthropy sont les suivants : l'impact du financement, sa traçabilité, le fait d'être une cause « négligée » par le grand public. Cela dit, l'Open Philanthropy a pu faire des dons à la Fondation Gates et l'USAID a pu recevoir 45 millions de dollars pour son unité d'innovation[323].

De surcroit, l'organisation bénéficiant d'une bonne partie des fonds de l'Open Philanthropy est Givewell, fondée en 2007 par deux anciens traders, Elie Hassenfeld et Holden Karnofvsky. Ces derniers [324] ont en tête l'idée d'appliquer les méthodes d'analyse financière à l'action philanthropique. GiveWell favorise donc un certain type d'ONG professionnalisée adoptant un fonctionnement et les codes proches du milieu dans lequel baignent les entrepreneurs[325]. Ainsi, une organisation fortement soutenue par GiveWell est Givedirectly. L'objectif de Givedirectly consiste à délivrer des programmes de cash transfert à des villages nigériens sélectionnés au préalable[326]. Différents acteurs de la Silicon Valley ont aussi financé le projet. C'est le cas de la fondation Google.org, de Jack Dorsay et Elon Musk ; ainsi que l'ex-compagne de Jef Bezos, Sam Bankman-Fried, ou encore le fondateur d'Ethereum, Vitalik Buterin[327].

---

[321] « Contrairement, par exemple, aux dons en faveur de la santé mondiale, qui aident les plus démunis sur la voie de la prospérité, les dons en faveur des camps de réfugiés sont un exemple de charité non durable. Le conflit n'étant pas près de s'achever, les camps de réfugiés syriens devront être soutenus peut-être pendant des décennies. Nous ne voulons pas nous retrouver dans une situation comme celle des Sud-Soudanais au Kenya ou en Ouganda, où les enfants risquent de passer toute leur vie dans des camps. », "Unlike, for example, donations to global health, which help the extremely poor on the road to prosperity, donating to refugee camps is an example of unsustainable charity. With no end to the conflict in sight, Syrian refugee camps would need to be supported perhaps for decades. We do not want to end up with a situation like the South Sudanese in Kenya or Uganda, where children may spend their whole lives in camps."
MACASKILL, William, "What is the most effective way to help refugees?", *The Guardian*, 04/09/2015
https://www.theguardian.com/commentisfree/2015/sep/04/help-refugees-donations-government-political-action

[322] https://www.openphilanthropy.org/research/our-progress-in-2022-and-plans-for-2023/

[323] BEASLEY, Stephanie, "Gates, Usaid among Open Philanthropy's $150M regrant contest winner", *Devex*, 12/01/2023, https://www.devex.com/news/gates-usaid-among-open-philanthropy-s-150m-regrant-contest-winners-104743

[324] BEASLEY, Stephanie, CHENEY, Catherine," Tech entrepreneurs bring new approaches, challenges to philanthropy", *Devex*,24/01/2022 https://www.devex.com/news/tech-entrepreneurs-bring-new-approaches-challenges-to-philanthropy-102174

[325] BEASLEY, Stephanie, CHENEY, Catherine, "Tech entrepreneurs bring new approaches, challenges to philanthropy", *Devex*, 24/01/2022 https://www.devex.com/news/tech-entrepreneurs-bring-new-approaches-challenges-to-philanthropy-102174
"Malaria Consortium's scientific, data-driven style of addressing malaria prevention aligns with the thinking of many tech philanthropists, said Chief Executive Charles Nelson." BEASLEY, Stephanie, CHENEY, Catherine, ibid.
ADAMS, Carol, CRARY, Alice, GRUEN, Lori, *The good it promises, the harm it does, critical essays on effective altruism*, Oxford University Press, 2023,280 p.

[326] JAGER, Anton, ZAMORA, Daniel, « Pourquoi la Silicon Valley défend le revenu universel », *Le Vent se lève,* 02/08/2023https://lvsl.fr/pourquoi-la-silicon-valley-defend-le-revenu-universel/

[327]SANDLER, Racher, "Why billionaires like Mackenzie Scott and Jack Dorsey are donating millions to this nonprofit that gives cash to the poor", *Forbes*, 22/07/2022
https://www.forbes.com/sites/rachelsandler/2022/07/22/why-billionaires-like-mackenzie-scott-and-jack-dorsey-are-donating-millions-to-this-nonprofit-that-gives-cash-to-the-poor/?sh=2e5f2d46dc7f

On a commencé à entrapercevoir qu'il existe une jonction entre l'élite technologique et l'altruisme efficace. Il est question de liens bien plus profonds qu'une affinité intellectuelle[328]. Pour rappel, l'Open Philanthropie a été créée par Dustin Moskowitz (le cofondateur de Facebook)[329]. L'équipe dirigeante de Givewell comportait Chris Hugues, un des co-fondateurs de l'entreprise dirigée par Mark Zuckerberg[330]. En outre, le fondateur d'Instagram, Mike Krieger a vanté l'action de Give Well et de l'Open Philanthropie, et a annoncé un partenariat avec cet organisme, avec un fonds de 750 000 euros[331]. Enfin, Sam Bankman Fried a largement soutenu le mouvement de l'altruisme efficace. Il a créé un fonds d'investissement Future Fund (FTX), destiné au développement de l'IA. Il est composé d'individus rattachés à l'altruisme efficace, et à des instituts de recherche d'Oxford. On y trouve ainsi Nick Beckstead, Leopold Aschenbrenner, un économiste affilié au Global Priorities institute d'Oxford, employé maintenant chez OpenAI, Avital Balwit, chercheuse employée par le Future Of humanity Institute[332]. Ce dernier a été rattaché à l'Universtité d'Oxford, jusqu'à ce qu'en avril 2024, l'université ferme le laboratoire de Nick Bostrom[333]. Ajoutons enfin qu'il existe également des liens forts entre altruisme efficace et acteurs travaillant sur l'IA. Le journaliste Brendan Bordelon — spécialisé sur le lobbying des acteurs des nouvelles technologies au sein des institutions états-uniennes — a enquêté sur le soutien apporté par l'Open Philanthropy à des acteurs influents de l'IA cherchant à mettre ce sujet à l'agenda de l'administration américaine[334].

Mais comment se fait-il que des partisans de l'altruisme efficace soient si impliqués dans l'étude des risques posés par l'IA ? Il faut comprendre que ce courant de pensée comprend une branche reliant l'éthique utilitariste et les recherches sur la quantification du don à une mouvance qualifiée de « longtermiste ». De façon globale, le longtermisme divise les altruistes efficaces, mais s'y rattache des auteurs importants de ce courant comme Toby Ord[335] et William McAskill qui ont publié des ouvrages reprenant ces idées[336]. Ce courant peut être résumé en une phrase : ses adeptes prescrivent de ne pas simplement chercher à « sauver »

---

[328] PIPER, Kelsey, "The giving pledge, the campaign to change billionaire philanthropy, explained", *Vox*, 10/07/2019. https://www.vox.com/future-perfect/2019/7/10/18693578/gates-buffett-giving-pledge-billionaire-philanthropyhttps://www.vox.com/future-perfect/2019/7/10/18693578/gates-buffett-giving-pledge-billionaire-philanthropy
CHENEY, Catherine, "How the Chan Zuckerberg Initiative could influence global giving", *Devex*, 03/12/2015 https://www.devex.com/news/how-the-chan-zuckerberg-initiative-could-influence-global-giving-87437
KIM, Whizy, "What does it mean to give away a $118 billion fortune?", *Vox*, 27/01/2023 https://www.vox.com/recode/23553730/jeff-bezos-philanthropy-giving-pledge-charity

[329] https://www.openphilanthropy.org/about/team/dustin-moskovitz/

[330] https://www.givedirectly.org/chris-hughes-joins-the-board/

[331] KARNOFSKY, Holden, Co-funding partnership with Kaitlyn Trigger and Mike Krieger, Open philanthropy, 23/04/2015 https://www.openphilanthropy.org/research/co-funding-partnership-with-kaitlyn-trigger-and-mike-krieger/

[332] SANDHU, Martin, "Effective altruism was the favoured creed of Sam Bankman-Fried.Can it survive his fall?", *Financial Times,* 29/12/2023, https://www.ft.com/content/128f3a15-b048-4741-b3e0-61c9346c390b

[333] ROBINS-EARLY, Nick, "Oxford shuts down institute run by Elon Musk-backed philosopher", *The Guardian*, 20/04/2024 https://www.theguardian.com/technology/2024/apr/19/oxford-future-of-humanity-institute-closes
SALIOU , Mathilde, "L'Université d'Oxford ferme le Future of Humanity Institute dirigé par Nick Bostrom", *Next*, 23/04/2024 https://next.ink/135101/luniversite-doxford-ferme-le-future-of-humanity-institute-dirige-par-nick-bostrom/

[334] BORDELON, Brendan, "How a billionaire-backed network of AI advisers took over Washington", *Politico*, 13/10/2023 https://www.politico.com/news/2023/10/13/open-philanthropy-funding-ai-policy-00121362

[335] ORD, Toby, *The Precipice: Existential Risk and the Future of Humanity*, London : Bloomsbury Publishing Plc, 2020, 480 p.

[336] GLEIBERMAN, Mollie, "Effective altruism, doing transhumanism better", working paper, 2023, *Insitute of development policy*, University of Antwerp https://www.openphilanthropy.org/grants/uc-berkeley-ai-safety-research-2018/

son prochain, mais l'humanité future[337]. Le longtermisme invite à pondérer ses choix actuels au regard de leurs impacts dans un avenir lointain. Sachant que le futur est envisagé à très grande échelle (jusqu'à plusieurs milliers, voire plusieurs millions d'années) [338]. On se situe loin du nexus humanitaire/développement qui cherche à dépasser la vocation strictement urgentiste de l'aide. L'objectif du longtermisme est de lutter contre l'extinction de l'espèce humaine menacée par des risques existentiels[339]. Ces derniers selon Nick Bostrom désignent initialement tout événement empêchant la réalisation d'une « post-humanité » ou selon une redéfinition récente, tout ce qui empêcherait d'atteindre une forme de « maturité technologique ». Et le longtermisme vise à maximiser la productivité économique et réaliser un potentiel humain [340]. Sont considérés comme « risque existentiel » les usages incontrôlés des technologies (nanotech, géo-ingénierie, IA), ou des pandémies. Le longtermisme a une vision ambiguë de la technologie, à la fois dystopique et enchantée. Les nouvelles technologies peuvent conduire à l'extinction de l'humanité, tout comme la sauver[341]. En outre, il parait évident que l'idéologie longtermiste s'oppose à l'esprit humanitaire et à l'action d'urgence, en réaction aux catastrophes présentes[342]. Ainsi pour Hilary Greaves et Nick Beckstead, il faut réduire les engagements ayant pour objectif l'amélioration des conditions de vie des plus pauvres (qui relève du court-termisme)[343]. Il s'agit au contraire de se concentrer sur l'avenir et des enjeux à plus long terme. Cette vision est formalisée par des chercheurs au sein du Future of humanity institute et du Global Priorities institute, d'Oxford. Ajoutons que ce mouvement de pensée oriente en partie l'action philanthropique de certains membres de la

[337] « Nous utiliserons le terme "humain" pour désigner à la fois l'Homo sapiens et tout descendant ayant un statut moral au moins comparable au nôtre, même si ces descendants sont d'une espèce différente et même s'ils ne sont pas biologiques. », « we will use "human" to refer both to Homo sapiens and to whatever descendants with a least comparable moral status we may have, even if those descendants are a different species, and even if they are non-biological. »
MACASKILL, William, GREAVES, Hilary, The case for strong longtermism", Global Priorities Institute, GPI Working Paper, n°5-2021

[338] « il pourrait s'écouler encore un milliard d'années avant que la Terre ne soit plus habitable pour l'homme, et des trillions d'années avant la dernière formation conventionnelle d'étoiles. », "there could be a further one billion years until the Earth is no longer habitable for human, and trillions of years until the last conventional star formation." MACASKILL, William, GREAVES, Hilary, "The case for strong longtermism", Global Priorities Institute, GPI Working Paper, n°5-2021

[339] TARSNEY, C. "The epistemic challenge to longtermism". *Synthese,*2023*,* 201, 195. https://doi.org/10.1007/s11229-023-04153-y

[340]BOSTROM, Nick, "Existential risk prevention as global priority", Global Policy, vol 4, issue 1, 2013, p.15-31
https://existential-risk.com/concept#:~:text=An%20existential%20risk%20is%20one,future%20development%20(Bostrom%202002).
BOSTROM, « L'hypothèse du monde vulnérable », *Future of humanity institute*, 2019 https://www.researchgate.net/profile/Daniel-Vuignier/publication/362317767_L'hypothese_du_monde_vulnerable/links/62e2f0db3c0ea8788764389c/Lhypothese-du-monde-vulnerable.pdf
READ, Rupert, Climate crisis and the dangers of tech obsesed "long termism", The conversation, 17/02/2022
https://theconversation.com/climate-crisis-and-the-dangers-of-tech-obsessed-long-termism-176951
TORRES, Emile, What "longtermims" gets wrong about climate change", *Bulletin of the atomic scientist*, 22/11/2022
https://thebulletin.org/2022/11/what-longtermism-gets-wrong-about-climate-change/
UNDRR, "Existential risk and rapid technological change, advancing risk informed development", 2023, https://www.undrr.org/media/86500/download?startDownload=true

[341] DE FILIPPI, Fabrizio, ROMELE Alberto, « Libérer l'éthique avec Nick Bostrom et Toby Ord ? (ou comment j'ai appris à ne plus m'en faire et à aimer la technique) », in : DAMOUR Franck, DEPREZ Stanislas, ROMELE Alberto (dir.), *Le transhumanisme : une anthologie* Paris : Hermann philosophie , 2020, p. 199-212. https://www.cairn.info/le-transhumanisme-une-anthologie--9791037005717-page-199.htm

[342] TORRES, P, Emile, "Understanding "longtermism": Why this suddenly influential philosophy is so toxic", *Salon,* 20/08/2022
https://www.salon.com/2022/08/20/understanding-longtermism-why-this-suddenly-influential-philosophy-is-so/
TORRES,P. Emile, « Against longtermism, » *Aeon*, 19/10/2021
https://aeon.co/essays/why-longtermism-is-the-worlds-most-dangerous-secular-credo

[343] Nick Beckstead a pu déclarer dans sa thèse : « Pour prendre un autre exemple, sauver des vies dans les pays pauvres peut avoir des effets d'entraînement nettement moins importants que sauver et améliorer des vies dans les pays riches. Pourquoi ?Les pays riches sont beaucoup plus innovants et leurs travailleurs sont beaucoup plus productifs sur le plan économique. Selon les normes ordinaires, du moins selon les normes humanitaires éclairées ordinaires, sauver et améliorer des vies dans les pays riches est à peu près aussi important que sauver et améliorer des vies dans les pays riches, à condition que les vies soient améliorées dans des proportions à peu près comparables. Mais il me semble désormais plus plausible que sauver une vie dans un pays riche soit nettement plus important que sauver une vie dans un pays pauvre, toutes choses égales par ailleurs. »
BECKSTEAD, Nicholas, "On the overwhelming importance of shaping the far future", Phd thesis, philosophy, New Jersey. 2013, P.11
https://rucore.libraries.rutgers.edu/rutgers-lib/40469/PDF/1/play/

Silicon Valley. Les liens entre les entrepreneurs du numérique et le longtermismes sont évidents[344]. Et Elon Musk, Peter Thiel, Jeff Bezos ou Jaan Tallinn, le fondateur de Skype[345], ont pu soutenir cette cause[346]. Tout ceci semble indiquer une divergence certaine entre l'action humanitaire et la conception du risque et des catastrophes pouvant se répandre dans le milieu californien. Le longtermisme serait symptomatique de la droitisation de certains acteurs de la Silicon Valley[347], qui a longtemps été identifiée comme un milieu « libéral » d'un point de vue des valeurs sociétales[348]. Cependant, il serait tout à fait erroné de se focaliser trop fortement sur l'altruisme efficace et le longtermisme. Ce cadre idéologique infuse certes le milieu, mais il divise également la Silicon Valley. Sans doute, une part des acteurs de la Silicon Valley est plutôt préoccupé par les catastrophes futures et finance des projets de recherches centrés sur la gestion de risque sur le long terme. Mais il reste des acteurs intéressés par les catastrophes présentes et défendant l'innovation comme solution pour porter secours aux victimes de crises contemporaines. En outre, tous les acteurs n'ont pas un positionnement univoque. Ainsi, Elon Musk a pu se dire proche du longtermisme, tout en soutenant (dans une certaine mesure) le secteur humanitaire en proposant des services de connectivité destinés à pallier la fracture numérique dans des zones reculées ou lors de crises[349]. Et si l'IA est considérée comme un risque pour l'humanité et comme un facteur potentiel de catastrophe futures, Google et Microsoft expérimentent des projets d'IA destinés aux acteurs humanitaires et aux crises contemporaines.

On a brossé un premier tableau de l'action philanthropique des GAFAM, qui s'investissent à la fois dans l'éducation, la santé, l'écologie, l'action d'urgence, etc. Mais dans le même temps, ils sont également influencés par des systèmes de pensée les éloignant de l'action d'urgence. Cela dit, il existe aussi d'autres modalités de relations et de partenariats entre « acteurs de la tech » et organisations humanitaires.

---

[344] PICARD, Alexandre, « Derrière l'IA, le retour d'utopies technologiques », *Le Monde,* 14/06/2023 https://www.lemonde.fr/economie/article/2023/06/13/derriere-l-ia-le-retour-d-utopies-technologiques_6177367_3234.html
SCHWARZ, Elke, "The escatological ambiguity of silicon valley longtermim, Centre For apocalyptic & post apocalyptic studies", 13/12/2022 https://www.youtube.com/watch?v=m_AdfjXRprM

[345] Il a participé à la création d'un centre pour l'étude des risques existentiels, Le Future of humanity, dirigé par Nick Bostrom.

[346] KARF, Dave, « 6. L'apocalypse remplace l'utopie », *Tèque*, 2024/1 (N° 4), p. 131-147 https://www.cairn.info/revue-teque-2024-1-page-131.htm

[347]ALEXANDRE, Olivier, "La Tech sur les chemins d'une contre-révolution", *AOC*, 09/07/2024 https://aoc.media/analyse/2024/07/09/la-tech-sur-les-chemins-dune-contre-revolution/
KANDEL, Maya, "La droite tech contre la démocratie : comment la Silicon Valley s'est radicalisée", *Mediapart*, 17/03/2024 https://www.mediapart.fr/journal/international/170324/la-droite-tech-contre-la-democratie-comment-la-silicon-valley-s-est-radicalisee

[348] « Le mélange d'opinions de ce groupe, conservateur sur le plan de la régulation de l'économie, très libéral sur les questions sociétales et favorable à la mondialisation, est unique dans la sociologie politique étatsunienne. Le fait que cette fraction particulière de l'élite se dit très concernée par le « bien-être » de la société peut en partie refléter leurs origines dans des strates moins solidement établies et, de leur point de vue, plus méritocratiques. Ainsi, l'élite technologique semble être caractérisée par une représentation de soi et du monde et une idéologie propre, relativement cohérente et largement partagée au sein du groupe, qui en fait une fraction distincte de la grande bourgeoisie. Cependant, bien qu'elles montrent un attachement à des idéaux tels que la démocratie et l'égalité, ces personnes se permettent de contourner les processus démocratiques et d'exercer une influence disproportionnée sur le jeu politique en finançant massivement les causes qui leur sont chères et en « capturant » une partie conséquente des médias et des institutions au service de leurs intérêts. » SMYRNAIOS Nikos, « La nouvelle bourgeoisie issue de la Silicon Valley », *La Pensée*, 2022/1 (N° 409), p. 31-42. https://www-cairn-info.ezproxy.utc.fr/revue-la-pensee-2022-1-page-31.htm

[349] "Starlink mobility : how starlink is improving emergency services globally", The clarus network group, 03/10/ 2023https://www.youtube.com/watch?v=ULsnvpWShFs

## § 2 — Secteur privé et numérique humanitaire : connectivité de crise et migrant connecté

Les GAFAM ne sont pas les seuls acteurs du secteur privé à investir l'humanitaire, un bon nombre d'entreprise privées nouent des partenariats avec les ONG. Ceux-ci sont difficiles à cartographier, du fait de leur absence de transparence, comme le surligne Giulio Coppi "Il y a un manque de transparence dans la façon dont les deux secteurs coopèrent, il y a beaucoup de plates-formes pour faciliter les réunions. Et encore quels sont les résultats, les risques associés, où en est la passation des marchés ? Faites-vous une DPIA ? Pourquoi n'est-elle pas publique ?"[350]

On peut en donner un premier aperçu, sans rentrer dans le détail de la structuration du marché du « numérique humanitaire ». Tout d'abord, des entreprises peuvent simplement fournir aux ONG du matériel et des logiciels, des solutions d'application mobile, des solutions cloud, de l'infrastructure réseau, etc. Ajoutons que le soutien à la connectivité de crise s'est fait via divers partenariats avec le secteur privé, avec des entreprises comme Salesforce ou Cisco [351]. Ils ont pris la forme d'ONG dédiées (comme NETHOPE), un cluster (comme l'« Emergency telecommunication cluster »), des consortiums privés (comme la GSMA[352]). La connectivité de crise est l'objet d'un écosystème d'acteurs divers[353], allant de compagnies locales à des firmes privées de télécommunication satellitaire[354]. Mais ce créneau est déjà bien structuré au sein de l'humanitaire, autour d'un consortium comme le « Crisis connectivity Charter », chapeauté par l'« Emergency telecom Cluster ». Il inclut différents opérateurs satellitaires et associations comme la « Global Satellite operators associations ».

Les GAFAM ont tenté d'investir le créneau de la connectivité de crise. Des projets comme Google Loon, Free Basic et Discover de Facebook ont été largement couverts par la presse. Starlink a fait parler d'elle récemment, lorsque Elon Musk a proposé d'« offrir » de la connectivité aux humanitaires à Gaza. Mais d'après Giullio Coppi leur succès serait mitigé en ce domaine. Et ils ne doivent pas totalement éclipser l'implication d'autres acteurs, plus modestes, agissant à plus petite échelle. Giullio Coppi rappelle ainsi que « dans l'ensemble, malgré leurs ressources et leur portée, l'intervention d'entreprises numériques mondiales telles que Meta et Alphabet semble avoir échoué à fournir des solutions innovantes pour combler le fossé numérique humanitaire en matière de connectivité, en mettant l'accent sur le fait que les organisations de base sont souvent des champions méconnus dans l'effort de

[350] there is a lack of transparency in the way the two sector are cooperating, there is a lot of plateform for faciliting meeting. AND still what the outcoumes are, the risk associated,where are the procurement? DO you do a DPIA? Why is not public? « "Humanitarian tech unveiled : from principles to corporate capture", Socio-techs, November 2023

[351] https://www.cisco.com/c/en/us/about/csr/impact/cisco-crisis-response.html#~transforming-lives

[352] La GSMA est une association internationale représentant les intérêts de plus de 750 opérateurs et constructeurs de téléphonie mobile https://www.gsma.com/

[353]MARCHAND Eleanor, « Internet governance in displacement", UNHCR Innovation Service, 2020 https://www.unhcr.org/innovation/wp-content/uploads/2020/04/Internet-Governance-in-Displacement_WEB042020.pdf

[354] MERAT, Victor, » Elon Musk va offrir une connexion Internet aux organisations humanitaires à Gaza, grâce à Starlink », *Le Figaro*, 28/10/2023https://www.lefigaro.fr/international/guerre-israel-hamas-musk-appele-a-installer-starlink-au-dessus-de-gaza-prive-d-internet-20231028

connectivité humanitaire, comme l'a montré au Yémen le chapitre local de l'Internet Society en collaboration avec la Fondation Watan pour le développement et la formation. »[355]

Sur ce sujet, l'organisation NetHope occupe une place important. Elle a joué un rôle clef dans la numérisation du secteur humanitaire en tant qu'intermédiaire entre des ONG et des entreprises[356]. Cette organisation a été créée en 2001, par un ingénieur, Dipak Basu de Cisco et par Edward G. Happ, « chief information officer » de Save the Children[357]. Parmi de nombreux sponsors, on peut trouver CISCO, Salesforce, mais surtout Microsoft, principal financier de l'organisation. Le mandat initial est la connectivité et la lutte contre la fracture numérique dans les pays du Sud, et ce, en développant les partenariats entre ONG et secteur privé[358]. Nethope a par la suite élargi son mandat et soutient la transition numérique des ONG.

À côté de la connectivité de crise, les dispositifs d'identité sont aussi une porte d'entrée intéressante pour les entreprises. Mastercard s'investit fortement dans ce qui constitue un marché humanitaire de l'identité numérique, notamment sur le domaine financier. Le marché de la biométrie et de l'identité est florissant et dépasse le seul domaine de l'humanitaire. Il concerne d'autres secteurs comme celui de la gestion des élections, notamment en Afrique[359].Il est très présent dans les acteurs liés aux politiques de développements, comme

---

[355] "Overall, despite their resources and outreach, the intervention of global digital companies such as Meta and Alphabet seem to have failed in providing innovative solutions to fill the humanitarian digital gap in connectivity, focusing al grassroots organizations are often unsung champions in the humanitarian connectivity effort, as shown in Yemen by the Internet Society local chapter in collaboration with the Watan Foundation for Development and Training. "COPPI, Giulio, "Mapping Humanitarian Tech, Exposing protection gaps in digital transformation programmes", *AccessNow*, February 2024https://www.accessnow.org/wp-content/uploads/2024/02/Mapping-humanitarian-tech-February-2024.pdf

[356] Cette organisation fondée en 2001 vise à améliorer les capacités de connectivité des ONG, mais organise également des événements, conférences ou webinaires sur le sujet des NTIC humanitaires. Nethope a eu comme partenaire, Accenture, Amazon, Cisco, Facebook, Google, Microsoft, Oracle NetSuite.

« Et le fait d'avoir des liens étroits avec NetHope nous permet de faire remonter rapidement les problèmes de mise en œuvre des subventions qui se posent par l'intermédiaire des responsables de NetHope. NetHope peut nous aider à concentrer nos efforts sur le rôle que Microsoft peut/doit jouer. Par exemple, NetHope s'efforce de renforcer les capacités en matière de TIC afin de pouvoir utiliser toute la technologie offerte à ces organisations. Dans ce cas, Microsoft s'associe à une ONG technologique au profit d'organisations humanitaires internationales non techniques qui accomplissent un travail remarquable. » "And having close ties to NetHope allows us to quickly escalate any grant implementation issues that arise via NetHope leadership. NetHope can help focus our efforts on the role Microsoft can/should play. For example, NetHope is trying to go into ICT capacity building so they can use all of the technology that is being donated to these organizations. In this case Microsoft is partnering with a technology NGO to benefit non-techy international relief agencies doing great work." FARMER, S. Benjamin, JOHNSON, Eric, "Nethope- Collaborating for the future of relief and development", Tuck School of Business at Dartmouth—Glassmeyer/McNamee Center for Digital Strategies

[357]« L'objectif est de mettre en œuvre l'expertise technologique et les moyens financiers nécessaires à la création d'une filière mondiale. Nous recherchons une grande entreprise qui relèvera ce défi et qui, en partenariat avec SAVE the Children, s'appropriera le processus de réalisation. », « The goal is to bring to bear the technology expertise and financial means to create a global pipeline. We are seeking a major corporate player to step up to this challenge and, working in partnership with SAVE the Children, own the process for making it happen. » HAPP, Edward, "Wiring the Global Village IT in a Developing World", Sudan project posting on globalgiving.com, September 10, 2004.

[358]« C'était comme une start-up dans un garage. Grâce au financement et au soutien technique de Cisco, NetHope a développé et déployé les deux premières générations du kit de secours en réseau. Ces versions initiales ont été conçues pour fournir aux travailleurs sur le terrain des moyens de communication de données. « "It was like a start-up in a garage. With funding and engineering support from Cisco, NetHope worked to develop and deploy the first two generations of the Network Relief Kit. These initial versions were designed to provide field workers with data communications."

NEE, Eric, Q&A : William Brindley, *Philanthropy news Digest*, 17/03/2009, https://philanthropynewsdigest.org/features/ssir-pnd/q-a-william-brindley

FARMER, S. Benjamin, JOHNSON, Eric, Nethope- Collaborating for the future of relief and development, Tuck School of Business at Dartmouth—Glassmeyer/McNamee Center for Digital Strategies

BRINDLEY, William, "The humanitarian Technologist's Dilemma", *Stanford Social Innovation Review*, 14/12/2012https://ssir.org/articles/entry/the_humanitarian_technologists_dilemma#

[359] DEBOS Marielle, DESGRANGES Guillaume, « L'invention d'un marché : économie politique de la biométrie électorale en Afrique », *Critique internationale*, 2023 / 1 (N° 98), p.117-139. DOI : https://doi-org.ezproxy.utc.fr/10.3917/crii.098.0117. URL : https://shs-cairn-info.ezproxy.utc.fr/article/CRII_098_0117?lang=fr

Boubacar Diagana. "Les recensements biométriques des populations en Afrique.", 7 juillet 2019, *Cahiers Costech*, numéro 3. URL https://www.costech.utc.fr/CahiersCostech/spip.php?article81

la Banque Mondiale, certaines instances de l'ONU. IL est relayé au sein de certaines ONG humanitaires, défendant l'adoption de dispositifs d'identité « fonctionnels », dans le cadre projets de cash transferts, mais aussi dans le cadre de l'enregistrement des réfugiés dans des camps ( et impliquant le HCR). L'usage croissant de dispositifs biométriques va de pair avec l'entrée dans le secteur d'une d'entreprises comme Thales et Accenture, mais aussi des firmes, majoritairement américaines ou britanniques, moins médiatisées comme C&C Technology Group,Warwick Warp ltd,Green Bit, GenKey, IriTech – Irishield,SmartSensors, Cognitec, IrisGuard [360].

Ajoutons que certaines entreprises peuvent également procurer aux ONG des produits voulus adaptés au contexte humanitaire. Mastercard a par exemple proposé un nouveau service aux ONG : une plateforme de paiement en ligne prenant en compte les contraintes de crise (comme le manque de connectivité) [361]. Ce type de produit est souvent développé au cours de « hackathon », des événements ayant connu un certain succès lors de la « crise migratoire » de 2015[362].

En outre, des actions *pro bono* peuvent être menées, soit le fait pour le secteur privé de contribuer par des services gratuits, plutôt que sur le plan matériel. Cela comprend, entre autres, l'externalisation d'employés, le bénévolat et le mentorat dans les domaines du marketing, des ressources humaines, de la technologie et de la finance. Ainsi en 1999, Marc Benioff le directeur de Saleforce aurait lancé le modèle 1-1-1 : 1 % des revenus de l'entreprise, 1 % du temps des employés et 1 % de leurs produits sont destinés aux ONG[363]. L'entreprise peut de cette façon offrir un transfert de compétences. Google[364] et Microsoft proposent de mettre à disposition pour une durée déterminée ses « data scientists » pour l'entrainement d'IA[365]. Le Cyberpeace Institute propose des partenariats pro bono[366] entre entreprises de cybersécurité et ONG afin de renforcer leurs compétences en la matière. En outre, les entreprises de la Silicon Valley peuvent être des « data stewart »[367]. Comme on le verra, des partenariats se multiplient avec comme objectif de favoriser l'accès d'ONG à des données détenues par des entreprises privées[368].

---

[360] COPPI, Giulio, "mapping humanitarian tech exposing protection gaps in digital transformation programmes", AccessNow, February 2024https://www.accessnow.org/wp-content/uploads/2024/02/Mapping-humanitarian-tech-February-2024.pdf

[361]MasterCard, « MasterCard Transforms Aid Distribution », 24/09/ 2015, https://newsroom.mastercard.com/press-releases/mastercard-transforms-aid-distribution/

[362] DIMINESCU, Dana, NICOLOSI, Guido, « Les risques et les opportunités de la migration "connectée" », *Socio-anthropologie*, 40 | 2019, http://journals.openedition.org/socio-anthropologie/6330

ORSINI, Alexis, « Applis, startups, hackathons... quand la tech vient en aide aux migrants », *Numerama*, 18/12/2017, https://www.numerama.com/politique/312100-applis-startups-hackathons-quand-la-tech-vient-en-aide-aux-migrants.html

DHUNNA AHMAD, Tazeen, "Refugee hackathons and 3D printing : apps for the world's displaced people", *The Guardian*, 20/06/2017

[363] Colin, CHRIS, « the Gospel of wealth according to Marc Benioff », Wired, 11/12/2019 https://www.wired.com/story/gospel-of-wealth-according-to-marc-benioff/

[364] https://ai.google/social-good/

[365] SMITH Brad, « Using AI to help save lives », Microsoft blog, 24/09/2018. https://blogs.microsoft.com/on-the-issues/2018/09/24/using-ai-to-help-save-lives/ Microsoft lance en 2018 en partenariat avec l'ONU un projet d'Intelligence artificielle destiné aux ONG humanitaires, dirigé par John Kahan.

[366] Pro bono : l'externalisation des employés, le bénévolat et le mentorat dans les domaines du marketing, des ressources humaines, de la technologie et de la finance.

[367] BERENS Jos, "Private Sector Data for Humanitarian Response: Closing the Gaps", *Bloombergneweconomy* https://www.bloombergneweconomy.com/news/private-sector-data-for-humanitarian-response/

OLSEN FOSSELI, Elisabeth, "Humanitarian organisation use of pro bono services in innovation projects, KPMG Norway", october 2020

[368] Facebook lance en 2017 un projet dirigé par Laura McGorman nommé « dataforgood » destiné à fournir à la société civiles des services en matière de gestion de données (cartographie, sondage, « insights »).

L'implication des entreprises numériques dans l'humanitaire s'inscrit dans l'histoire longue du secteur, mais leur action a connu trois pics : la crise migratoire de 2015, la crise de la Covid 19, qui aurait représenté un bond en avant dans la transformation numérique des organisations, ainsi qu'en termes d'investissement en infrastructure[369], ainsi que le conflit russo-ukrainien, du moins à partir de 2022, comme on a pu le voir précédemment au sujet des GAFAM.

Pour mettre l'accent sur 2015, cette période coïncide donc avec un accroissement d'applications numériques, exploitant l'imaginaire du « migrant connecté »[370]. Ces dernières sont destinées à soutenir les réfugiés en leur fournissant des informations utiles en matière de santé, d'infrastructures d'accueil. Il s'agit d'initiatives parfois sans lendemain, constituant un cimetière numérique d'applications non utilisées[371]. Pour structurer ces dernières ont été aussi créées des organisations comme Techfugee — destinée à l'innovation — ou Singa. Cette dernière cherche à favoriser l'intégration des réfugiés via le numérique, selon un idéal du « réfugié entrepreneur » [372]. Ce rapprochement avec le secteur privé a pu causer des inquiétudes au sein du secteur, notamment en raison de la crainte qu'il ne remette en cause les principes humanitaires[373], mais il va aussi de pair avec la diffusion d'un certain nombre de valeurs, dont celle de l'innovation.

## Section 3 - Innovation et expérimentation humanitaire

### § 1 — L'impératif d'innovation

Notre hypothèse initiale est que la numérisation de l'humanitaire va de pair avec la diffusion de pratiques et de discours managériaux ainsi qu'une injonction à l'innovation. Cela dit, dans un certain sens, les humanitaires ont toujours été contraints d'innover, de trouver des solutions pour — dans des contextes volatiles et d'urgence — maintenir la continuité de l'aide. Ainsi selon Ben Ramalingam : « L'acheminement de l'aide humanitaire peut se heurter à des défis logistiques et bureaucratiques imprévisibles à chaque étape, et des adaptations sont nécessaires simplement pour fournir l'assistance. De ce point de vue, on peut dire que les agences humanitaires innovent quotidiennement. » [374] D'ailleurs, l'action humanitaire consiste à procurer des biens et des services à des communautés affectées par des catastrophes, des crises et conflits. Pour monter un camp, il est nécessaire de disposer de tentes, de sanitaires, de s'assurer de l'approvisionnement en eau, etc. Les ONG ont alors développé des « produits » innovants dédiés spécifiquement aux bénéficiaires, que ce soit le

[369] « Digital progress and trend report 2023 », World Bank https://www.banquemondiale.org/fr/news/press-release/2024/03/05/accelerated-by-covid-and-ai-global-digital-landscape-remains-uneven
[370] DIMINESCU, Dana, « Le Migrant connecté : pour un manifeste épistémologique », *Migrations/Société*, vol.17, n° 102, p. 275-292
[371] BENTON, Meghan, "Digital litter: the downside of using technology to help refugees", *Migration policy Institute*, 19/06/2019 https://www.migrationpolicy.org/article/digital-litter-downside-using-technology-help-refugees
[372] GLENNIE, Alex, BENTON, Meghan, « Digital humanitarianism : how tech entrepreneurs are supporting refugee integration », Migration Policy Institute Octobre 2016
https://www.migrationpolicy.org/sites/default/files/publications/TCM-Asylum-Benton-FINAL.pdf
[373] SMITH, Trevor, RAYMOND, Nathaniel, "The problem with emergency aid's growing reliance on corporations",The New humanitarian, 15/04/2024, https://www.thenewhumanitarian.org/opinion/2024/04/15/problem-emergency-aids-growing-reliance-corporations
[374] « Delivery of humanitarian aid can encounter unpredictable logistical and bureaucratic challenges at every step, and adaptations are needed simply to deliver assistance. From this perspective, humanitarian agencies could be said to innovate on a daily basis. »

biscuit d'Oxfam Plumpy'nut dans les années 1980, ou plus récemment des systèmes de filtration d'eau (Drinking Straw)[375].

Ainsi, des chercheurs comme Peter Redfield, Thom Scott-Smith ou Jamie Cross ont décrit, en s'appuyant sur les travaux de Michel Callon, la vie d'objets humanitaires. Ils ont analysé les efforts des organisations pour concevoir des produits, les récits élaborés à leur sujet, ainsi que l'imaginaire social et politique qu'ils véhiculent[376]. Et de fait, les humanitaires ont toujours eu un certain gout pour la nouveauté, comme a pu l'écrire Thom Scott Smith, qui fait part d'une véritable « néophilie » au sein du secteur. Mais un tournant se serait opéré à la fin des années 2000, plus précisément en 2009 avec la publication par Ben Ramalingam d'un rapport sur le sujet pour l'ANALP (acronyme d'« Active Learning Netwfork for accountability and performance »). Le rapport enjoignait le secteur à embrasser une approche « innovante » définie par un large spectre d'actions : « le rôle de la technologie, des produits et des processus provenant d'autres secteurs, les nouvelles formes de partenariat et l'utilisation des idées et des capacités d'adaptation des personnes touchées par la crise. »[377] Il est d'emblée surligné que le terme d'innovation n'est pas synonyme d'invention : « elle n'implique pas nécessairement la création de quelque chose d'absolument nouveau, mais prend souvent la forme d'une adaptation à un contexte différent. (…) Une solution n'a pas besoin d'un seuil de changement particulier pour être qualifiée d'innovation. Elle peut "changer la donne" en ayant un degré élevé de progrès technologique et d'impact sur le marché, ou elle peut être incrémentale. »[378]

Plus précisément, le rapport de Ben Ramalingam constitue en une description des méthodes de management dédiées à la création d'un environnement favorable à l'innovation. Il est — à l'instar de partisans de l'innovation — convaincu de l'aspect sclérosé du secteur humanitaire, sa bureaucratisation empêchant la réactivité et la souplesse d'action nécessaire face aux crises. A cela s'ajoute une critique du secteur public jugé aussi manquant d'« agilité ». Pour Ben Ramalingam les solutions innovantes viennent du secteur privé. Il n'est plus question de bricolage et de solution de rechange en contexte d'urgence, il s'agit d'innover comme une entreprise et de calquer la démarche entrepreneuriale : « Pour créer quelque chose de

---

[375] CROMBE, Xavier, "Independence and Innovation, looking beyond the magic of Words", *Crash*, 2008. https://msf-crash.org/sites/default/files/2017-05/9404-xc-2008-independence-and-innovation-looking-beyond-the-magic-of-words-_uk-art-p.4_.pdf

[376] CROSS, Jamie, "The 100th object : solar lighting technology and humanitarian good", *Journal of Material culture*, 0(0) 1-21, 2013 https://pure.manchester.ac.uk/ws/portalfiles/portal/216123131/FULL_TEXT.PDF

SCOTT-SMITH, Tom, "The fetishism of humanitarian objects and the management of malnutrition in emergencies", *Third World Quarterly*, 34:5,2013, p. 913-928, 10.1080/01436597.2013.800749

« En d'autres termes, ce concept de "néophilie humanitaire" ne décrit pas seulement les principales caractéristiques du mouvement de l'innovation (sa recherche de nouvelles technologies et de nouvelles opportunités de marché) ; il implique également une critique : les néophiles humanitaires sont tellement intéressés par la nouveauté qu'ils peuvent perdre de vue le fait qu'une innovation change véritablement la donne ou qu'elle se contente d'apporter des modifications mineures. Ils ne voient pas quand les innovations peuvent se faire au détriment d'activités plus routinières, qui ont un impact bien plus important sur les pauvres. »

"This concept of 'humanitarian neophilia', in other words, not only describes the main characteristics of the innovation movement (its pursuit of new technology and new market opportunities); it also implies a critique: that humanitarian neophiliacs are so interested in novelty that they may lose sight of whether an innovation is genuinely game-changing or whether it fiddles around the edges. They miss when innovations might take place at the expense of more routine activities, which have a far bigger impact on the poor. " Tom Scott-Smith, "Humanitarian neophilia: the 'innovation turn' and its implications", *Third World Quarterly*, 2016, 37:12, p. 2229-2251

[377] «The role of technology, products and processes from other sectors, new forms of partnership, and the use of the ideas and coping capacities of crisis-affected people. » RAMALINGAM, Ben, SCRIVEN, Kim, FOLEY, Conor, "Innovations in international humanitarian action", Calpnetwork, 2009, https://www.calpnetwork.org/wp-content/uploads/2020/01/8rhach3-2.pdf

[378] "it need not involve the creation of something absolut novel, but often takes the form of adapting something to a different context. Third, a solution does not require a particular threshold of change to qualify as innovation. It may be "game-changing" in having a high degree of technological progress and market impact, or it may be incremental." RAMALINGAM, Ben, SCRIVEN, Kim, FOLEY, Conor, ibid.

nouveau, il faut aussi démolir les modes de pensée conventionnels. Cela rejoint l'idée de Schumpeter selon laquelle l'innovation est un processus de destruction créatrice. » [379] L'auteur défend une conception pragmatique et se distancie quelque peu de l'approche fondée sur les principes humanitaires, valorisant l'action immédiate[380]. L'adoption d'outils numériques permettrait de plus des formes d'organisation plus fluides et agiles [381]. Christophe Fabian, directeur du service innovation d'UNICEF, déclare ainsi que « Changer la façon dont l'UNICEF s'acquitte de sa mission d'aide aux enfants les plus vulnérables du monde signifie rechercher et expérimenter de nouvelles technologies. (…)UNICEF doit « penser comme des entreprises et […] travailler avec des start-ups. »[382]

Le rapport de Ben Ramalingam de 2009 a été suivi d'une cristallisation de la notion d'innovation humanitaire et par une série d'événements consacrée à ce thème. Une foire à l'innovation a été organisée par l'ANALP. En 2010, le DFID, le bailleur anglais, crée l'Humanitarian Innovation Fund, première bourse destinée à l'innovation humanitaire. En 2016, l'innovation est un des piliers du Sommet Humanitaire mondial.

Ces différents événements participent à diffuser l'idée qu'afin de remplir leur mandat humanitaire, les organisations ne doivent pas rater le coche technologique. Les NTIC permettraient de mieux répondre aux besoins des bénéficiaires. Yves Daccord, directeur général du Comité international de la croix rouge, déclare ainsi que « L'innovation n'est dès lors plus un choix, mais une obligation. »[383] Être innovant devient un impératif moral. Et comme le rapporte le chercheur Tom Scott Smith, il existerait une proximité entre les valeurs

---

[379] « literally, 'destroyers of icons'(…) to create something new, one also has to tear down conventional ways of thinking. This resonates with Schumpeter's idea of innovation as a process of creative destruction."
RAMALINGAM, Ben, SCRIVEN, Kim, FOLEY, Conor, ibid

[380] « Un ingénieur en eau du CICR et un ingénieur en eau d'une ONG peuvent tous deux travailler à l'installation d'une canalisation, mais ils le font pour des raisons institutionnelles très différentes, avec des significations très différentes associées à leur travail. Alors que le CICR adopte des positions de principe, affirmant la pertinence, le caractère indispensable et central des principes humanitaires d'indépendance et de neutralité, l'ONG peut avoir une approche plus pragmatique, accordant une plus grande importance à l'action immédiate, à la fourniture de services et à la coopération avec les gouvernements et d'autres acteurs. », "An ICRC water engineer and an NGO water engineer can both be working to install a pipe, but they do so for very different institutional reasons, with very different meanings associated with their work. While the ICRC takes principled positions, affirming the continued relevance, indispensability and centrality of humanitarian principles of independence and neutrality, the NGO might have a more pragmatic approach, placing a higher premium on immediate action, service delivery and cooperation with governments and other actors."Ibid.
« La première fois que j'ai sauté d'un avion, cela me dépassait. Mais en faisant des recherches pour mon dernier livre, Upshift, qui traite de la performance et de la créativité sous pression, j'ai appris que nous avons tous cette capacité innée, et que nous pouvons la débloquer et l'améliorer grâce à un effort conscient et à la pratique », "The first time I jumped out of a plane this was beyond me. But in researching my latest book, *Upshift*, which is about performance and creativity under pressure, I learned that we all have this innate ability, and that we can unlock and improve it through conscious effort and practice" RAMALINGAM, Ben, "I jumped out of a plane to learn the beneft of stress", *The Guardian*, 23/11/2023. https://www.theguardian.com/society/2023/apr/23/i-jumped-out-of-a-plane-to-learn-more-about-stress-ben-ramalingam
RAMALINGAM, Ben, "New Ideas can transform aid delivery", *The Guardian*, 22/02/2011
https://www.theguardian.com/global-development/poverty-matters/2011/feb/22/humanitarian-aid-innovation

[381]TERBECHE Mehdi, CARRIER Michael, « Pour un "Manifeste agile" des projets d'aide humanitaire et de coopération au développement », Revue HEM, URD, 26/03/2019. https://www.urd.org/fr/revue_humanitaires/pour-un-manifeste-agile-des-projets-daide-humanitaire-et-de-cooperation-au-developpement/
DAOUD Lisa, WATCH Edmond, « Les technologies de l'information : le cache-misère d'un secteur en manque d'agilité ? », Revue HEM, URD, 26/03/2019. https://www.urd.org/fr/revue_humanitaires/les-technologies-de-linformation-le-cache-misere-dun-secteur-en-manque-dagilite/

[382] "the work of UNICEF Innovation is essentially about connecting the needs of humans to profit. That is connecting 50 million refugees on the move because of violence with businesses to 'create stronger businesses and help humanity'. Changing the way UNICEF does its business of helping the world's most vulnerable children means pursuing and experimenting with new technology: 'we think that some of the best solutions for kids come from startups and from the space of technology', as Fabian has explained it. UNICEF needs to 'think like businesses and . . . work with startups", FEJERSKOV, Adam, *The Global lab : inequality, technology, and the experimental movement*, Oxford University Press, 2022, p.48

[383]MOTTOLA, Nina, « L'innovation au service de l'humanitaire », *Medium*, 01/08/ 2019 https://medium.com/21croixrouge/linnovation-au-service-de-l-humanitaire-468b9dca0284

défendues par les membres de la Silicon Valley et les partisans d'approches innovantes dans l'humanitaire[384]. Ils partageraient une confiance et une foi dans la technologie qui est considérée comme un vecteur d'émancipation et comme la solution la plus efficace pour résoudre les problèmes rencontrés : « Elle a les mêmes intentions progressistes, encourageant les réformes humanitaires et défendant les voix réduites au silence. Elle met la même emphase sur la libération, libérant les gens de la souffrance et l'aide du contrôle du haut vers le bas. Elle accorde la même valeur à l'esprit d'entreprise, cherchant à libérer les citoyens productifs des camps de réfugiés de la dépendance à l'égard de l'aide. Mais surtout, elle célèbre la nouveauté. »[385] Ainsi, le Caplnetwork présente l'entreprise de scan d'iris utilisé par le HCR, Irisguard comme suit : « Irisguard permet d'identifier une personne parmi des millions de personnes, n'importe où dans le monde, avec 100 % d'acuité et en moins de 3 secondes, et sans que la personne détienne de papiers d'identité. Il permet une méthode d'identification transparente, dépourvue d'erreur, sure, sécurisée, et sans contact. « [386] Ce type de discours s'inscrit dans un ensemble plus vaste d'événements de promotion (conférences, publications sur les réseaux sociaux, rapports). La chercheuse Margie Cheeman a pu montrer comment ces derniers produisent tout un imaginaire qui sert de fondement au marché de l'innovation[387]. Ils participent à construire des dispositifs technologiques en tant que fétiches, pour reprendre l'expression de Thom Scott Smith qui l'emprunte lui-même à Marx. Sachant qu'en l'occurrence, un fétiche désignerait le fait de camoufler les structures économiques et politiques à l'œuvre dans ce processus de numérisation[388].

Progressivement, s'est constituée une coalition d'acteurs venant de différents horizons : ONG, secteur étatique, privé et académique. Ont été investis différents espaces comme des laboratoires d'innovation au sein d'ONG. Pour Paul Curion, les premiers lieux de ces types ont été les « Centres d'information humanitaire ». Il s'agit de structures dédiées au partage de données et des tout premiers logiciels d'information géographique (SIG). Selon Paul Curion,

---

[384] "Face à de nouvelles menaces, à des crises de plus grande ampleur et à des déficits de financement et de capacité, l'innovation est présentée comme une question de survie. Sans innovation", peut-on lire dans un document d'information pour le Sommet humanitaire mondial, "la communauté humanitaire deviendra soit inutile, soit trop rigide pour fonctionner efficacement". "With new threats, crises on a bigger scale and shortfalls in funding and capacity, innovation is presented as a matter of survival. 'Without innovation', reads a back-ground paper for the World Humanitarian Summit, 'the humanitarian community will either become irrelevant or too rigid to function effectively." SCOTT SMITH, Tom, « Humanitarian neophilia: the 'innovation turn' and its implications », *Third World Quarterly*, 37:12, p.2229-2251, 2016, DOI: 10.1080/01436597.2016.1176856
READ, Róisín, TAITHE, Bertrand, MAC GINTY, Roger, "Data hubris? Humanitarian information systems and the mirage of technology", *Third World Quarterly*, 2016, 37:8, p. 1314-1331, DOI: 10.1080/01436597.2015.1136208

[385] « Elle a les mêmes intentions progressistes, encourageant les réformes humanitaires et défendant les voix réduites au silence. Elle met la même emphase sur la libération, libérant les gens de la souffrance et l'aide du contrôle du haut vers le bas. Elle accorde la même valeur à l'esprit d'entreprise, cherchant à libérer les citoyens productifs des camps de réfugiés de la dépendance de l'aide. Mais surtout, elle célèbre la nouveauté." "It has the same progressive intentions, promoting humanitarian reforms and championing silenced voices. It has the same emphasis on liberation, freeing people from suffering and aid from top-down control. It places the same value on entrepreneurship, seeking to liberate the productive citizens of refugee camps from the dependency of aid. But most crucially it celebrates novelty. "SCOTT SMITH, Tom, ibid

[386] OCHA, "The business case a study of private sector engagement in humanitarian action", November 2017, https://www.unocha.org/publication/business-case-study-private-sector-engagement-humanitarian-action

[387] CHEESMAN, M.," Conjuring a Blockchain Pilot: Ignorance and Innovation in Humanitarian Aid", *Geopolitics*, 2024, p. 1–28. https://doi.org/10.1080/14650045.2024.2389284

[388] SCOTT SMITH, Tom, « Humanitarian neophilia: the 'innovation turn' and its implications », *Third World Quarterly*, 37:12, p.2229-2251, 2016, DOI: 10.1080/01436597.2016.1176856

Ces structures situées au Kosovo et au Rwanda auraient eu une approche innovante, mais sans être reconnue comme telle, l'innovation n'était pas encore inscrite à l'agenda humanitaire[389].

C'est Unicef qui se présente comme une organisation pionnière en la matière, avec l'ouverture en 2007 de laboratoires d'innovation au Danemark, au Kosovo, en Ouganda et au Zimbabwe. Pour Unicef, un laboratoire d'innovation est défini comme suit, ce sont des « accélérateurs d'incubation ouverts et collaboratifs qui rassemblent les entreprises, les universités, les gouvernements et la société civile afin de créer des solutions durables aux défis les plus urgents. »[390] Les chercheuses Louise Bloom et Romy Faulkner parlent d'« espaces physiques ou virtuels qui permettent et soutiennent l'innovation (technologique ou autre) de ceux qui y participent. Les espaces d'innovation facilitent la créativité et la pensée critique de leurs participants par le biais d'une série d'activités et d'événements. Les espaces peuvent prendre la forme d'unités de travail, de laboratoires, de réseaux ou de centres créés dans le but de soutenir l'innovation au sein d'une organisation ou d'un environnement particulier. »[391]

Ce modèle essaime. L'UNHCR fonde un laboratoire en 2012. Le WFP en 2015 se dote aussi d'un « accélérateur d'innovation », la Croix-Rouge néerlandaise en 2016. Au sein de l'ONU, ce type d'organe se structure autour du réseau de l'ONU pour l'innovation[392]. On peut mentionner l'UN Global Pulse New York Lab, l'Uganda Lab, le Jakarta Lab etc. La Croix rouge australienne suit le mouvement avec la fondation en 2019 d'Humanitech. Toujours en 2019, MSF ouvre son propre espace d'innovation, la Croix-Rouge Française fonde 21, son laboratoire dirigé par Axelle Le Maire, ancienne ministre du Numérique sous François Hollande. Il existe aussi d'autres types d'espace d'innovation : des fablabs humanitaires qu'on a pu explorer lors de recherches précédentes[393]. On peut citer ceux de Terre des Hommes, de l'organisation Comunitere ou encore d'Habibi Works. Ces espaces ont d'autres racines, sont proche d'une culture maker. Et ils se veulent plus ouverts et participatifs que les laboratoires déjà cités, bien

[389]« Cela était en partie dû au fait qu'OCHA ne comprenait pas comment capitaliser sur le concept : à ce stade, OCHA n'avait pas encore reconnu la valeur de la gestion de l'information, bien qu'il ait depuis fait de grands progrès avec des projets tels que les HIC. L'idée d'innovation n'a pas vraiment fait son chemin dans le secteur humanitaire (...) Ce n'est qu'avec le recul que nous pouvons reconnaître les HIC pour ce qu'ils étaient vraiment : des laboratoires d'innovation, avant que les laboratoires d'innovation ne soient cool. Le HIC devait agir en tant que prestataire de services indépendant pour l'ensemble de la communauté humanitaire, financé et doté en personnel sur une base inter-agences, fournissant un accès à la technologie (en particulier les systèmes d'information géographique, ou SIG) que les agences individuelles ne pouvaient pas s'offrir. », "This was partly due to OCHA's lack of understanding of how to capitalise on the concept: at that stage OCHA had not yet recognised the value of information management, although it has since made great progress with projects such as the idea of innovation didn't really land in the humanitarian sector (…)It's only with hindsight that we can recognise the HICs for what they really were: innovation labs, before innovation labs were cool.HIC was to act as an independent service provider for the entire humanitarian community, funded and staffed on an inter-agency basis, providing access to technology (particularly Geographic Information Systems, or GIS) that individual agencies could not afford."CURRION, Paul, "The Life and death of an innovation lab : a personal reflection", *ODI-HPN*, 01/11/2016 https://reliefweb.int/report/world/life-and-death-innovation-lab-personal-reflection

[390]« open, collaborative incubation accelerators that bring business, universities, governments and civil society together to create sustainable solutions to the most pressing challenges"
UNICEF," Innovation at UNICEF, From start-up to scale-up", May 2015. http://archive.unicef.cn/cn/uploadfile/2016/0317/20160317121428604.pdf

[391]« Physical or virtual spaces that enable and support the innovation (technological or otherwise) of those who participate in the space. Innovation spaces facilitate the creativity and critical thinking of their participants through a range of activities and events. Spaces may take the form of working units, labs, networks or centres that are established with a focus on supporting innovation within a particular organization or environment."
BLOOM, Louise, ROMY, Faulkner, "Innovation spaces, transforming humanitarian practice in the United nations",Working paper, Refugee studies centre, Oxford, 2015
BLOOM, Louise, BETTS, Alexander, "The two worlds of humanitarian innovation", Working paper, Refugee studies centre, 2013

[392] https://www.uninnovation.network/

[393] DELLA TORRE, Laetitia. « Formes horizontales d'organisation humanitaire. "Fablabs" et "Makerspaces" en Grèce pour l'aide aux réfugiés : réparer les vivants, réparer les choses (Master-2) », 19 janvier 2019, *Cahiers Costech*, numéro 2. https://www.costech.utc.fr/CahiersCostech/spip.php?article76

qu'il existe un mouvement d'institutionnalisation des Fablabs qui convergeraient avec les évolutions du capitalisme contemporain[394].

Certains bailleurs étatiques ont mis en place des fonds destinés à l'innovation : le DFID en 2010, l'USAID a fondé le Global Development lab en 2014. Mais il est difficile d'évaluer leur poids dans le financement de l'innovation. Selon une idée répandue, les bailleurs seraient plus réticents au financement de projets innovants, en raison d'un manque d'appétence au risque, et privilégieraient des projets standardisés aux résultats moins incertains. Le fonctionnement des financements bailleurs — courts et sur projet — ne permettrait pas en outre de couvrir toutes les phases d'innovation. Enfin, les bailleurs manqueraient de souplesse et d'adaptabilité et seraient centrés sur des innovations en faveur de leur propre agenda économique et sécuritaire (comme la biométrie)[395]. L'innovation serait alors plutôt soutenue par des acteurs privés. Citons aussi le « Mobile for humanitarian Innovation Fund » de GSMA, fondé en 2017 et soutenu par le ministère du développement britannique [396].

Dans le même temps, il est parfois regretté que l'innovation ne serait pas suffisamment soutenue, qu'il existerait un décalage entre le secteur privé et le secteur humanitaire en matière de R&D[397]. Une étude commandée au cabinet de conseil Deloitte pour le Sommet mondial de l'aide humanitaire suggère que le secteur humanitaire serait « à la traîne » sur ce sujet. En 2015, un document financé par le DFID affirme que le financement de l'innovation humanitaire serait « incroyablement faible ». Il l'estime à environ 37 millions de dollars par an, soit 0,27 % du total des dépenses humanitaires mondiales[398]. Des données récentes confirmeraient cette tendance. Dans un rapport d'octobre 2023 de l'ANALP, il existerait toujours un manque de financement sur ce sujet, malgré une augmentation des fonds. On peut y lire : « Bien qu'il n'y ait pas de données actuelles sur les dépenses totales de R&D dans le secteur, les personnes interrogées ont souligné la rareté des financements. Les huit fonds inclus dans cette étude représentent la majorité des fonds intermédiaires axés exclusivement sur le secteur humanitaire. Leurs investissements totaux représentent moins de 80 millions de dollars sur dix ans (…) Étant donné que le financement des appels humanitaires de l'ONU

---

[394]LHOSTE, Evelyne, BARBIER, Marc, « Fablabs : l'institutionnalisation de tiers-lieux du « soft hacking », 2015. ⟨hal-01259868

[395] EGGER, C., " The politics and spaces of public-private partnerships in humanitarian tech innovations", *Environment and Planning C: Politics and Space*, *0*(0).2023, https://doi.org/10.1177/23996544231206822

BRUDER, M., BAAR, T." Innovation in humanitarian assistance—a systematic literature review", *Int J Humanitarian Action*, 2024, 9, 2 https://doi.org/10.1186/s41018-023-00144-3

[396] GSMA, "Digital Innovation in Humanitarian Settings: Lessons from the GSMA, Mobile for Humanitarian Innovation programme", June 2023 https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2023/06/Innovation-Paper_R_Web.pdf

[397] WARNER, Alexandra, « Monitoring humanitarian innovation », *Alnap*, 2017

PARKER, Ben, "Humanitarian innovation faces rethink as innovators take stock", *The New humanitarian*, 20/03/2019 https://www.thenewhumanitarian.org/analysis/2019/03/20/humanitarian-innovation-faces-rethink-innovators-take-stock

[398] GRAY, Ian, HOFFMAN, Kurt, "Finance case study", USAID, May 2015, https://assets.publishing.service.gov.uk/media/57a0896ce5274a27b2000097/Finance_Case-study-MIHIS-project-FINAL.pdf

Capgemini Consulting, "Technological innovation for humanitarian aid and assistance", European Parliamentary Research Service,2019 https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634411/EPRS_STU(2019)634411_EN.pdf

« A study commissioned for the World Humanitarian Summit from consultancy Deloitte suggested the humanitarian sector was "lagging" in research and development. A DFID-funded paper in 2015 found funding for humanitarian innovation was "breathtakingly low", with a provisional estimate of $37 million a year, or 0.27 percent of total global humanitarian spending"

PARKER, Ben, « Humanitarian Innovation faces rethink as innovators take stock", *The New Humanitarian*, 20/03/2019 https://www.thenewhumanitarian.org/analysis/2019/03/20/humanitarian-innovation-faces-rethink-innovators-take-stock

a atteint plus de 20 milliards de dollars en 2021, cela représente une fraction extraordinairement faible des fonds. »[399]

En guise de conclusion, le secteur humanitaire se retrouve dans une situation contrastée : il existe une forte valorisation de l'innovation, qui se manifeste de façon le plus visible au sein d'espaces spécifiques (les laboratoires d'innovation) ou au sein d'organisations comme l'ANALP. Mais il existerait dans le même temps un manque de financement, ainsi que de transparence concernant les partenariats. Et surtout, l'impératif d'innovation peut être remis en perspective. Tout d'abord, au-delà de ces laboratoires d'innovation, la perception du numérique pourrait être plus partagée. Par exemple Giulio Coppi, membre de l'ONG de défense des droits humains en ligne, Access now, remet en cause l'image d'un secteur influencé par un imaginaire technophile, dans lequel le numérique serait une solution à tout problème. Il existerait selon lui une réticence à l'adoption d'outils numériques, qui se traduirait par un manque de connaissance et d'esprit critique à l'égard des NTIC. Giulio Coppi fait le diagnostic suivant : « le secteur est très conservateur, très sceptique, mais au lieu de traduire ce scepticisme en laissez-moi vous expliquer comment cela fonctionne, laissez-moi découvrir ce qui se cache derrière cela. Ils se cachent la tête dans le sable jusqu'à ce que l'organisation adopte un outil et c'est tout, maintenant vous devez l'utiliser. Nous voulons être hypercritiques, mais nous ne prenons pas nos responsabilités. »[400] Giulio Coppi prend à contre-pied l'importance de l'innovation au sein de l'humanitaire. Pour notre part, on s'intéressera plutôt à des acteurs adoptant un positionnement d'expertise vis-à-vis du numérique, afin de réguler l'innovation et d'atténuer les effets potentiellement délétères, à savoir les délégués à la protection des données d'ONG. S'intéresser à ces acteurs permet aussi de nuancer la thèse de l'humanitaire comme laboratoire technologique.

## § 2 — De l'expérimentation médicale à l'expérimentation numérique

En effet d'autres chercheurs et chercheuses remettent en perspective l'imaginaire de l'innovation technologique en le reliant à la notion d'expérimentation. Pour Kristin Sandvik ce terme désigne « un processus défini et structuré permettant de tester et de valider l'effet et l'efficacité de nouveaux produits ou de nouvelles approches. Le travail humanitaire, en raison de son contexte incertain et souvent insécurisant, est par nature expérimental »[401]. Elles établissent donc un lien implicite entre crise et expérimentation, entre urgence et

[399] "Although there is no current data on total R&D spending in the sector, those interviewed emphasised the paucity of funding. The eight funds included in this study represent the majority of intermediate funds focused exclusively on the humanitarian sector. Their total investments represented less than $80 million over ten years (…) Given that funding for UN humanitarian appeals reached over $20 billion in 2021, this represents an extraordinarily small fraction of funds." ANALP, "Assessing the promise of innovation for improving humanitarian performance, a 10-year review for the state of humanitarian system report", 16/10/2023, https://www.alnap.org/help-library/assessing-the-promise-of-innovation-for-improving-humanitarian-performance-a-10-year

[400] "the sector is very conservative, very skeptical but instate of translating this scepticism in let me explain in how that works, letme find out what's behind this. They hide their head in the sand until the organisation is adopting a tool and that is it , now you have to use it. We want to be to be hypercritical but we don't take our responsability." COPPI, Giullio, "Humanitarian tech unveiled : from principles to corporate capture", Socio-techs, November 2023

[401] « defined, structured process to test and validate the effect and effectiveness of new products or approaches. Humanitarian work, due to its uncertain and often insecure context, is by nature experimental. »
SANDVIK, Kristin, LINDSKOV JACOBSEN, Katja, MCDONALD, Sean Martin, "Do no harm : a taxonomy of the Challenges of humanitarian experimentation", *International Review of the Red Cross* (2017), 99 (1), p. 319–344

abaissement du seuil de risque tolérable face à l'impératif d'action. La pression de l'urgence fait que toute solution apparait comme bonne à prendre : « Quelque chose doit être fait ». Kristin Sandvik se réfère à Craig Calhoun pour qui l'urgence a sa propre représentation du monde, oriente le système moral, influe sur le type de risque pouvant possiblement être toléré [402]. Précisons que sans que cela mette en cause l'impératif d'assistance, l'aide humanitaire se déploie dans des temporalités variées qui ne relèvent pas nécessairement de l'urgence [403]. Selon un rapport de l'organisation ANALP, la plupart des innovations humanitaires seraient éprouvées dans des situations « stabilisées »[404]. Mais, utiliser ce terme permet aussi pour les chercheuses de dénoncer le manque de cadre éthique solide de l'innovation humanitaire, notamment en matière de consentement. Et surtout, il permettrait de mettre à jour ce qu'elles doivent à l'héritage colonial, ce terme faisant écho aux expérimentations médicales menées en contexte colonial dans des réserves autochtones en Amérique du Nord ou en Afrique [405]. De nombreux travaux ont en effet porté sur les « laboratoires en plein air » coloniaux. Des historiens ont décrit les expérimentations de vaccins sur des tirailleurs sénégalais[406], de traitement de la « maladie du sommeil »[407] par Robert Koch, ainsi que le traitement de la malnutrition et du « kwashiorkor » sur des enfants en Ouganda[408]. Selon Bruno Latour les médecins pasteuriens ont pu construire dans les colonies un espace ordonné par la rationalité scientifique et consacré à la mise en place de protocoles expérimentaux[409]. L'expérimentation médicale n'est cependant pas réductible au terrain colonial. Ainsi, Grégoire Chamayou s'en détache pour retracer l'histoire longue de l'expérimentation sur des êtres humains. Il défend la thèse que ce sont les « êtres vils » — ou plutôt les « corps vils » — dont la vie parait moins digne de valeur, qui peuvent faire l'objet

---

[402] SANDVIK, Kristin, LINDSKOV JACOBSEN, Katja, MCDONALD, Sean Martin, Do no harm : a taxonomy of the Challenges of humanitarian experimentation, International Review of the Red Cross (2017), 99 (1), 319–344. Migration and displacement
CALHOUN, Craig, "A World of Emergencies: Fear, Intervention, and the Limits of Cosmopolitan Order"*, Canadian Review of sociology*, Volume41, Issue4, 2004, p. 373-395

[403] AGIER, Michel, « Quel temps aujourd'hui », *L'Homme*, 185-186, 2008, http://journals.openedition.org/lhomme/24122

[404] « La plupart des innovations ont été testées dans des contextes opérationnels relativement plus faciles, (...) Seuls 6 % des projets ont été testés dans des situations d'urgence de niveau 3. Le fait de tester dans des contextes opérationnels plus faciles a réduit les risques financiers et de réputation, ainsi que le risque d'échec (ou d'absence d'apprentissage). » « Most innovations were tested in relatively easier operational contexts, (…) Only 6% of the projects were tested in level 3 emergencies. Testing in easier operational contexts reduced financial and reputational risks as well as the risk of failure (or of not learning). It also meant organisations did not test new projects with the most vulnerable communities. However it is important that tested innovations are also taken to more complex humanitarian environments, where the needs are often greatest. »ANALP, "Assessing the promise of innovation for improving humanitarian performance, a 10-year review of the state of humanitarian system report", 16/10/2023 https://www.alnap.org/help-library/assessing-the-promise-of-innovation-for-improving-humanitarian-performance-a-10-year

[405] LATOUR, Bruno, "Give me a laboratory and I will raise the World", in KNORR-CETINA, Karin, MULKAY, Michael (ed.), *Science observed, perspectives on the social study of science,* London: Sage Publication, 1983,263 p.
OWENS, Deirdre Cooper, *Medical Bondage , race, gender and the origine of American gynecology,* University of Georgia Press, 2017, p.182
WASHINGTON, HARRIET, *Medical Apartheid: The Dark History of Medical Experimentation on Black Americans from Colonial Times to the Present*, New York: Harlem Moon, 2006, 528 p.
LUX,Maureen, *Medicine that walks : disease, medicine, and Canadian plains native people, 1880-1940*, University of Toronto Press, 2001, 288 p.
KELM, Mary-Ellen, *Colonizing Bodies: Aboriginal Health and Healing in British Columbia, 1900–50*, Vancouver : ubc Press, 1998, 272 p.
LOGAN MCCALLUM, Mary Jane, "Indigenous Historical Perspectives Starvation, Experimentation, Segregation, and Trauma: Words for Reading Indigenous Health History", *Canadian Historical Review*, 2017, 98:1, p.96-113

[406]VIAL, Adrien, « Quand les tirailleurs sénégalais servaient de cobayes », *Afrique XXI*, 12/10/2022
https://afriquexxi.info/Quand-les-tirailleurs-senegalais-servaient-de-cobayes

[407] LACHENAL, Guillaume, *Le médecin qui voulut être roi. Sur les traces d'une utopie coloniale*, Paris : Seuil, 2017, 353 p
ECKART, Wolfgang, « The colony as laboratory: German sleeping sickness campaigns in German East Africa and in Togo, 1900-1914 ». *History and Philosophy of the Life Sciences* 24, no. 1 (2002): 69–89. http://www.jstor.org/stable/23332441.

[408] GRABOYES, Melissa, "Introduction : Incorporating Medical Research into the History of Medicine in East Africa." *The International Journal of African Historical Studies*, vol. 47, no. 3, 2014, p. 379–98. http://www.jstor.org/stable/24393435.

[409] LATOUR Bruno, *Pasteur : guerre et paix des microbes. Suivi de Irréductions,* Paris : La Découverte, « Poche / Sciences humaines et sociales », 2011, 364 p.

d'expériences scientifiques et médicales[410]. Il s'agit de populations captives, pouvant se prêter à des expérimentations dans des environnements clos, prisons, hospices, camps, navires négriers[411]. Grégoire Chamayou cherche à mettre en lumière le statut d'exceptionnalité de ces corps. En effet, comment certaines catégories de sujets sont-elles constituées en tant que sujets légitimes d'expérience alors que cela reste de l'ordre de l'impensable pour le reste de la population ? Grégoire Chamayou parle de technique d'acquisition, de méthodes d'avilissement, soit l'ensemble des procédés visant à « avilir » des catégories de sujets, à les dégrader, au sens propre comme au figuré, matériellement comme symboliquement. Cependant, à la fin du XIXe, une conscience éthique commence à émerger, tandis que se développe l'industrie pharmaceutique en Europe. Grégoire Chamayou émet alors l'hypothèse d'une délocalisation des expérimentations en colonies[412].

Mais le fruit de ces expérimentations ne resterait pas nécessairement dans des territoires marginaux. Certains auteurs postulent l'existence d'un « effet boomerang ». Celui-ci ne concerne cependant pas spécifiquement la médecine, mais désigne également des techniques de gouvernance et des techniques sécuritaires[413], policières et de renseignement[414]. Elles seraient testées en colonies, puis seraient réutilisées — une fois bien éprouvées — en métropole, d'abord dans ses espaces marginaux, en banlieues et sur populations minorisées, puis à l'échelle plus globale. Cette thèse est défendue par Hannah Arendt : les colonies ont pu constituer des champs d'expérimentation de méthodes de gouvernement. C'est particulièrement le cas dans les camps en Afrique du Sud — soit des crimes qui ont été ensuite portés à leur comble de l'horreur dans des régimes totalitaires[415]. On retrouve aussi cette thèse ponctuellement chez Michel Foucault, en particulier dans ses cours au Collège de France « il faut défendre la Société »[416]. Cet « effet de retour » a été à nouveau travaillé par des chercheurs plus contemporains, comme Stephen Graham ou encore Paul Rabinow[417]. Ce

[410] CHAMAYOU, Grégoire, *Les corps vils : expérimenter sur les êtres humains aux XVIIIe et XIXe siècle*, Paris : La Découverte, 2014, 424 p.

[411] DOWNS, Jim, *Maladies of empire, how colonialism, slavery and war transformed medicine*, The Belknap press of Harvard University, 2021,272 p.

[412] « Est-ce un hasard que ces expériences aient lieu là-bas au moment même où ici la déontologie et la codification juridique de l'expérimentation avaient remporté leurs premières victoires ? » CHAMAYOU, Grégoire, *Les corps vils.* La Découverte, « Poche / Sciences humaines et sociales », 2014, 424 p.

[413] RIGOUSTE, Mathieu, « L'Ennemi intérieur, de la guerre coloniale au contrôle sécuritaire », *Cultures& conflits*, 67, 2007

RIGOUSTE, Mathieu, « Purifier le territoire. De la lutte anti-migratoire comme laboratoire sécuritaire (1968-1974) », *REVUE Asylon(s),* N°4, mai 2008

SCHRADER, Stuart, *Badges without borders, how global counterinsurgency transformed American policing*, University of California Press, 2019, p.416.

BLANCHARD, Emmanuel, « Conclusion : Les forces de l'ordre colonial, entre conservatoires et laboratoires policiers. » DENYS, C., DENIS V., (dir.). *Polices d'Empires, XVIIIe-XIXe siècles*, Presses Universitaires de Rennes, p.171-187, 2012

[414] BAT, Jean-Pierre, COURTIN, Nicolas, HIRIBAREN, Vincent (dir.), *Histoire du renseignement en situation coloniale*, Presses universitaires de Rennes, 2021, 294 p.

[415] OWENS, Patricia, "The Boomerang Effect: On the Imperial Origins of Total War", *Between War and Politics: International Relations and the Thought of Hannah Arendt*, Oxford University Press, 2007, 232 p.

[416]Il formule ce point dans un paragraphe de dix lignes glissé entre de plus amples développements sur les conquêtes normandes en Angleterre et ses effets juridico-politiques :

« en cette fin du XVIe siècle, sinon pour la première fois, du moins une première fois, je crois, une espèce d'effet de retour, sur les structures juridico-politiques de l'Occident, de la pratique coloniale. Il ne faut jamais oublier que la colonisation, avec ses techniques et ses armes politiques et juridiques, a bien sûr transporté des modèles européens sur d'autres continents, mais qu'elle a eu aussi de nombreux effets de retour sur les mécanismes de pouvoir en Occident, sur les appareils, institutions et techniques de pouvoir. Il y a eu toute une série de modèles coloniaux qui ont été rapportés en Occident, et qui a fait que l'Occident a pu pratiquer aussi sur lui-même quelque chose comme une colonisation, un colonialisme interne. » FOUCAULT,Michel, *Il faut défendre la société » : Cours au collège de France*, Paris, Seuil, 2012, p.96-97

[417] RABINOW, Paul, *Une France si moderne, naissance du social, 1800-1950*, Paris : Buchet-Chastel, 2006, 636 p.

dernier a qualifié les colonies de « laboratoires de la modernité »[418] — notamment urbaine. Cette thèse est toutefois critiquée et peut être nuancée. Guillaume Lachenal par exemple met en avant la nécessité de l'ancrer empiriquement. Cela implique, comme l'incite à le faire aussi Anne Stoller, de décrire les circulations d'acteurs, des savoirs, au sein d'empires coloniaux[419]. Enfin, Stuart Schrader parle plutôt d'aller-retour, de trajectoires multidirectionnelles[420]. La thèse du boomerang repose en effet sur le présupposé d'un ordre libéral et démocratique initial. Et pour Stuart Schrader, il n'est pas tout à fait juste de voir la naissance de la violence impériale dans les colonies. Il existait déjà des techniques de police (violentes et arbitraires) sur le sol américain avant leur exportation dans des terrains coloniaux, puis leur réimportation sur le sol domestique. Enfin, cette circulation peut aussi être inversée. Pour prendre un exemple plus contemporain, et concernant le numérique, si l'Afrique a été décrite comme un laboratoire d'expérimentation, certains pays du continent sont aussi le pays de destination de matériels informatiques usagés d'utilisateurs occidentaux[421].

Dernier point, cette circulation d'expérimentation suppose leur réussite relative. Or il ne faut pas oublier comme le surligne Guillaume Lachenal que toute expérimentation peut aussi finir sur un échec. Il se réfère à Frédéric Cooper [422]ou à Achille Mbembe et à ses réflexions sur l'« indiscipline » en situation coloniale camouflée par les discours volontaristes des médecins[423]. Ainsi pour Guillaume Lachenal, il faut parler, plutôt que d'un laboratoire colonial, d'« une constellation de projets à la fois matériels et narratifs, réels et théâtraux, qui servirent de miroir, c'est-à-dire de reflet désiré et idéalisé, aux entrepreneurs de la santé publique de métropole. »[424] Il ne s'agit pas pour lui de se limiter à une critique du décalage entre discours et réalité, mais d'analyser ce que ce décalage raconte et s'intéresser à la mise en récit de l'échec. Il refuse de voir dans ces laboratoires une forme pure de gouvernance des corps et des populations, par une raison médicale rationnelle et froide. Et il met l'accent sur les failles des médecins coloniaux, leur obstination dans l'échec, leur hubris, leurs errements. [425] [426] Helen Tilley au contraire a pu parler de l'Afrique comme « laboratoire », mais en insistant cependant bien sur le fait que le contexte local influe et transforme les savoirs des Britanniques et peut transformer les représentations des acteurs[427]. Et, point important, il faut

---

[418] BERNAULT, Florence, « l'Afrique et la modernité des sciences sociales », *Vingtième siècle, revue d'histoire*, 2001/2 (n°70), p.127-138, éditions Presses de Sciences Po.

[419] LACHENAL, Guillaume, « Médecine, comparaisons et échanges inter-impériaux dans le mandat camerounais : une histoire croisée franco-allemande de la mission Jamot », *Canadian Bulletin of Medical History*, 2013 30:2, p.23-45

STOLER, Ann Laura, COOPER, Frederick, (eds), *Tensions of Empire: Colonial Cultures in a Bourgeois World*, University of California Press, 1997, 463 p.

[420]"In fact, the routes of transit for counterinsurgency and policing during the 1960s were more multidirectional, exorbitant to a vision of empire that, in its flattest variants, can let US imperialism off the hook for what happens overseas as long as those operations remain far afield and never boomerang homeward." SCHRADER, Stuart, Badges without borders, how global counterinsurgency transformed American policing, University of California Press, 2019, 413 p.

[421] DIOP, Cheikh, MOLO THIOUNE, Ramata, Les déchets électroniques et informatiques en Afrique : Défis et opportunités pour un développement durable au Bénin, au Mali et au Sénégal, Paris : Karthala, 2014, 204 p.

[422] COOPER, Frederick, STOLER, Ann Laura (eds.), *Tensions of Empire : Colonial Cultures in a Bourgeois World*, University of California Press, 1997, 463 p.

[423] MBEMBE, Achille, *La naissance du maquis dans le Sud-Cameroun, 1920-1960. Histoire des usages de la raison en colonie*, Paris : Éd. Karthala, 1996, 440 p.

[424] LACHENAL Guillaume, « Le médecin qui voulut être roi. Médecine coloniale et utopie au Cameroun », *Annales. Histoire, Sciences Sociales*, 2010/1, p. 121-156. https://www-cairn-info.ezproxy.utc.fr/revue-annales-2010-1-page-121.htm

[425] FABIEN, Johannes, *Out of Our Minds. Reason and Madness in the Exploration of Central Africa*, University of California Press, 2000, 335 p.

[426] LACHENAL Guillaume, « Le médecin qui voulut être roi. Médecine coloniale et utopie au Cameroun », *Annales. Histoire, Sciences Sociales*, 2010/1, p. 121-156. https://www.cairn.info/revue-annales-2010-1-page-121.htm

[427] TILLEY, Helen, *Africa as a living laboratory: empire, development, and the problem of scientific knowledge, 1870-1950*, University of Chicago Press, 2011, 520 p.

ajouter qu'elle remet en cause l'exception africaine et coloniale dans la conduite d'expérimentation médicale[428].

Pour revenir à la période contemporaine, en matière de recherche clinique, un cadre éthique a été depuis mis en place, après la Seconde Guerre mondiale, en réaction aux expérimentations médicales conduites dans les camps d'extermination nazis. La Déclaration de Manille a complété celle d'Helsinki, en précisant les conditions des essais cliniques dans les pays en voie de développement[429]. Kristin Sandvik appelle à prendre exemple sur le cadre éthique médical pour encadrer les expérimentations numériques en contexte humanitaire[430]. Mais leur application fait débat[431]. Et certains chercheurs comme Melissa Graboyes ou Jean-Philippe Chippaux (qui a depuis nuancé son analyse) [432]ou romanciers comme John le Carré [433] dénoncent les continuités coloniales révélées par des cas de dérives contemporaines d'essais cliniques mal encadrés[434]. Ces essais révéleraient l'inégale application de normes éthiques, selon Adriana Petruna [435], Fouzieyha Towghi et Kalindi Vora. Ces chercheuses montrent comment le niveau de risque tolérable dépend aussi de critères de genre[436], de classe et de dynamiques coloniales[437]. Un bon nombre de ces travaux adoptent un point de vue foucaldien : les essais cliniques seraient le lieu d'exercice d'une biopolitique et d'une gouvernance des corps. Par exemple Veronica Gomez Temesio décrit lors de l'épidémie d'Ebola l'enrôlement des corps noirs dans le travail médical, via le don d'échantillons sanguins pour servir de matière d'expérimentation de traitement[438]. Cependant, d'autres chercheurs déconstruisent l'idée de l'Afrique comme laboratoire. Selon Frederick Eboko le nombre d'essais cliniques n'y serait pas si élevé. Entre autres explications, les laboratoires n'y testeraient pas de traitement pour des maladies endémiques, mais seraient simplement intéressés par des maladies dont le traitement peut être exploité commercialement de façon

---

[428] « En termes purement statistiques, on peut affirmer sans risque que les populations coloniales n'ont jamais été majoritaires en tant que sujets d'expérimentation dans le monde, du moins si l'on utilise une définition étroite du sujet d'expérimentation. C'est l'un des paradoxes de l'interaction entre la science et l'empire : si les États autocratiques ont pu dépouiller les peuples de leur souveraineté, ils n'ont pas toujours été en mesure de traduire le pouvoir politique en pouvoir expérimental. » "in sheer statistical terms, it seems safe to assert that colonial populations were never in the majority as test subjects around the world, at least not if we use a narrow definition of experimental subject. This is one of the paradoxes of the interplay between science and empire: though autocratic states were able to strip people of their sovereignty, they were not always able to translate political power into experimental power into experimental power." TILLEY, Helen. "Conclusion : Experimentation in Colonial East Africa and Beyond." *The International Journal of African Historical Studies*, 2014, vol. 47, no. 3, p. 495–505 http://www.jstor.org/stable/24393440.

[429] CHIPPAUX, Jean-Philippe, *Pratique des essais cliniques en Afrique*, IRD,2004, 318 p.

[430] MCDONAL, Sean Martin, SANDVIK, Kristin, JACOBSEN, Katja," From principle to practice : humanitarian innovation and experimentation", Norwegian centre for humanitarian studies, Blog, 22/12/2017
https://www.humanitarianstudies.no/from-principle-to-practice-humanitarian-innovation-and-experimentation/

[431] HUME-FERKATADJI, François, MACADRE, Olivia, « En Afrique, la science a-t-elle appris de ses erreurs? », *Mediapart*, 28/04/2020
https://www.mediapart.fr/journal/international/280420/en-afrique-la-science-t-elle-appris-de-ses-erreurs

[432] CHIPPAUX, Jean-Philippe, « L'Afrique, cobaye de Big Pharma », *Le Monde diplomatique*, juin 2005
https://www.monde-diplomatique.fr/2005/06/CHIPPAUX/12513

[433] LE CARRE, John, *La constance du jardinier*, Paris : Seuil, 2001, 504 p.

[434]HOFFMANN, N., « Involuntary experiments in former colonies: the case for a moratorium »,
*University of Sussex, journal contribution*, 2019, https://hdl.handle.net/10779/uos.23474837
CAMPAGNE, Gérard, CHIPPAUX Jean-Philippe, GARBA Amadou, « Information et recueil du consentement parental au Niger », *Autrepart*, 2003/4 (n° 28), p. 111-124. https://www.cairn.info/revue-autrepart-2003-4-page-111.htm

[435] PETRYNA, Adriana, *When experiments travel, Clinical trials and the global search for human subjects*, Princeton university press, 2009, 272 p.

[436] MURPHY, Michelle, *Experimental Futures : Seizing the Means of Reproduction : Entanglements of Feminism, Health, and Technoscience,* Durham, NC, USA: Duke University Press, 2012.

[437] FOUZIEYHA, Towghi, KALINDI, Vora, "Bodies, Markets, and the Experimental in South Asia", *Ethnos,* 79:1,2014, p. 1-18

[438] GOMEZ-TEMESIO, Veronica, LE MARCIS, Frédéric, « La mise en camp de la Guinée », *L'Homme,* 222 | 2017, http://journals.openedition.org/lhomme/30147
GOMEZ-TEMESIO, Veronica, LE MARCIS, Frederic, *Governing Lives in the Times of Global Health*, The SAGE Handbook of Cultural Anthropology, 2021.

plus globale [439]. Le chercheur déplore donc au contraire un manque d'essais cliniques en Afrique.

Qu'en est-il des expérimentations numériques ? Cambridge analytica a été testé en 2015 au Niger et en 2017 au Kenya avant d'être déployé aux États-Unis et en Grande-Bretagne[440]. Et l'humanitaire parait être un terrain idéal pour une « phase de test », comme le déclare un membre d'une startup de blockchain médicale que nous avons interrogé : « *En menant un projet pilote avec des réfugiés, nous pouvons créer un produit minimum viable et disposer d'une solide preuve de concept. C'est une bonne chose pour les réfugiés, qui ont désespérément besoin de notre aide, mais c'est aussi une bonne chose pour nous de pouvoir démontrer notre approche dans un contexte réel.* « [441] Peut-on toutefois — en se référant à Grégoire Chamayou — parler de processus d'« avilissement » au sujet d'expérimentations numériques humanitaires ? Katja Jacobsen propose de réfléchir à cette question à partir des écrits de Michel Agier. Ce dernier déchiffre le gouvernement humanitaire et les formes de « désubjectivation » qu'il implique, réduisant les exilés à être des « indésirables »[442]. Précisons toutefois que ni Michel Agier ni Grégoire Chamayou n'adhère totalement au concept de « vie nue » théorisé par Giorgio Agamben : le sujet ne serait jamais dépourvu d'un minimum d'agentivité. Les exilés peuvent résister et s'opposer aux mécanismes de domination[443].

Toujours est-il que dans un contexte de criminalisation des exilés et de sécuritisation de l'aide, le camp en tant qu'espace fermé et zone d'exception parait constituer un laboratoire idéal. Il s'agit d'un lieu parfait pour expérimenter des techniques — numérique ou non — de gouvernance et de contrôle des sujets et des populations. Cette thèse est défendue par de nombreux chercheurs, de Michael Bourne[444] à Ariana Dongus[445] ou Léa Macias[446] et Petra

---

[439] EBOKO, Fred, « Non, l'Afrique n'est pas, ni de près ni de loin, la cible privilégiée des essais cliniques », *Le Monde*, 08/04/2020 https://www.lemonde.fr/afrique/article/2020/04/08/non-l-afrique-n-est-pas-ni-de-pres-ni-de-loin-la-cible-privilegiee-des-essais-cliniques_6035948_3212.html

[440] EKDALE, Brian, TULLY, Melissa, "African Elections as a Testing Ground: Comparing Coverage of Cambridge Analytica in Nigerian and Kenyan Newspapers", *African Journalism Studies*, 40:4, 2019, p. 27-43.

[441]"If we can focus on projects in the developing world and prove ourselves there it may help EU countries to have more faith in adoption in the longer-term. »« By running a pilot with refugees, we can create a Minimum Viable Product and have a strong proof of concept. It is good for the refugees, who desperately need our help, but it is also good for us to be able to demonstrate our approach in a real-world setting. » DISNEY, Helen, « Healthcare IT needs a dose of medicine, interview with Vasja Bocko, Iryo », *Unblocked*, 07/02/2018 https://un-blocked.co.uk/2018/02/07/healthcare-it-interview-vasja-bocko-iryo/

[442] AGIER, Michel, « Penser le sujet, observer la frontière », *L'Homme,* 203-204, 2012, http://journals.openedition.org/lhomme/23096 ;

[443] « Dans cette perspective, il est important de souligner, comme le fait Judith Butler en critiquant l'idée, présente chez Agamben, d'un pouvoir qui réduirait ses sujets à la « vie nue », dans une logique purement soustractive de dépouillement de ses attributs, que « personne n'est jamais retourné à la vie nue, si indigente, si démunie que soit la situation où il est tombé, parce qu'il existe un ensemble de pouvoirs qui produisent et perpétuent sa situation d'indigence, de dépossession et de déplacement. »
CHAMAYOU, Grégoire, *Les corps vils : expérimenter sur les êtres humains aux XVIIIème et XIXème siècle*, Paris : La Découverte, 2014, 424 p.
AGIER, Michel, « Le biopouvoir à l'épreuve de ses formes sensibles. Brève introduction à un projet d'ethnographie des hétérotopies contemporaines », *Chimères*, 2010/3 (N° 74), p. 259-270. https://www.cairn.info/revue-chimeres-2010-3-page-259.htm

[444] BOURNE, M., JOHNSON, H., LISLE, D., « Laboratizing the border: The production, translation and anticipation of security technologies », *Security Dialogue*, *46*(4), 2015, p. 307-325. https://doi.org/10.1177/0967010615578399

[445] GRAF, Vanessa, « Refugee camps as proving grounds for new technologies : Ariana Dongus », *Ars Electronica*, 27/08/2018 https://ars.electronica.art/aeblog/en/2018/08/27/ariana-dongus/
DONGUS, Ariana, « Galton's Utopia. Data accumulation in biometric capitalism spheres », *Journal for Digital Cultures. Spectres of AI*,2019, Nr. 5, S. 1–16 https://spheres-journal.org/wp-content/uploads/spheres-5_Dongus.pdf

[446] MACIAS, Léa « Usages expérimentaux des nouvelles technologies par l'action humanitaire : un data colonialisme ? », *Hommes & migrations*, 1337 | 2022, http://journals.openedition.org/hommesmigrations/13907

Molnar[447], Mirjam Twigt[448]et Claudia Aradau[449]. Différents rapports d'ONG de défense de droits en ligne, comme l'European Digital Rights (EDRI)[450] ou la « Platform for International Cooperation on Undocumented Migrants » (PICUM)[451] vont dans le même sens. La forme « camp » est elle-même décrite comme le fruit de nombreuses expérimentations, circulations et transformations de technologies de pouvoir, des camps des colonies[452], aux camps nazis et aux actuels camps de réfugiés [453] . Hannah Arendt, dans son ouvrage « L'origine du totalitarisme » fait le lien entre les premières expériences allemandes dans les colonies, en Afrique du Sud-Ouest, et dans les camps de la Seconde Guerre mondiale[454]. Les acteurs du champ de la sécurité[455] expérimentent dans des camps et aux frontières des technologies comme de l'intelligence artificielle, des drones, des détecteurs de mensonges[456], etc. — C'est ce qu'a pu montrer dans son travail d'enquête la chercheuse Petra Molnar[457] . Ainsi, en Grèce, le camp de Samos sert depuis son inauguration en 2021 de vitrine à un déploiement de technologies de surveillance comme des drones et des caméras de surveillance augmentées, caméras thermiques, etc. [458]. Et selon un rapport de Statewatch, publié en juillet 2023,[459] le pays recevrait en effet plus de fonds destinés au contrôle des migrations que la plupart des pays méditerranéens. La Grèce serait donc particulièrement représentative d'expérimentation de gestion des populations dans le cadre de surveillance des exilés par des acteurs de politiques migratoires répressives[460].

---

[447]MOLNAR, Petra," Technological Testing Grounds Migration Management Experiments and Reflections from the Ground Up", 2020, EDRI. https://edri.org/wp-content/uploads/2020/11/Technological-Testing-Grounds.pdf
MOLNAR, Petra, *The Walls have eyes, Surviving migration in the age of Artificial intelligence*, New Press, 2024, 320 p. (à venir).

[448]TWIGT, Mirjam, "Doing Refugee Right(s) with Technologies? Humanitarian Crises and the Multiplication of "Exceptional" Legal States », *Refugee Survey Quarterly*, 2024,volume 43, issue 1, p.1-21 https://doi.org/10.1093/rsq/

[449] ARADAU, Claudia "Experimentality, Surplus Data and the Politics of Debilitation in Borderzones". *Geopolitics*, 27(1), 2022, p.26-46.

[450] EDRI, "Regulating border tech experiments in a hostile world", 22/04/2022 https://edri.org/our-work/regulating-border-tech-experiments-in-a-hostile-world/

[451] PICUM, "Digital technology, policing and migration - what does it means for undocumented migrants", 2022 https://picum.org/wp-content/uploads/2022/02/Digital-technology-policing-and-migration-What-does-it-mean-for-undocumented-migrants.pdf

[452] BERNARDOT, Marc, *Camps d'étrangers*, Editions du Croquant, 2008, 223 p.

[453] Ceci n'implique pas une équivalence de toute forme de camp, pour citer Michel Agier : « À quelle profondeur historique et à quel fonds empirique peut se référer aujourd'hui une recherche sur les camps ? Le modèle qui s'impose dans ce que je connais des camps actuels n'est pas celui du camp de la mort, le camp nazi, dont l'existence a relevé d'une logique exterminatrice et génocidaire, mais qu'on ne peut pas, à strictement parler, adosser à la forme du camp comme espace de pouvoir, voire d'exception »
AGIER, Michel, *Gérer les indésirables, des camps de réfugiés au gouvernement humain*, Paris : Flammarion, 2008,350 p.

[454] NETZ, Reviel, *Barbed Wire, an ecology of modernity,* Connecticut : Wesleyan University press, 2004,288 p.

[455] BIGO, Didier, « La mondialisation de l'(in)sécurité ? », *Cultures & Conflits*, 58 | 2005, http://journals.openedition.org/conflits/1813

[456] CLAVEY, Martin, « iBorderCtrl : la CJUE refuse de lever le voile sur le détecteur de mensonges aux frontières financé par l'Europe », *Next,* 14/09/2023 https://next.ink/866/iborderctrl-cjue-refuse-lever-voile-sur-detecteur-mensonges-aux-frontieres-finance-par-europe/

[457] MOLNAR, Petra, "Technological Testing Grounds Migration Management Experiments and Reflections from the Ground Up", 2020, EDRI.https://edri.org/wp-content/uploads/2020/11/Technological-Testing-Grounds.pdf

[458] KARAISKOU, Alexandra, « Drone & artificial intelligence at Greece's hight-tech borders », *Homo Digitalis*, 23/08/2023 https://homodigitalis.gr/en/posts/131019/

[459] JONES, Chris, LANNEAU, Romain, MACCANICO, Yasha, "Europe's techno borders", *Statewatch,* July 2023 https://www.statewatch.org/media/3964/europe-techno-borders-sw-emr-7-23.pdf

[460] « Ce que nous voyons en Grèce, c'est une expérimentation spectaculaire d'une variété de systèmes que l'on ne trouverait pas de manière aussi condensée dans d'autres contextes nationaux", a déclaré Caterina Rodelli, analyste politique de l'organisation à but non lucratif Access Now, spécialisée dans les droits numériques. Elle a ajouté : "Alors que dans d'autres pays européens, on peut trouver une surveillance des migrants, des demandeurs d'asile ... la Grèce a ouvert la voie à des environnements de test plus denses" dans les camps de réfugiés - en particulier depuis la création de ses camps de réfugiés financés par l'UE et truffés de technologies. "What we see in Greece is spectacular experimentation of a variety of systems that we might not find in this condensed way in other national contexts," said Caterina Rodelli, a policy analyst at the digital rights non-profit Access Now.She added: "Whereas in other European countries you might find surveillance of

Les ONG humanitaire participent également dans une certaine mesure à ce laboratoire technologique, réactivant ainsi l'héritage colonial de l'aide. Cependant, il existerait plutôt un conflit entre discours de protection et réification des sujets. On n'assisterait pas à un pur avilissement de l'autre – l'éthique humanitaire défend aussi la dignité des bénéficiaires, dans une certaine mesure, comme on le verra. Pour le moment, afin d'approfondir notre réflexion on s'appuiera sur différentes expérimentations particulièrement représentatives du numériques humanitaires. Elles correspondent à plusieurs modalités de gestion des populations : identifier, grâce à de la biométrie, et cartographier, grâce à de l'imagerie satellitaire, mais aussi les drones, et grâce à des projets de traçage de population recourant à des données massives.

Biométrie

L'origine coloniale de la biométrie est bien connue et documentée. Cette dernière est née dans l'Empire britannique, cette technologie aurait circulé d'abord entre l'Afrique du Sud et l'Inde, puis se serait diffusé dans les pays européens à des fins d'identifications de populations criminalisées, et en médecine légale[461]. Quant aux usages humanitaires de la biométrie à des finalités d'identification des exilés (par le HCR par exemple), ils sont à l'heure actuelle tout à fait documentés[462]. On reviendra pour notre part à leur origine, en se référant au test en 2002 par l'UNHCR d'un dispositif biométrique inédit de scan d'iris à la frontière pakistano-afghane[463]. L'objectif était alors de rendre plus efficace l'enregistrement des bénéficiaires et lutter contre la fraude. L'UNHCR craint en effet que des réfugiés afghans s'inscrivent plusieurs fois pour obtenir d'avantage d'aide. Pour résoudre ce "problème", l'UNHCR s'était rapproché d'une entreprise de reconnaissance d'iris, Irisguard. Notons que malgré son aspect futuriste, il s'agit d'une technologie faisant l'objet de recherches depuis les années 1930. Au cours des années 1990, les technologies à la base du scan d'iris connaissent une grande avancée grâce aux travaux du chercheur britannique John Daugman[464]. La firme « Iridian Technologies » en

migrant people, asylum seekers … Greece has paved the way for having more dense testing environments" within refugee camps – particularly since the creation of its EU-funded and tech-riddled refugee camps
EMMANOUILIDOU, Lydia, "Greek data watchdog to rule on AI systems in Refugee camps", *Pulitzer Center*, 30/10/2023. https://pulitzercenter.org/stories/greek-data-watchdog-rule-ai-systems-refugee-camps
SIBLEY Anna, « La Grèce, à la pointe des technologies liberticides », *Plein droit*, 2024/1 (n° 140), p. 45-46. https://www.cairn.info/revue-plein-droit-2024-1-page-45.htm

[461] BRECKENRIDGE, Keith, *Biometric State : the global politics of identification and surveillance in Suth Africa, 1850 to the present*, Cambridge University Press, 2014, 266 p. Pour rappel, les données biométriques sont tout simplement des Caractéristique physique ou biologique permettant d'identifier une personne (ADN, contour de la main, empreintes digitales...). Elles sont particulièrement sensibles car immuables, et propres à un individu. De nombreuses caractéristiques physiques sont transcodables, potentiellement utilisées pour être lisibles via un dispositif numérique pour identifier une personne. Dernièrement, des scientifiques indiens exploreraient ainsi la possibilité — encore expérimentale — d'identifier un utilisateur de smartphone grâce à son « empreinte respiratoire ». Mukesh Karunanethy, Rahul Tripathi, Mahesh V Panchagnula, Raghunathan Rengaswamy, »User authentification system based on human exhaled breath physics, Paperwithcode », 2/01/2024 https://arxiv.org/pdf/2401.02447v1.pdf
PIAZZA, Pierre, *Aux origines de la police scientifique. Alphonse Bertillon, précurseur de la science du crime.* Karthala, « Hommes et sociétés », 2011, 384 p.
[462] AWENENGO DALBERTO Séverine, BANEGAS Richard, CUTOLO Armando, « Biomaîtriser les identités ? État documentaire et citoyenneté au tournant biométrique », *Politique africaine*, 2018/4 (n° 152), p. 5-29 https://www.cairn.info/revue-politique-africaine-2018-4-page-5.htm
[463] JACOBSEN, Katja, *The politics of humanitarian technology, Good intentions, unintended consequences and insecurity*, Routledge studies in conflict, security and technology,2015
JACOBSEN, K., "Experimentation in humanitarian locations: UNHCR and biometric registration of Afghan refugees",2015, *Security Dialogue*, *46*(2), p.144-164.
[464] DAUGMAN, John, "Iris Recognition: The Colored Part of the Eye Contains Delicate Patterns That Vary Randomly from Person to Person, Offering a Powerful Means of Identification", *American Scientist* 89, no. 4 (2001), p. 326–33. http://www.jstor.org/stable/27857501
DAUGMAN, John, "How iris recognition works", 2004, https://www.cl.cam.ac.uk/~jgd1000/irisrecog.pdf

a alors racheté le brevet de la technologie. De premiers essais sont effectués en 2001, d'abord en environnement fermé, dans des laboratoires, puis dans des aéroports d'Heathrow et en Arabie Saoudite. La technologie est ensuite expérimentée à la frontière pakistano-afghane pour identifier les réfugiés afghans. Mais le scan d'iris n'avait jamais été expérimenté sur une large frange de population ni en vue d'identifier des individus ; la fonctionnalité d'« authentification » était alors plus aboutie. En outre, le contexte était éprouvant et l'environnement offrait des conditions non idéales, les scans d'iris étant réalisés en plein air, en pleine chaleur. Cela est, selon la chercheuse Katja Jacobsen, typique d'un procédé expérimental : sélectionner une technologie testée en laboratoire, mais qui n'a pas fait ses « preuves » dans le « monde réel », et la confronter si possible à des contextes contraignants et difficiles, où la technologie n'a jamais été utilisée. Il s'agit pour les entreprises de mettre à l'épreuve leur produit pour en tester la résistance. D'après cette chercheuse, certains experts auraient averti le HCR que le risque de faux appariement était assez élevé. La possibilité que ce type de technologie puisse relier deux images d'iris et déterminer leur ressemblance n'avait alors été testée que sur de « petites » bases de données. Ajoutons que l'UNHCR n'avait pas prévu d'alternative en cas de refus de s'enregistrer via le dispositif biométrique. Ce point est révélateur selon Katja Jacobsen d'une foi quasi aveugle de l'organisation en la technologie, et d'un manque de prise en compte du consentement des bénéficiaires. Toujours est-il que les rapports de l'UNHCR avaient été dans l'ensemble positifs. Et les connaissances acquises lors de l'expérimentation par l'UNHCR ont pu être exploitées pour améliorer la technologie et l'utiliser en fin de compte à grande échelle dans des zones « stables »[465], par exemple à l'aéroport britannique d'Heathrow, à partir de juin 2005, dans le cadre du programme e-Borders[466]. Le scan d'iris a ainsi été intégré à des politiques de contrôle de frontière, dans des aéroports, mais la technologie a pu aussi être employée au sein de prisons américaines[467], ou parmi les forces de l'ordre[468]. Et les expérimentations les plus récentes de scans présentées au salon de la sécurité Milipol Asia-Pacific vantent la possibilité de scanner l'iris des passagers en mouvement et à distance[469]. On aurait ici un cas de transfert de technologie clair. Quant à l'Afghanistan, le pays s'est progressivement doté de base de données biométriques, et ce à l'initiative du gouvernement, de l'UNHCR et surtout de l'armée américaine. Or, après le départ de cette dernière, en 2021, de nombreuses ONG de défense des droits de l'homme se sont inquiétées du possible accès à ces bases de données par les talibans, mettant les populations

[465] "What is more, even if the experiment would fail to prove the technology's accuracy and certify its proclaimed low failure rate, from an experimentation perspective the endeavor could still be deemed a 'success' because it had helped provide new knowledge about the technology's limitations. This knowledge in turn would make it possible to minimize/counterbalance the newly discovered limitations and thus make the technology 'safe' for use in large-scale, identification schemes in 'tame' zones." JACOBSEN, Katja, *The politics of humanitarian technology, Good intentions, unintended consequences and insecurity*, London: Routledge,2015

[466] E-border Inquiery https://committees.parliament.uk/work/4307/eborders-inquiry/publications/

[467] Associated Press, "Jails hope eye scanners can provide foolproof identification system for inmate", *The New York Time*, 28/02/2010 https://www.nytimes.com/2010/02/28/us/28eyes.html

[468] BBC news, "Heathrow eye scan checks extended", 10/03/2006 http://news.bbc.co.uk/2/hi/uk_news/england/london/4792206.stm
JOSEPH, George, "the Biometric frontier", *the Intercept*, 08/07/2017https://theintercept.com/2017/07/08/border-sheriffs-iris-surveillance-biometrics/
Biometric surveillance, Electronic Frontier Foundation https://sls.eff.org/technologies/biometric-surveillance

[469] https://www.htx.gov.sg/techx/techxplore-next-gen-clearance-concept
GONZALES, Bianca, "Singapore agency develops iris biometrics gates in motion capture with NRC tech", *Biometricupdate*, 24/04/2024, https://www.biometricupdate.com/202404/singapore-agency-develops-iris-biometrics-gates-for-in-motion-capture-with-nec-tech

locales en danger[470]. Quant à l'UNHCR, l'usage de la biométrie s'est progressivement généralisé au sein de l'organisation, également sous la forme de collecte d'empreintes digitales. Une politique de relative aux opérations d'enregistrement biométrique des réfugiés a été publiée en 2010. Et l'organisation a mené des opérations de collecte d'empreinte tout d'abord en Malaisie, ainsi qu'en Afrique de l'Est, en Tanzanie, puis à Djibouti, au Kenya et au Ghana, puis à partir de 2013 au Mali et en 2014 au Malawi. Après ces différents tests, le HCR a qualifié la question de la biométrie en tant qu'« enjeu stratégique » à partir de 2014, et ceci à l'initiative non pas des bureaux régionaux, mais du siège du HCR à Genève et des donateurs[471]. Pour la chercheuse Katja Jacobsen, cette « banalisation » de l'usage de la biométrie ne signifierait pas la fin de la phase « expérimentale » de cette technologie. Initialement utilisé pour l'enregistrement des bénéficiaires, le scan d'iris a pu être ainsi utilisé dans le cadre de programmes de transfert monétaire.

L'utilisation par l'UNHCR du scan d'iris la plus médiatisée concerne son usage en Jordanie. L'agence humanitaire a noué un partenariat avec le WFP l'entreprise IrisGuard afin de développer un programme de cash transfert[472], notamment au camp de Zaatari. Le dispositif biométrique permet ainsi d'identifier un bénéficiaire lorsqu'il dépense les fonds que lui a versés le WFP dans des supermarchés participant au projet. Le cas a été largement couvert par la presse. Ajoutons que l'UNHCR utilise le scan d'iris pour les opérations d'enregistrement des réfugiés au moins d'abord au Malawi en 2013, puis au Kenya, au Bangladesh, ainsi qu'à l'échelle régionale au Liban, en Irak et en Syrie. C'est d'ailleurs dans cette zone que l'UNHCR utilise le système de scan d'Iris pour des opérations de transfert monétaire, menées au Liban[473], en Irak[474] et en Égypte[475]. Et il faut savoir que l'UNHCR projette d'étendre son système de scan d'Iris pour des opérations de cash transfert au Bangladesh, en Éthiopie, en Zambie et au Malawi. Il est à noter que le Covid19 semble avoir renforcé ce tournant du « sans contact »[476].

---

[470] UNHCR, 30/03/2022, "New evidence that biometric data systems imperil Afghans"
https://www.hrw.org/news/2022/03/30/new-evidence-biometric-data-systems-imperil-afghans
CIESIELSKI, Rebeca, ZIERER, Maximilian, "How biometric devices are putting Afghans in danger", *Interaktiv*, 27/12/2022,Br24
https://interaktiv.br.de/biometrie-afghanistan/en/index.html
JACOBSEN, Katja, "Biometric data flows and unintended consequences of counterterrorism", *IRRC* February 2022, No. 916-917
https://international-review.icrc.org/articles/biometric-data-flows-and-unintended-consequences-of-counterterrorism-916
TOFT DJANEGARA, Nina, "Biometrics and counter-terrorism case study of Iraq and Afghanistan", *Privacy international*, May 2021,
https://privacyinternational.org/report/4529/biometrics-and-counter-terrorism-case-study-iraq-and-afghanistan

[471] BARDELLI, Nora, « Entre témoignage et biométrie : la production du « réfugié » au Burkina Faso », *Politique africaine*, 2018/4 (n° 152), p. 121-140. https://www.cairn.info/revue-politique-africaine-2018-4-page-121.htm

[472] Les données collectées par IrisGuard sont hébergées sur la plateforme Population Registration and Identity Management Eco-system (PRIMES), centralisant les données biométriques de l'UNHCR. https://www.unhcr.org/registration-guidance/chapter3/registration-tools/

[473] https://www.irisguard.com/industry-sectors/liban-post/

[474] BURT, Chris, « UNHCR and Zain wallet use irisguard biometrics for refugees aid disbursement", *BiometricUpdate*, 23/08/2019, https://www.biometricupdate.com/21908/unhcr-and-zain-wallet-use-irisguard-biometrics-for-refugee-aid-disbursement

[475] « IRISGUARD Eyepay partner with Egypt post and UNHCR, the UN refugee agency enabling aid cash transfert for refugees », GSMA,24/02/2020 https://www.gsma.com/get-involved/gsma-membership/gsma_resources/irisguard-eyepay-partner-with-egypt-post and-unhcr-the-un-refugee-agency-enabling-aid-cash-transfer-to-refugees/
"Regional Cash Assistance Monitoring Update– Syria and Iraq situations, January and December 2019",UNHCR
https://reporting.unhcr.org/sites/default/files/UNHCR%202019%20Regional%20Cash%20Assistance%20Monitoring%20Report%20Iraq%20and%20Syria%20Situations%20-%20May%202020.pdf
UNHCR "Cash assistance and Covid 19 : emerging field practices", 2020,https://www.unhcr.org/media/unhcr-cash-assistance-and-covid-19-emerging-field-practices-i

[476] https://www.unhcr.org/media/unhcr-cash-assistance-and-covid-19-emerging-field-practices-i

Plus généralement, le recours à la biométrie au sein du secteur irait croissant, il existerait même une pression de la part des bailleurs pour aller dans ce sens[477]. Et comme le déplore un enquêté : « *il y a cette volonté de course à l'innovation, on s'autorise à pas respecter le reste, une course à l'efficience, contre la fraude, il y a plein d'excuse pour mettre de la biométrie, c'est plus une analyse de la plus-value versus risque qui n'est pas toujours qui n'est pas toujours faite, ça ne veut pas dire qu'elles ne se sont pas posées la question, mais d'autres intérêts ont pris le pas sur les questions de droit*. « [478] Certaines ONG tentent de freiner ce type d'usage. Par exemple, Oxfam a stoppé le développement de la biométrie, pour éditer en 2018 un premier rapport sur le sujet[479]. L'ONG a publié en 2021 une politique de protection de données biométriques. Oxfam a ensuite annoncé un partenariat avec Simprints, une entreprise spécialisée dans le développement de la biométrie dans les pays en voie de développement. Elle affiche une politique respectueuse de la vie privée des bénéficiaires. Cependant Simprints participe à des projets éthiquement discutables comme l'expérimentation de la collecte de biométrie d'enfants en bas âge[480]. Jusqu'alors, il était difficile de collecter des données biométriques de nouveau-nés et de jeunes enfants, leurs caractéristiques physiques n'étant pas encore figées. Des essais ont été conduits en Inde. Ces travaux sont portés entre autres par Anil Jain, un informaticien de l'Université de Michigan. Des essais ont été menés avec le WFP, partenariat pour développer un « proof of concept » pour tester ce que le WFP considère comme un problème : des familles présentant des enfants comme les siens (alors que ce n'est pas le cas) pour obtenir plus d'aide alimentaire. Le test aurait été une réussite : il est possible de recueillir des données biométriques d'enfant de moins de 5 ans, mais davantage d'expérimentations seraient nécessaires pour s'assurer de la réussite de ce concept[481].

Pour conclure, on peut noter que la question de l'expérimentation de technologies lors de crises humanitaires dans des contextes européens sur des citoyens occidentaux reste ouverte. Toujours est-il que si les GAFAM ont pu investir le conflit ukrainien, parfois décrit comme un laboratoire de la numérisation des conflits, la population locale s'est toutefois opposée à la collecte de données biométriques par les humanitaires. Et les ONG ont — pour une fois — pris en compte cette contestation. Cela n'avait pas été le cas au Yémen, où le WFP avait suspendu l'allocation de l'aide en réaction au refus des houthis de se transmettre les données biométriques des yéménites[482].

---

[477] PEROSA, Teresa, TSUI, Quito, "Biometric in the humanitarian sector", *The Engine room*, July 2023https://www.theengineroom.org/wp-content/uploads/2023/07/TER-Biometrics-Humanitarian-Sector.pdf

[478] Entretien n°9, ONG 3, 19/12/19

[479] RAHMAN, Zara," Biometric in the humanitarian sector", *The Engine Room, Oxfam*, 2018 https://reliefweb.int/report/world/biometrics-humanitarian-sector

[480] BURT, Chris,"Consultant sought by Simprints to assess biometric vaccine delivery in Ghana", *Biometricupdate*, 08/03/2024 https://www.biometricupdate.com/202403/consultant-sought-by-simprints-to-assess-biometric-vaccine-delivery-in-ghana
AL AMIN, Mohammad, PRABHU, Maya," Unique and universal : how fingerprint tech is helping get kids protected in Bangladesh", Gavi, 05/10/2023 https://www.gavi.org/vaccineswork/unique-and-universal-how-fingerprint-tech-helping-get-kids-protected-bangladesh

[481] JACOBSEN, Katja, "Biometric data flows and unintended consequences of counterterrorism", *IRRC* No. 916-917 February 2022 https://international-review.icrc.org/articles/biometric-data-flows-and-unintended-consequences-of-counterterrorism-916#footnoteref16_5yqioe0

[482] WILLE, Belkis, "You don't need to demand sensitive biometric data to give aid. The ukraine response shows how", *The New humanitarian*, 11/07/2023 https://www.hrw.org/news/2023/07/11/you-dont-need-demand-sensitive-biometric-data-give-aid-ukraine-response-shows-how

Drones

Il semblerait dans un premier temps que le développement des drones n'a pas suivi la trajectoire d'une première expérimentation humanitaire puis d'une généralisation postérieure à d'autres secteurs. Ce sont en effet les conflits armés qui ont servi de premier laboratoire aux drones. Initialement, ces derniers ont été employés à des finalités militaires, d'abord lors de la Première Guerre mondiale, puis de conflits postcoloniaux, notamment au Vietnam. Et leur essor correspond aux conflits suivant les attentats du 11 septembre 2001, en Irak et en Afghanistan[483]. Ce n'est que dans un second temps, au début des années 2010, que des humanitaires et des civils ont commencé à utiliser des drones[484]. Dans un article datant de 2014, la chercheuse Kristin Sandvik a défendu l'idée que ce transfert technologique d'un usage militaire à un usage humanitaire serait lié à la volonté de « blanchir » l'image des drones. Ils souffraient d'une mauvaise réputation en raison de critiques relatives à leur utilisation pour des assassinats ciblés dans le cadre de la lutte américaine contre le terrorisme. Il s'agissait en outre pour les firmes de relancer un marché qui serait, d'après la chercheuse, mis potentiellement en cause en raison de coupe du budget militaire au début des années 2010[485]. Cette période correspond donc à l'amorce d'un transfert technologique des usages militaires à des usages civils.

L'humanitaire n'aurait pas tant servi de champ d'expérimentation, mais de moyen de légitimation. Par voie de conséquence, les acteurs du marché ont construit l'image d'un « drone humanitaire »[486]. Les humanitaires eux-mêmes tentent de se défaire de la généalogie guerrière des drones et gagner la confiance des populations[487]. En effet, pour tenter de se distinguer des usages militaires, les projets de drones humanitaires ne concernent jamais des zones conflictuelles, et ceux allant dans ce sens n'ont pas donné suite [488]. Leur usage d'abord

---

[483] SANDVIK, Kristin, "African Drone stories", *BEHEMOTH A Journal on Civilization*, 2015, Volume 8 Issue No. 2
GREENWOOD, Faine, "Data colonialism, Surveillance and drones", in : Specht, Doug ( eds.), *Mapping Crisis: Participation, Datafication and Humanitarianism in the Age of Digital Mapping*, University of London Press, 2020.

[484]" while drones demonstrated considerable promise in these early disaster response deployments of the technology, they would not become truly easy to use, widely available, or legal to use in most countries until the late 2010s. The 2013 introduction of the DJI Phantom drone and the growing popularity of the DIY drone building hobby combined to launch drones into the mainstream around the world. " » Bien que les drones se soient révélés très prometteurs lors de ces premiers déploiements de la technologie dans le cadre des interventions en cas de catastrophe, ce n'est qu'à la fin des années 2010 qu'ils sont devenus véritablement faciles à utiliser, largement disponibles ou légaux dans la plupart des pays. L'introduction en 2013 du drone DJI Phantom et la popularité croissante de la construction de drones par des particuliers se sont conjuguées pour démocratiser l'usage des drones partout dans le monde. « GREENWOOD, Faine, JOSEPH, Dan, "Aid from the air : a review of drone use in the RCRC global network", *American Red Cross*, August 2020 https://americanredcross.github.io/rcrc-drones/Aid_from_the_Air.pdf

[485] Cette baisse de vitesse est relativisée par d'autres chercheurs et spécialistes du secteur. ROZEC, Yann, " Le marché des drones militaires toujours florissant", *Le Monde diplomatique*, Décembre 2013 https://www.monde-diplomatique.fr/2013/12/ROZEC/49975
Et aujourd'hui le marché du drone militaire est présenté comme étant en pleine expansion https://www.polytechnique-insights.com/tribunes/geopolitique/quelles-tendances-sur-le-marche-des-drones-militaires/#note-content-1

[486]SANDVIK, K. B., LOHNE, K., "The Rise of the Humanitarian Drone: Giving Content to an Emerging Concept", *Millennium*, 2014, *43*(1),p. 145-164. https://doi.org/10.1177/0305829814529470
BERGTORA SANDVIK, Kristin, JUMBERT, GABRIELSEN, « Les drones humanitaires », *Revue internationale et stratégique*, 2015,n° 98, p. 139-146

[487] GREENWOOD, Faine, "Drones and distrust in humanitarian aid", *ICRC*, 22/07/2021 https://blogs.icrc.org/law-and-policy/2021/07/22/drones-distrust-humanitarian/

[488] BORGER, Julian, "US and UK explore possibility of aid airdrops in Syria", *The Guardian*, 04/12/2016https://www.theguardian.com/world/2016/dec/04/us-uk-explore-possibility-aid-airdrops-syria-drones
JACOBSEN, Mark, "The dubious prospects for cargo-delivery drones in Ukraine", *War on the rocks*, 25/05/2022
https://warontherocks.com/2022/05/the-dubious-prospects-for-cargo-delivery-drones-in-ukraine/
WILDER, Shelby, "In Ukraine, humanitarian drones can save lives", *Al Jazeera*, 09/09/2022
https://www.aljazeera.com/news/2022/9/9/in-ukraine-humanitarian-drones-can-save-lives

limité à différents tests (à Haïti en 2010, au Népal en 2015) s'est démocratisé. On aurait même assisté à une appropriation individuelle d'une technologie, ainsi qu'au développement de pratiques d'amateurs éclairés[489]. Les ONG utilisent surtout les drones pour des projets de cartographie, et de façon plus marginale pour des projets de livraison de petit matériel (des médicaments par exemple). Ils permettent de produire des cartes de zones de catastrophe ou de camps de réfugiés[490]. Et surtout, il existe aussi un bon nombre de projets de cartographies participatives défendant l'inclusion de populations locales. Des ONG comme Humanitarian Open street map, Missing Map, Webrobotic, FLying Lab, etc., soutiennent un usage émancipateur des drones[491]. L'exemple des drones permettrait de nuancer la thèse du technocolonialisme. D'autant qu'il semblerait que les individus peuvent bricoler leur drone, voire en fabriquer de façon artisanale[492]. Soit l'idée opposée d'un développement expérimental d'un dispositif numérique impulsé de façon verticale par des entreprises. Et une ONG comme Webrobotic et le Flying Lab s'inscrivent clairement dans la tradition DIY des « makers ». Ces derniers misent aussi sur un développement local en cohérence avec l'agenda de localisation de l'aide[493]. Werobotics, dont le siège est en Suisse, chapeaute une série de laboratoires locaux situés dans une trentaine de pays du Sud. L'organisation met en avant une série de caractéristiques favorisant la localisation de l'aide : partenariats avec des acteurs de la « société locale » du pays concerné, possibilité pour les ateliers de mener ses propres programmes au niveau local, gouvernance horizontale[494], etc. Plus généralement, la localisation de l'aide serait une façon d'atténuer les effets de dominations propres au « colonialisme de la donnée ». Et comme le déclare Faine Greenwood : « Les connaissances locales et contextuelles protègent contre les processus de colonisation des données et le fait d'impliquer plus étroitement les personnes dans les processus de protection des données leur donne une chance de conserver un pouvoir sur les informations qui sont collectées à leur

---

HOFMAN, Michiel, « Drones humanitaires : des outils utiles, une image toxique », *Alternatives humanitaires*, n°8,2018
https://www.alternatives-humanitaires.org/fr/2018/07/03/drones-humanitaires-outils-utiles-image-toxique/#r+20688+1+1
"NGOs against MONUSCO drones for humanitarian work", *The new humanitarian*, 23/07/2014
https://www.thenewhumanitarian.org/analysis/2014/07/23/ngos-against-monusco-drones-humanitarian-work
SANDVIK, Kristin, GABRIELSEN JUMBERT, Maria (ed.), *The Good drone*, Routledge, 2016, 212 p

[489]JABLONOWSKI, Maximilian, "Drone It yourself : on the decentring of drone stories", *Culture machine*, 2015, 16, p.1-15

[490] Une des premières expérimentations de drones humanitaires date de 2007. Le WFP avait alors testé un prototype de drone à l'Université de Turin. En 2010, les USA ont utilisé des drones militaires Predator et de l'imagerie satellitaire à Haïti (ainsi qu'en Bosnie ou aux Philippines) pour cartographier l'étendue des dommages à la suite d'un tremblement de terre. L'OIM a obtenu en 2012 une autorisation de vol pour ce type d'aéronef pour des projets similaires. Des drones ont été déployés après le Typhon Haiyan en 2013 avec le même objectif, puis au Népal en 2015 après un tremblement de terre.
MEIER, Patrick, "UN World food program to use UAVs", *Irevolution*, 09/04/2008,
https://irevolutions.org/2008/04/09/un-world-food-program-to-use-uavs/
Using High-resolution Imagery to Support the Post-earthquake Census in Port-au-Prince, Haiti", in "Drones in humanitarian action, a guide to the use of airborne systems in humanitarian crises", CartONG, Uaviators, 2016
WANG, Ning, ""We Live on Hope...": Ethical Considerations of Humanitarian Use of Drones in Post-Disaster Nepal," in *IEEE Technology and Society Magazine*, vol. 39, no. 3, p. 76-85, Sept. 2020, doi: 10.1109/MTS.2020.3012332.

[491] DOUG, SPECHT, *Mapping Crisis Participation, Datafication and Humanitarianism in the Age of Digital Mapping*, University of London Press, 2020,276 p.

[492] DE MATHAREL, Lelia, "Les technologies en kit : drone It yourself, pour fabriquer votre quadricoptère", *L'Usine digitale*, 25/03/2014 https://www.usine-digitale.fr/article/les-technologies-en-kit-drone-it-yourself-pour-fabriquer-votre-quadricoptere.N250687

[493] On trouverait des premières traces de cet impératif au milieu des années 2000, l'expression s'est depuis ancrée dans les discours et normes humanitaires. Il s'agit de rééquilibrer les relations entre parties prenantes, en donnant plus de place aux organisations locales dans la délivrance des programmes. Coordination sud, la localisation de l'aide plus de proximité permet-il d'assurer l'autonomie des projets déployés. Coordination sud, *La localisation de l'aide, plus de proximité permet-il d'assurer l'autonomie des projets déployés?*, 2019 https://www.coordinationsud.org/wp-content/uploads/synthese-etude-localisation-aide.pdf
CHENEY, Catherine, « A robotics group offers ideas to 'shift power' to drive localization », *Devex*, 14/04/ 2022,https://www.devex.com/news/a-robotics-group-offers-ideas-to-shift-power-to-drive-localization-102987

[494] "What is the power footprint of International Organizations?", *WeRobotics*, 11/10/2021 https://werobotics.org/blog/power-footprint-ingos/

sujet. »[495] De manière générale, les initiatives visant à localiser l'aide ne sont pas exemptes de dynamiques de pouvoir, des inégalités[496]. Dans notre cas, le projet FLyinLab reste marqué par des formes de dépendance en termes d'infrastructures et de financements. Concernant les FLyinLab, cette question nécessiterait pour le coup des recherches supplémentaires, sur le terrain. Mais notons simplement que le modèle économique des FlyingLab est encore relativement dépendant de financements internationaux. En effet, les FlyingLab ont pu recevoir des fonds transitant par Werobotic [497] ; mais également par des bailleurs américains et australiens, de la Banque mondiale, la Rockefeller foundation, l'Hewlett Parckard Foundation[498], ou encore de Pfizer qui a financé un projet de Cargo Drone en République dominicaine, en partenariat avec la compagnie allemande Wingcopter[499].

Et surtout, malgré leur proximité avec un imaginaire « maker », la plupart des drones ne sont pas produits sur place et il reste difficile de les réparer en raison d'un manque d'accès à des pièces de rechange, d'où une dépendance pouvant même selon Webrobotics être entretenue par les entreprises elles-mêmes[500]. Et dans le cas des drones civils, le principal fournisseur est non pas américain ou européen, mais en l'occurrence chinois, comme le rappelle Faine Greenwood. La compagnie chinoise Da jiang innovation (DJI) représente plus de 70 % des drones grand public aux Etats-Unis[501]. Par exemple, les FlyingLab de Werobotics utilisent pour certains de leurs projets ce type de drone peu couteux[502], quand bien même des initiatives existent pour localiser la production[503]. On ne dispose pas de statistiques sur le degré de dépendance à DJI par le réseau FlyingLab. Toujours est-il que la compagnie chinoise est bannie

---

[495] "Local, contextual knowledge is protective against processes of data colonialism and involving people more closely in data protection processes gives them a chance to maintain agency over information that is collected about them."
GREENWOOD, Faine, "Data Colonialism, Surveillance Capitalism and Drones", in : DOUG, Specht (ed.), *Mapping Crisis: Participation, Datafication and Humanitarianism in the Age of Digital Mapping*, University of London Press, 2020, p. 89–118.

[496] SCHRODER-BERGEN, Susanne, GLASZE, Georg, MICHEL, Boris, "De/colonizing OpenStreetMap? Local mappers, humanitarian and commercial actors and the changing modes of collaborative mapping", *GeoJournal*, 2021, 87 (5)
SHUAYB, Maha, "localisation only pays lip service to fixing aid's colonial legacy", *The new humanitarian,* 08/02/2022https://www.thenewhumanitarian.org/opinion/2022/2/8/Localisation-lip-service-fixing-aid-colonial-legacy
PLOWRIGHT, William, "The imperial past and decolonised future of humanitarian action", *Alternatives humanitaires*, n°25, March 2024https://www.alternatives-humanitaires.org/en/2024/03/20/the-imperial-past-and-decolonised-future-of-humanitarian-action/
PATEL, Smruti, "Localisation, racism and decolonisation: hollow talk or real look in the mirror?", *Humanitarian Practice Network*, 29/09/2021https://odihpn.org/publication/localisation-racism-and-decolonisation-hollow-talk-or-real-look-in-the-mirror/
Cartong, "Changer de perspective : pour une approche locale de la donnée, débats et défis de la localisation de l'aide et de la gestion de données", Janvier 2024 https://www.im-portal.org/Changer-de-perspective-pour-une-approche-locale-de-la-donn%C3%A9e

[497] "While just 5% of funding from international organizations directly reached local and national groups in 2020, WeRobotics transferred 38% of its revenue to Flying Labs that year."
Werobotics, "The majority of localization efforts have failed, this one continue to shine",25/01/2022 https://werobotics.org/assets/Documents-Reports-PDF/Localization-A-Success-Story.pdf

[498] « La start-up a la particularité d'être à but non lucratif. Elle est soutenue avant tout par des fondations, comme Rockefeller, Hewlett, Autodesk, mais aussi Usaid, l'Agence des Etats-Unis pour le développement international. L'équipe de Sonja Betschart bénéficie aussi de soutiens comme celui du Forum économique mondial (WEF) – la cofondatrice est cette semaine invitée par celui-ci à son événement de Tianjin, en Chine. «Nous sommes toujours en train de lever des fonds. Et à moyen terme, nous visons à ce que les Flying Labs soient entièrement autofinancés. A priori, WeRobotics ne sera jamais une grande société, notre but est vraiment que les acteurs locaux grandissent en nombre et créent des services viables et utiles autour des drones» » SEYDTAGHIA, Anouch, "WeRobotics, des drones au chevet des pays émergents", Le Temps, 20/09/2018 https://www.letemps.ch/cyber/werobotics-drones-chevet-pays-emergents

[499]WEROBOTICS, "Field-Testing Cargo Drones for Medicine Deliveries in Rural Environments of the Dominican Republic", november 2019

[500] Werobotics, "The right to repair, technology for Good", 22/07/2021, https://werobotics.org/blog/the-right-to-repair-technology-for-good/

[501] NORMAND, Jean-Michel, « Drones civils: face à l'offensive américaine, le chinois DJI contre-attaque », *Le Monde*, 27/09/2019 https://www.lemonde.fr/economie/article/2019/09/27/drones-civils-face-a-l-offensive-americaine-le-chinois-dji-contre-attaque_6013263_3234.html

[502]MURISON, Malek," How the DJI M300 is Being Used to Deliver Medical Supplies & Drive Decentralization", *DJI blog*, 14/07/2022 https://enterprise-insights.dji.com/blog/werobotics-m300-cargo-medical-delivery

[503]"Expanding technology access by designing a low-cost drone", 22/03/2021, *Flying labs* https://blog.flyinglabs.org/2021/03/22/expanding-technology-access-by-designing-a-low-cost-drone/

par l'armée américaine[504]. À cette date, il n'est pas encore question d'interdire totalement son import aux États-Unis — quand bien même cela a été envisagé[505] : dans le cadre de la guerre économique sino-américaine, les agences de sécurité américaines alertent régulièrement sur les risques de cybersécurité des drones DJI[506]. Cette dépendance à un fournisseur fortement marquée par des jeux géopolitiques d'opposition de grandes puissances nuance donc la thèse d'une localisation technologique.

L'idée que les drones participent de la localisation de l'aide peut être nuancée, mais surtout l'usage de drones à des finalités de cartographie serait « peu » couteux, contrairement aux « drones » destinés aux livraisons, dont l'usage civil est encore peu répandu, jusqu'alors seuls les modèles militaires ont des capacités de charge conséquentes, ces derniers pouvant avoir jusqu'à vingt mètres d'envergure et transporter plusieurs centaines de kilos. La plupart des projets de livraison sont de charge plus modeste que les drones militaires, mais demandent des investissements conséquents et sont menés par des startup pouvant bénéficier de levées de fonds importantes ( comme les compagnies américaines Zipline, ou Matternet). Encore une fois, Werobotics ambitionne de contester ce modèle. Depuis 2016, l'organisation chapeaute une série de projets d'expérimentation de drone de livraison ; en le présentant comme étant « décolonial », et en mettant l'accent sur la nécessité de nouer des partenariats avec de plus « petits » joueurs, pour éviter que le marché soit concentré aux mains de compagnies américaines[507]. Depuis 2016, Werobotics soutient des expérimentations de drones cargo au sein des antennes Flyinglab. Ainsi au Népal, une série de vols de drones de livraison a été conduite avec Dronelp, une compagnie népalaise. Notons tout de même qu'une série de partenariats semble nuancer la politique d'indépendance et d'ancrage local de l'organisation. Les FLying lab ont travaillé aux Fiji et au Brésil avec Redwing[508], une compagnie indienne de drone de livraison. Cette dernière est financée, d'après son profil Forbes, par des fonds d'investissement américains (Techstar, Asymetry Venture, Cloud Capital, mais aussi Lestventure Beyond Capital (fonds philanthropique basé en Inde)[509]. Et un projet mené au

[504]GREENWOOD, Faine, "The world is dependent on drones made by just one chinese company - and that's a problem," *Faineg,* 08/08/2023 https://faineg.com/the-world-is-dependent-on-drones-made-by-chinas-dji-and-thats-a-problem/

[505]"U.S department of Defense, Department statement on DJI Systems", 23/07/2021. https://www.defense.gov/News/Releases/Release/Article/2706082/department-statement-on-dji-systems/

[506] "US warns of potential data leaks from Chinese-made drones", *Financial times*, 20/05/2019 https://www.ft.com/content/b4193d5e-7b2b-11e9-81d2-f785092ab560

[507] « Dans le cadre d'un projet avec les Centres de contrôle et de prévention des maladies en Papouasie-Nouvelle-Guinée, WeRobotics s'est associé à Redwing Labs, une jeune entreprise indienne, plutôt qu'à des sociétés plus connues comme Swoop Aero ou Wingcopter. Ce mois-ci, WeRobotics lance trois projets différents de drones cargo avec trois laboratoires volants dans trois pays, et le renforcement des capacités et le transfert de technologie sont au cœur de chacun des projets, a déclaré M. Meier. Le renforcement des capacités et le transfert de technologies sont au cœur de chacun de ces projets. L'espoir est qu'au fil du temps, moins de pays devront se tourner vers l'extérieur pour obtenir de l'expertise en matière de drones. Les détracteurs de Zipline se sont inquiétés du fait que les entreprises qui effectuent leurs tests dans les pays en développement pourraient partir dès que de nouveaux marchés plus rentables s'ouvrent à elles" ».”In a project with the Centers for Disease Control and Prevention in Papua New Guinea, WeRobotics partnered with Redwing Labs, an Indian startup, rather than going with better-known companies such as Swoop Aero or Wingcopter.This month, WeRobotics is launching three different cargo drone projects with three flying labs in three countries, and capacity building and technology transfer is central to each of the projects, Meier said. The hope is that over time, fewer countries will have to look beyond their borders for drone expertise. Critics of Zipline have expressed concerns that companies doing their testing in developing countries might leave as soon as new and more profitable markets open up." CHENEY, Catherine, "What role should donors play in helping drones for delivery take flight?", *Devex*, 20/05/2019https://www.devex.com/news/what-role-should-donors-play-in-helping-drones-for-delivery-take-flight-94895

[508]« redwing labs joins flying labs network as technology partner », *We robotics*, 11/05/2022 https://werobotics.org/blog/redwing-labs-joins-flying-labs-network-as-technology-partner
MEIER, Patrick, "Decolonizing Medical Cargo Drone Technology: Step 1", *I revolution*, 25/11/2019, https://irevolutions.org/2019/11/25/decolonizing-medical-cargo-drone-technology-step-1/

[509] https://www.forbes.com/profile/redwing-labs/

Pérou a été réalisé avec un financement de la Becton, Dickinson and Company (BD)[510], une multinationale étatsunienne commercialisant des services médicaux. La Becton Dickinson and company aurait pris part au projet et comme on peut le lire dans un rapport publié par Werobotics : « L'entreprise est déjà présente au Pérou. BD était donc particulièrement intéressé par notre approche communautaire de la robotique et par la possibilité d'apprendre par la pratique afin de mieux comprendre les possibilités et les limites de l'utilisation de drones cargo plus abordables pour la livraison de marchandises diverses entre des cliniques et des villages isolés. » [511]

Werobitics a aussi mené un projet en République dominicaine, toutefois en partenariat avec le laboratoire Pfizer américain pour des livraisons de vaccins contre le Covid19, avec des financements de la Bill &Bellinda Foundation, et au Ghana c'est avec la compagnie Zipline étatsunienne que Werobotics s'est associé[512]. Or Zipline fait partie des principales compagnies de livraisons avec Matternet et Wingcopper. Toutes les trois ont investi le terrain humanitaire et ont noué des partenariats avec des ONG, en 2014 avec MSF en Papouasie Nouvelle-Guinée[513], avec l'OMS au Bhoutan[514], puis en 2017 au Malawi et en 2018 au Kazakhstan avec UNICEF[515], cette dernière a également un projet au Vanuatu avec une compagnie de drone indienne en 2018 [516]. Ainsi, un projet présenté comme s'inscrivant dans l'agenda de localisation de l'aide et ambitionnant une approche « décoloniale » de l'innovation, reste en partie ancré dans les circuits financiers propres à l'économie de la santé globale.

L'humanitaire constituerait donc un terrain d'expérimentation pour ces entreprises, mais c'est surtout l'Afrique qui a acquis l'image de « laboratoire » idéal pour les drones[517]. Le continent serait en effet doté d'un cadre juridique jugé plus souple, d'autorités de gouvernance du trafic aérien encore faibles[518] et d'un trafic aérien moindre. Dans le même temps, le continent

---

[510]"Fleet of cargo drones tested in the Amazon", *We Robotics*, 18/10/2017, https://werobotics.org/blog/cargo-drones-tested-amazon/

[511] "Unlike our previous field tests in the Amazon, this time we had the opportunity to work directly with one of the leading medical technology companies in the world, BD. The company already has operations in Peru, so BD was particularly interested to learn more about our community-based approach to robotics and to learn-by-doing with us to better understand the opportunities and limitations around using more affordable cargo drones to deliver a range of cargo between clinics and remote villages. The BD team's deep understanding of the public health space made these field tests far more relevant for everyone involved. Their partnership was an invaluable opportunity for us and our Flying Labs team to better understand the health care challenges in the region and how cargo drones could potentially address some of these challenges and thus make a very real and meaningful difference for the lives of many in the Amazon." "WeRobotics Report Cargo Drone Field Tests in the Amazon », October 2017, *We Robotics* https://werobotics.org/assets/Documents-Reports-PDF/WeRobotics-Report-on-Drone-Cargo-Field-Tests-Peru-2017.pdf

"Why drone mapping is key for cargo drone delivery", Flying Labs, 04/09/2020[512] https://blog.flyinglabs.org/2020/09/04/why-drone-mapping-is-key-for-cargo-drone-delivery/

[513] "Using Drones for Medical Payload Delivery in Papua New Guinea", in "Drones in humanitarian action, a guide to the use of airborne systems in humanitarian crises", CartONG, Uaviators, 2016

[514] DIORIO, David R.," Operation Unified Response, Haiti Earthquake 2010", Joint Forces Staff College, 2010, http://jfsc.ndu.edu/Portals/72/Documents/JC2IOS/

[516] "Vanuatu awards international drone companies with commercial contracts for vaccine delivery", 25/10/2018 https://www.unicef.org/pacificislands/press-releases/vanuatu-awards-international-drone-companies-commercial-contracts-vaccine-delivery

[517] HOCHET-BODIN, Noé, "L'Afrique, nouveau terrain de jeu des exportateurs de drones", *Le Monde*, 27/12/2023 https://www.lemonde.fr/afrique/article/2023/12/27/l-afrique-nouveau-terrain-de-jeu-des-exportateurs-de-drones_6207953_3212.html

[518]Sur ce point, le directeur de Zipline, une compagnie de drone de livraison, est clair : «De nombreux opérateurs de drones commerciaux aux États-Unis attendent l'autorisation de la FAA (Federal Aviation Authority). Mais la FAA dit « nous voulons plus de données ». Mais personne ne vole. Je pense donc que [...] l'une des meilleures façons de collaborer avec la FAA pour aider cette technologie à décoller aux États-Unis est d'opérer dans un pays où nous pouvons répondre à un besoin très clair et obtenir des dizaines de milliers d'heures de données de vol en toute sécurité. » ; « A lot of commercial [drone] operators in the US are waiting to get permission from the FAA [Federal Aviation

souffrirait d'un manque d'infrastructures routières[519]. C'est en tout cas l'argumentation régulièrement reprise par plusieurs promoteurs du drone africain, comme Jonathan Ledgard et Norman Foster, concepteurs du premier « droneport » au Rwanda, ou comme Andreas Raptopoulos, le directeur de Matternet[520]. Cependant, en dépit de l'image d'un espace aérien « vierge », sorte de « caelum nullius »[521] à conquérir, l'Afrique est loin d'être un vide juridique en matière de régulation des drones et des couloirs aériens. De nombreux pays du continent sont certes dépourvus de cadre juridique sur ce point, mais la situation évolue et plusieurs États se sont dotés d'une régulation : l'Afrique du Sud, le Rwanda, le Ghana, la Tanzanie et le Kenya. Concernant le Rwanda, le pays joue la carte de l'innovation et a adopté depuis 2019 un cadre favorable à l'usage de drone. Mais dans le même temps, le gouvernement rwandais maintient un relatif contrôle des projets de drones[522], comme l'a montré le chercheur Andy Lockhart. Et de fait, selon lui, seule une compagnie — Zipline — a pu s'implanter de façon durable dans le pays. Ce choix fait écho à l'alliage entre développementalisme et autoritarisme propre aux États africains des années 1970[523]. Cela dit, il faut aussi noter l'influence dans la mise en place de régulation d'acteurs privés, comme des organisations internationales, le Forum économique mondial en l'occurrence a pu participer à l'élaboration du cadre normatif rwandais [524]. Enfin, de manière plus générale, il est également nécessaire de prendre en compte les moyens déployés pour la mise en œuvre du cadre législatif. Au-delà du terrain africain, on pense au cas du Népal. Ce pays a adopté une loi régulant l'usage de ce type d'engin volant après un tremblement de terre en 2015,où les drones avaient été massivement employés à des fins de secours, mais sans cadre clair[525]. Mais d'après la chercheuse Ning Wang le Népal — n'aurait pas les moyens ni l'expertise requise pour contrôler l'usage de ces derniers sur son territoire et assurer la souveraineté de son espace aérien[526].

Pour illustrer les différents points qu'on a évoqués dans les lignes précédentes, on peut évoquer le cas de Zipline, une des principales compagnies de drones de livraison de produits médicaux. Fondée en 2011, de premières expérimentations ont lieu en Californie, mais très

---

Authority]. But the FAA is saying "we want more data." But no one is actually flying. So, I actually think that […] one of the best ways that we can work together with the FAA to help this technology take off in the US is by operating in a country where we can basically serve a very clear need and get tens of thousands of hours of safe flight data." WYROBEK, Keenan, " Drone Keynote", TiEcon 2017

[519] BURCHARDT, Marian, UMLAUF, René, "Dreams and realities of infrastructural leapfrogging: airspace, drone corridors, and logistic in African healthcare, in BURCHARDT, Marian, LAAK, Dirk (ed.), *Making spaces through infrastructure : visions, technologies, and tensions*,Berlin, De Gruyter Oldenbourg, 2023,276 p.

[520] GEORGE, Alison, "Forget roads-drones are the future of good transports", *NewScientist,* 04/09/2013 https://www.newscientist.com/article/mg21929334-900-forget-roads-drones-are-the-future-of-goods-transport/

[521] l'expression "caelum nullius" fait écho à celle de « terra nullius », soit l'image d'une terre vierge, n'appartenant à aucun Etat, libre d'être conquise par un colonisateur.

[522] LOCKHART, Andy, WHILE, Aidan, MARVIN, Simon, KOVACIC, Mateja, ODENDAAL, Nancy, ALEXANDER, Christian, "Making space for drones: the contested reregulation of airspace in Tanzania and Rwanda", *Transactions of the institute of british geographers*, Volume 46, 4, 2021, p.850-865

[523] LOGEZ, Hugo, « Dérives autoritaires et retour de l'autoritarisme en Afrique de l'Ouest », *Fondation Jean Jaurès*, 15/11/2021 https://www.jean-jaures.org/publication/derives-autoritaires-et-retour-de-lautoritarisme-en-afrique-de-louest/

[524] "Accelerating the adoption of drone technology through regulatory change", *World economic forum*, october 2020, https://www3.weforum.org/docs/WEF_C4IR_Case_Study_Drones_in_Rwanda_2020.pdf

SOULE, Folashadé, « Rivalités géopolitiques et partenariats numériques en Afrique, stratégies d'adaptation et défis », *IFRI*, décembre 2023 https://www.ifri.org/sites/default/files/atoms/files/ifri_soule_partenariats_numeriques_afrique_2023.pdf

[525] HERN, Alex, "Nepal moves to limit drone flights following earthquake", THe Guardian, 06/05/2015https://www.theguardian.com/technology/2015/may/06/nepal-moves-to-limit-drone-flights-following-earthquake

[526] WANG, Ning et all., "Supporting value sensitivity in the humanitarian use of drone through an ethics assessment framework", *International review of the red cross,* 2022, 104, 919, p.1397-1428 https://international-review.icrc.org/sites/default/files/reviews-pdf/2022-06/supporting-value-sensitivity-in-the-humanitarian-use-of-drones-919.pdf

WANG, N., CHRISTEN, M. HUNT, M., "Ethical Considerations Associated with "Humanitarian Drones": A Scoping Literature Review", *Sci Eng Ethics* 27, 51,2021 https://doi.org/10.1007/s11948-021-00327-4

vite l'entreprise choisit de s'implanter sur le terrain africain[527]. Pour le chercheur René Umlauf l'entreprise se serait positionnée sur un marché de niche, pour s'en emparer avant qu'il soit investi par d'autres acteurs plus puissants, comme les GAFAM, sachant que les tentatives de livraisons par drones par Amazon ont été jusqu'alors infructueuses[528] ; son échec est présenté comme étant lié au fait que la régulation du ciel états-unien serait trop contraignant pour les drones de livraison. Toujours est-il que Zipline reste malgré son ancrage africain, une compagnie conservant de forts liens avec les Etats-Unis, où sont situés son siège et son unité de recherche. Parmi ses bailleurs on compte la Fondation Bill & Melinda Gates, UPS et GAVI [529]. Et surtout le modèle de gestion des données de la firme est clairement axé sur l'exploitation de données produite par les drones[530]. Zipline s'intéresse tout particulièrement aux données de vol et aux données météorologiques, ainsi qu'aux données de santé que l'entreprise collecte lors de la commande de matériel médical [531]. D'ailleurs, d'après le chercheur George Macaire Eyenga, le contrat entre Zipline et le ministère de la Santé du Ghana mentionne expressément que ce dernier fournira à l'entreprise l'ensemble des données de son système de santé nécessaire à son fonctionnement[532]. Pour le chercheur René Umlauf, un des objectifs du projet est de collecter des données de vol afin d'améliorer le produit. Cela est d'autant plus intéressant pour l'entreprise que les conditions de vol sont souvent mauvaises : « Une telle prise de risque crée également des données de vol précieuses, une ressource au nom de laquelle le ciel africain et les sols qui s'y trouvent sont transformés en laboratoires lointains de la Silicon Valley. »[533] Après avoir été expérimenté sur des terrains africains, le drone est maintenant prêt à être employé aux Etats-Unis. La compagnie garde cependant un pied dans le continent africain, et déploie ses activités, à la date de 2024, en Côte d'Ivoire, au Kenya et au Nigeria[534]. Aux Etats-Unis, Zipline opère dans l'Arkansas, en Caroline du Nord et dans l'Utah. Zipline a bénéficié du Covid 19 pour pouvoir y développer ses activités [535]. Enfin, elle a obtenu une certification auprès de l'organisme de régulation de

---

[527] EYENGA Georges Macaire, « Une gouvernance sanitaire agile ? L'expérience des drones médicaux dans la gestion de la pandémie du Covid-19 au Ghana », *Cahiers d'études africaines*, 2023/2 (n° 250), p. 315-341. https://www-cairn-info.ezproxy.utc.fr/revue-cahiers-d-etudes-africaines-2023-2-page-315.htm

CASTELLON, T., Alexandre, « The social construction of the humanitarian health drone : socialising the UAV », Mémoire, International relations, 2020, University of Nottingham, https://www.nottingham.edu.cn/en/library/documents/research/global-university-publications-licence-2.0.pdf

[528] DUPONT, Sarah, « Amazon tente de revenir dans la course sur le marché encore émergent de la livraison par drone », *Le Monde*, 17/06/2022 https://www.lemonde.fr/en/economy/article/2022/06/21/amazon-attempts-to-break-into-the-still-emerging-drone-delivery-market_5987542_19.html

https://www.usine-digitale.fr/article/nouvel-episode-dans-le-decollage-poussif-de-prime-air.N2096931

[529] CHENEY, Catherine, "Technology alone won't launch 'drones for good' from pilots to progress", *Devex,* 28/05/2019 https://www.devex.com/news/technology-alone-won-t-launch-drones-for-good-from-pilots-to-progress-94963

[530]"Data-driven drones deliver lifesaving medical aid around the world", Databricks https://www.databricks.com/customers/zipline

[531] Center for Global Development, "Drone Delivery of PPE and Test Kits for COVID-19", https://www.youtube.com/watch?v=z50lBJ4Vsjo

[532] MACAIRE, EYENGA, George, « Drone médicaux, Comment Zipline redéfinit la délivrance des soins de santé en Afrique », *Afrique XXI,* 07/09/2022 https://afriquexxi.info/Comment-Zipline-redefinit-la-delivrance-des-soins-de-sante-en-Afrique

[533] "such risk taking also creates valuable flight data, a resource in the name of which African Skies and the grounds below them are turned into Silicon Valley's distant laboratories."

UMLAUF, R., BURCHARDT, M. "Infrastructure-as-a-service: Empty skies, bad roads, and the rise of cargo drones", *Environment and Planning A: Economy and Space*, *54*(8), 2022, p. 1489-1509. https://doi.org/10.1177/0308518X221118915

[534]VELLUET, Quentin, « Côte d'Ivoire, Rwanda, Ghana...Les drones de Zipline boostés par une nouvelle levée de fonds », *Jeuneafrique*, 05/05/2023 https://www.jeuneafrique.com/1442743/economie-entreprises/cote-divoire-rwanda-ghana-les-drones-de-zipline-boostes-par-une-nouvelle-levee-de-fonds/

BOULARD, Laure, « Comment Zipline a fait de l'Afrique le tremplin de ses drones de livraison », *Le Monde*, 20/03/2023 https://www.lemonde.fr/afrique/article/2023/03/20/comment-zipline-a-fait-de-l-afrique-le-tremplin-de-ses-drones-de-livraison_6166291_3212.html

[535] BROULARD, Laure, « Au Rwanda, le confinement accélère la livraison de médicaments par drones », *Le Monde*, 04/05/2020 https://www.lemonde.fr/afrique/article/2020/05/04/au-rwanda-le-confinement-accelere-la-livraison-de-medicaments-par-drones_6038597_3212.html

l'espace américain, la Federal aviation administration (FAA) en septembre 2023[536], 10 ans après sa création. Zipline se concentre toujours dans le secteur médical, mais elle a investi également le secteur de la grande distribution avec Walmart, et projette de collaborer avec une chaine de restauration rapide, SweetGreen[537].

Zipline est une compagnie dont l'objectif est clairement commercial, ce n'est pas le cas de Matternet ou Wingcopter qui ont pour partenaires des ONG humanitaires. Ainsi Matternet a mené des vols d'essai en Papouasie Nouvelle-Guinée en 2014, au Bhoutan avec l'OMS en 2015, au Malawi avec Unicef en 2017[538], et en Papouasie Nouvelle-Guinée avec MSF[539]. « À l'époque, la plateforme Matternet était encore en cours de développement et n'était donc pas encore aussi mature que les versions Matternet One ou Matternet Two. » [540] Un « corridor » de vol a été ouvert au Malawi en 2017. Sachant que ce terme désigne pour Unicef : « une plateforme contrôlée pour le secteur privé, les universités et d'autres partenaires pour explorer comment les drones, également connus sous le nom de véhicules aériens sans pilote (UAV), peuvent aider à fournir des services qui profitent aux communautés et aux écoles. »[541]Mais contrairement à Zipline dont le projet est mieux implanté au Rwanda, ce ne sont que des essais localisés. Le projet d'UNICEF est maintenu, mais reste limité à différents tests dans des corridors de vols, sans que cela débouche sur des vols pérennes. Ce type de projet dépend en grande partie de financement de bailleurs. Ce sont des expérimentations ponctuelles dont les retombées sur place seraient limitées[542]. L'expérience a néanmoins été utile à Matternet. Après s'être concentrée sur le marché africain, la compagnie semble se repositionner progressivement sur le terrain occidental. Elle a mené un vol en Suisse, à Berlin, et a pu obtenir un certificat de vol par l'agence américaine d'aviation en 2022[543], une première

[536] "Federal aviation administration, FAA Authorizes Zipline International, Inc. to Deliver Commercial Packages Using Drones That Fly Beyond Operator's Line of Sight", 18/09/2023 https://www.faa.gov/newsroom/faa-authorizes-zipline-deliver-commercial-packages-beyond-line-sight

[537] KONRAD, Alex, CAI, Kenrick, "Drone delivery startup Zipline boost valuation to $4,2 billion", *Forbes,* 28/11/2023 https://www.forbes.com/sites/alexkonrad/2023/04/28/drone-delivery-startup-zipline-boosts-valuation-to-4-billion/?sh=582a75c35846
ROTH, Emma, "Walmart is bringing drone deliveries to 1,8 million more texas households", *The Verge*, 09/01/2024 https://www.theverge.com/2024/1/9/24031714/walmart-drone-delivery-wing-zipline-dallas-fort-worth-texas

[538] MURRAY BUECHNER, Maryanne, "how UNICEF is using drones to save lives in Malawi", *Forbes*, 06/01/2016 https://www.forbes.com/sites/unicefusa/2017/01/06/how-unicef-is-using-drones-to-save-lives-in-malawi/?sh=59849d336206
BLAUVELT, Carla, ZIBA, Matthew, "Could UAVS reduce waiting time for pediatric HIV test results?" *VillageReach*, 28/03/2016https://www.villagereach.org/2016/03/28/looking-to-the-sky-for-answers-understanding-the-cost-of-uavs-at-the-last-mile/ https://www.villagereach.org/2016/03/28/looking-to-the-sky-for-answers-understanding-the-cost-of-uavs-at-the-last-mile/

[539]" Using drones for medical payload delivery in Papua New Guinea", *Zoinet*, 2018 https://zoinet.org/wp-content/uploads/2018/01/2Case-Study-PapuaNewGuinea.pdf

[540]ibid. "At the time, the Matternet platform was still under development and thus not yet as mature as the Matternet One or Matternet Two versions."

[541] "a controlled platform for the private sector, universities and other partners to explore how drones, also known as unmanned aerial vehicles (UAVs), can help deliver services hat benefit communities and schools."
Unicef, "Humanitarian drone corridor launched in Malawi", 23/08/2017 https://www.unicef.org/stories/humanitarian-drone-corridor-launched-malawi

[542] CHENEY, Catherine, "Technology alone won't launch 'drones for good' from pilots to progress", Devex, 28/05/2019https://www.devex.com/news/technology-alone-won-t-launch-drones-for-good-from-pilots-to-progress-94963
PHILIPPS, N., BLAUVELT, C., ZIBA, M., SHERMAN, J., SAKA, E., BANCROFT, E., WILCOX, A. "Costs Associated with the Use of Unmanned Aerial Vehicles for Transportation of Laboratory Samples in Malawi. Seattle: VillageReach, 2016 https://www.villagereach.org/wp-content/uploads/2017/06/Malawi-UAS-Report_MOH-Draft_-FINAL_14_07_16.pdf
European Commission, Innovation in the skies: bridging gaps and breaching barriers in Malawi, International Partnerships, 2020https://international-partnerships.ec.europa.eu/policies/programming/projects/innovation-skies-bridging-gaps-and-breaching-barriers-malawi_en

[543] Matternet M2 Drone Delivery System First to Achieve FAA Type Certification,07/09/2022 https://www.mttr.net/images/Matternet_Press_M2_Type_Certificate_20220907.pdf

pour ce type d'entreprise[544]. Matternet semble s'être retirée du terrain humanitaire[545], et UNICEF continue ses expérimentations avec une firme allemande, plus récente, Wingcoper. On peut faire l'hypothèse que comme Zipline les données générées par les drones lui ont été utiles pour améliorer son produit, il faut effectivement savoir que les drones Matternet sont fournis avec un cloud (géré par Cisco, fournisseur américain) [546]et une application mobile, utilisée pour la gestion des plans de vol.

En somme, le cas des drones est relativement contrasté : ce type de technologie a été approprié par des acteurs souhaitant développer un usage plus inclusif du numérique, dans une logique de localisation de l'aide, remettant en cause les dynamiques post-coloniales. Mais ces dernières ne sont pas exemptes de dépendances financières, et s'inscrivent dans le marché de la santé globale, du fait de leurs bailleurs, tandis que si les drones à des finalités de cartographies peuvent être plus facilement appropriable par de petites structures, locales, les drones cargo restent en majeure partie expérimentées par des entreprises ayant soit un modèle extractif, basé sur l'exploitation des données de vol et potentiellement de santé, soit comme objectif un redéploiement plus large, avec des finalités plus clairement commerciales.

Mobilité et données massives : du « big data disaster » au « data for good

Dans cette section, on s'intéressera aux initiatives de type « data for good ». Ces dernières consistent à tirer profit de données privées pour le bien commun et à des finalités sociales et humanitaires. Soit une façon de remettre en cause les mécanismes extractifs du « data colonialisme » ?

Au tournant des années 2010, il s'est progressivement constitué un réseau d'acteurs défendant l'usage de données massives afin de soutenir des projets humanitaires[547]. La numérisation accrue du secteur générant une vaste quantité de données, l'exploitation de ces dernières a semblé constituer une bonne opportunité afin d'outiller les humanitaires et produire de meilleures analyses en contexte de crise. Ont vu ainsi le jour des projets comme le « Displacement Tracking Matrix »[548], en français la « matrice du suivi des déplacements ». Il s'agit d'un système mis en place par l'OIM ayant pour finalité d'objectiver des trajectoires

---

[544] CHENEY, Catherine, "A robotics group offers ideas to 'shift power' to drive localization", *Devex,* 14/04/2022 https://www.devex.com/news/a-robotics-group-offers-ideas-to-shift-power-to-drive-localization-102987

[545] COLEMAN, Alison, "Matternet's vision for drones to become a mainstream delivery channel", *Forbes*, 12/07/2023 https://www.forbes.com/sites/alisoncoleman/2023/07/12/matternets-vision-for-drones-to-become-a-mainstream-delivery-channel/?sh=6605710373bb

CHENEY, Catherine, "Why a drone startup that launched with a humanitarian focus is switching gears", *Devex*, 07/06/2019 https://www.devex.com/news/why-a-drone-startup-that-launched-with-a-humanitarian-focus-is-switching-gears-95057

[546] CISCO, "Technology for good: stratus information systems helps Matternet drones deliver critical medical supplies", 12/10/2020https://blogs.cisco.com/partner/stratus-information-systems-helps-matternet-drones-deliver-critical-medical-supplies

[547] MEIER, Patrick, "New information technologies and their impact on the humanitarian sector", *International Review of the Red Cross*, Vol. 93, N° 884,2011, pp. 1239-1263.

TAYLOR, L., SCHROEDER, R. "Is bigger better? The emergence of big data as a tool for international development policy" *GeoJournal* 80, 2015, p.503–518 https://doi.org/10.1007/s10708-014-9603-5

ZWITTER, Andrej, "International Humanitarian and Development Aid and Big Data Governance", in: SCHIPPERS, Birgit (eds.*), The Routledge handbook to rethinking ethics in international relations*, London : Routledge, 2020, p.428

QADIR, Junaid, ANWAAR, Ali, RASOOL, Raihan, ZWITTER, Andrej, SATHIASEELAND, Arjuna, CROWCROF, Jon, BOERSMA Kees, FONIO Chiara, *Big data surveillance and crisis management*, London : Routledge studies in surveillance, 2019, 256 p.

ROCA,Thomas, LETOUZE, Emmanuel, « La révolution des données est-elle en marche ? Implications pour la statistique publique et la démocratie », *Afrique contemporaine*, 2016/2 (n° 258), p. 95-111. https://www.cairn.info/revue-afrique-contemporaine1-2016-2-page-95.htm

[548] https://www.globaldtm.info/fr/

récurrentes de flux migratoires à partir de données mobiles et d'adresses IP[549].Ces projets nécessitent la collecte de données provenant d'entreprises, de compagnies téléphoniques et de réseaux sociaux. D'où le fait que les acteurs prônant l'usage de données massives[550] soutiennent le développement de partenariats avec des acteurs privés. Ainsi, on peut lire sur le site des Nations-Unies qu'« une grande partie des mégadonnées les plus susceptibles d'être utilisées pour l'intérêt public est recueillie par le secteur privé. Par conséquent, les partenariats public-privé vont probablement se généraliser. Le défi sera de s'assurer qu'ils sont viables et que des cadres clairs de réglementation seront en place pour définir les rôles et les attentes de toutes les parties. »[551] De nouveaux termes ont été forgés pour désigner ce type de partenariat : « data for good », « data philanthropie », etc. C'est l'ingénieur Brian Behlendorf — développeur du logiciel Open Source Apache[552] — qui aurait créé le terme de « data philanthropy » au World Economic Forum en 2011. Il désignerait pour la chercheuse Yafit Lev-Aretz la promotion de projets facilitant le partage de données d'acteurs privés à des finalités sociales et pour le bien commun. Il s'agit de données produites par des plateformes, des opérateurs de télécommunication, des compagnies satellitaires, des réseaux sociaux[553].

---

[549] KOCH A. "The International Organization for Migration as a Data Entrepreneur: The Displacement Tracking Matrix and Data Responsibility Deficits.", In: BRADLEY, M, COSTELLO, C, SHERWOOD, A, (eds.), *IOM Unbound?: Obligations and Accountability of the International Organization for Migration in an Era of Expansion*, Cambridge University Press, 2023, p.235-269.

[550]Selon la définition bien connue les données massives sont caractérisées par trois termes : Volume, Variété, Vélocité.

Volume : les données massives supposent évidemment de disposer d'une vaste quantité d'information, sachant que la valeur de chaque donnée croit de façon proportionnelle à la masse d'information collectée, et s'enrichit exponentiellement par recoupement de jeu de données.

Variété : Ce sont des données de multiples formats et provenant de diverses sources, ce sont des données personnelles ou des métadonnées, etc.

Vélocité : elles s'accumulent en temps réel, la vélocité désigne la rapidité de production des données et l'immédiateté de la possibilité de collecte.

« Les Big Data signifient donc surtout le franchissement d'un seuil de quantité, de complexité, de rapidité de prolifération des données à partir duquel nous serions contraints d'automatiser et d'accélérer (pour tenir compte de l'accroissement continu, à grande vitesse, des masses de données) les processus de transformation des données numériques en informations opérationnelles. 30 L'expression Big Data renvoie donc aux masses de données numériques complexes à accumulation rapide, mais aussi à l'ensemble des nouvelles techniques logicielles (Data Mining, Machine Learning, Social Network Analysis, Predictive Analytics, "Sensemaking", Natural Language Processing, Visualization,…) sans lesquelles les données resteraient "muettes", et qui présupposent à leur tour l'utilisation de capacités de stockage et de traitement gigantesques. Cette puissance ne pouvant être offerte par un seul ordinateur, aussi puissant soit-il, on se tourne alors vers la parallélisassions des traitements et des données qui se basent sur l'utilisation simultanée d'un grand nombre de serveurs constitués en grappes (clusters) sur lesquels les données sont distribuées et qui collaborent selon des modèles de calcul distribué , à la détection des relations subtiles, qui seraient autrement restées imperceptibles, entre des données très hétérogènes, récoltées dans divers contextes. »

ROUVROY, A, « Des données et des Hommes. Droits et libertés fondamentaux dans un monde de données Massives ». VOL. T-PD-BUR(2015)09REV, T-PD-BUR(2015)09REV edn, Conseil de l'Europe, Strasbourg.

BOULLIER, Dominique, « Les Sciences sociales face aux traces du big data ? Société, opinion et répliques », FMSH-WP-2015-88, avril 2015

CARDON, Dominique, *A quoi rêvent les algorithmes*, Paris: Seuil,2015, 112 p.

[551] « Les mégadonnées au service du développement », ONU, https://www.un.org/fr/global-issues/big-data-for-sustainable-development

[552]« Ce dont nous avons besoin maintenant, c'est d'une philanthropie des données, un terme qui a émergé spontanément lors d'une conversation à Davos avec Brian Behlendorf, visionnaire des logiciels libres et directeur technique du Forum économique mondial. Nous appelons les entreprises à fournir des données dans le cadre de leur philanthropie stratégique et à collaborer avec des bénéficiaires comme nous pour mettre en place des processus de sauvegarde et d'anonymisation des données. », " « What we need now is data philanthropy, a term that emerged spontaneously during a Davos conversation with open-source visionary and World Economic Forum CTO Brian Behlendorf. We are calling on companies to provide data as part of their strategic philanthropy, and to work with recipients like ourselves to establish processes to safeguard and properly anonymize data. »

WOLFE, Nathan, GUNASEKARA, Lucky, BOGUE, Zachary, « Crunching digital data can help the world », *CNN*, 03/02/2011 http://edition.cnn.com/2011/OPINION/02/02/wolfe.gunasekara.bogue.data/index.html

[553] NOVECK, Beth Simone, « Data Collaboratives: Sharing Public Data in Private Hands for Social Good », *FORBES*,24/09/2015, https://www.forbes.com/sites/bethsimonenoveck/2015/09/24/private-data-sharing-for-public-good/#397107b351cd

MEIER, Patrick, "Big Data philanthropy for humanitarian response", *Irevolution*, 04/06/2012 https://irevolutions.org/2012/06/04/big-data-philanthropy-for-humanitarian-response/

KIRKPATRICK, Robert, « Data philanthropy is good for business *», Forbes*, 20/09/2011 https://www.forbes.com/sites/oreillymedia/2011/09/20/data-philanthropy-is-good-for-business/?sh=63d8bcaa5f70

KIRKPATRICK, Robert, "A new type of philanthropy : donating data", *Harvard Business Review*, 21/03/2013 https://hbr.org/2013/03/a-new-type-of-philanthropy-don

Cette idée est soutenue par des agences onusiennes comme le Global Pulse, le Global Partnership for Sustainable Development Data, the Development Data Hub[554] et the Digital Impact Hub[555], ainsi que par le laboratoire d'innovation d'UNICEF.

On s'intéressera pour notre part aux projets exploitant des données de géolocalisation générées par différents dispositifs numériques, notamment les téléphones mobiles. Il existe en effet tout un écosystème d'entreprises commercialisant des données de localisation, généralement à des fins de marketing[556]. Les téléphones mobiles de type smartphone génèrent des données GPS, mais également des statistiques téléphoniques, des « Call data records » en anglais. Les opérateurs de téléphonie mobile conservent en effet des données d'usagers générées automatiquement lors d'appels ou d'envoi de messages. Or les humanitaires sont aussi intéressés par ce type de données. Leur exploitation leur permettrait, entre autres, de comprendre des trajectoires récurrentes de bénéficiaires, et ainsi mieux cibler l'aide en fonction des déplacements[557]. Mais ce type d'expérimentation relèverait surtout de politiques de gestion de population[558], les exilés étant alors assimilés à des flux qu'il serait nécessaire de contrôler[559]. Ainsi, en Somalie l'Unicef, le Gov Lab et la Banque Mondiale, ont conduit un projet commun pour tenter de mieux comprendre les déplacements de groupes[560]. Et le programme « winter operations cell » de l'UNHCR qui agrège des données météorologiques pour tenter de déterminer l'évolution de flux migratoires. Pour notre part, deux cas nous intéressent : l'utilisation de données téléphoniques (Call detail records) dans le secteur humanitaire, et le programme « Data for good », de Facebook. Ce dernier propose de donner accès à des cartes constituées à partir des données du réseau social.

---

PAWELKE, Andreas, TATEVOSSIAN, Anoush Rima, "Data Philanthropy: Where Are We Now?" *United Nations Global Pulse Blog*, 08/05/2013 https://www.unglobalpulse.org/data-philanthropy-where-are-we-now
"International Organization for Migration, Harnessing Data Innovation for Migration Policy: A Handbook for Practitioners", 2023

[554] http://data.devinit.org/

[555] https://www.un.org/fr/sections/issues-depth/big-data-sustainable-development/index.html

[556] THOMPSON,A., Stuart, WARZEL, Charlie," Twelve million phones, one dataset, zero privacy", *The New York Times*, 19/12/2019 https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html
"Bad data "for good" : how data brokers try to hide behind academic research", *Electronic Frontier Foundation*, 16/08/2022https://www.eff.org/fr/deeplinks/2022/08/bad-data-good-how-data-brokers-try-hide-academic-research

[557] "Data philanthropy, international organizations and development policy : ethical issues to consider", *UNDP*, 2020 https://www.agora-parl.org/sites/default/files/agora-documents/Data%20Philanthropy%2C%20International%20Organizations%20and%20Development%20Policy%20-%20Ethical%20Issues%20to%20Consider.pdf
GALIT, Sarfaty, "Corporate Data Responsibility" in : DICKINSON, Laura, BERG, Edward (eds.), *Big Data and Armed Conflict: Legal Issues Above and Below the Armed Conflict Threshold*, Oxford University Press, 2022
Big data, migration and human mobility, Migration data portal
https://www.migrationdataportal.org/themes/big-data-migration-and-human-mobility
Big data for migration alliance
https://data4migration.org/about/
ACAPS, "Call Detail Records The use of mobile phone data to track and predict population displacement in disasters",Urban response 12/06/2013 https://www.urban-response.org/system/files/content/resource/files/main/call-detail-records-the-use-of-mobile-phone-data-to-track-and-predict-population-displacement-in-disasters.pdf
Global Pulse, GSMA, "The state of mobile data for social good report", June 2017 https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/06/Mobile-Data-for-Social-Good-Report_29June.pdf

[558] TAYLOR, L. , MEISSNER, F., « A Crisis of Opportunity: Market-Making, Big Data, and the Consolidation of Migration as Risk », *Antipode*, 52, 2020, p. 270-290

[559] QUET, Mathieu, *Flux, comment la pensée logistique gouverne le monde*, Paris, Zones, éditions la Découverte, 2022,176 p.
JOHNS, Fleur,"Populations: from statistic to data science", in JOHNS, Fleur, *#Help Digital Humanitarianism and the Remaking of International Order*, Oxford University press, 2023, p. 71-101

[560]Migration, Mitigation and Maps: The predictive role of UNHCR's first Winter Cell https://www.unhcr.org/innovation/migration-mitigation-and-maps-the-predictive-role-of-unhcrs-first-winter-cell/

Concernant les « Call detail record », c'est à la fin des années 2000 que sont réalisés de premiers travaux exploitant les données de téléphonie mobile. L'objectif est d'abord de comparer des formes de mobilités urbaines et rurales[561], ou de tracer des mouvements de population afin de soutenir des politiques de développement [562] .

| Cell-Id | Source | Call Time | Duration | Direction | Event | Target |
|---|---|---|---|---|---|---|
| 12103 | 21D7B5 | 2020-03-04 20:00:10 | 00:29:57 | Incoming | Call | 65H8I9 |

Ce type de données permet de déduire de nombreuses informations sur les usagers, dont leur localisation. En effet, chaque statistique d'appel inclut le numéro de la « tour cellulaire » la plus proche d'un usager. Ces données peuvent être utilisées pour analyser les trajectoires récurrentes de mobilité, afin d'appuyer des politiques d'urbanisation, ou des études d'épidémiologistes[563], de politiques sanitaires, [564] comme cela avait été le cas lors du Covid19 [565]. Elles sont exploitées dans le cadre d'études comportementales, ou encore d'études socio-économiques. Une première expérimentation a lieu en 2010, à Haïti : Digicel — une compagnie de téléphonie mobile locale — avait alors autorisé l'accès à des chercheurs de l'université américaine de Columbia et à Flowminder, organisation spécialisée sur ce sujet[566], à des données de CDR. Leur étude portait sur l'analyse des déplacements de population après un tremblement de terre et une épidémie de choléra[567]. Puis, en 2012, Orange avait organisé un concours — le Data for development challenge ; les gagnants avaient eu accès à des données de statistiques téléphoniques pour produire des résultats de recherche mobilisables pour des politiques de développement. Cette dernière initiative a eu un grand retentissement au sein de l'ONU, du Forum économique mondial, au MIT et à Cambridge. Et lorsqu'une épidémie d'Ebola touche l'Afrique de l'Ouest en 2014, un groupe d'universitaires — notamment du MIT[568] — et d'acteurs de la solidarité internationale — comme UNICEF et

---

[561] EAGLE, Nathan, MONTJOYE, Yves-Alexandre, LUIS, Bettencourt, » Community Computing: Comparisons between Rural and Urban Societies Using Mobile Phone Data", *IEEE international conference on computational science and engineering*, 2009, p. 144-150. 10.1109/CSE.2009.91.

[562] BLUMENSTOCK, Joshua, "Inferring patterns of internal migration from mobile phone call records: evidence from Rwanda", *Information Technology for Development*, 18:2, 2012, p. 107-125.

[563] WESOLOWSKI Amy et al. « Quantifying the Impact of Human Mobility on Malaria », *Science,* 338, 2012, p. 267-270

[564] BALSARI, Satchit, BUCKEE, Caroline, CHAN, Jennifer, SCHROEDER, Andrew, "the Use of Human Mobility Data in Public Health Emergencies", *Crisis ready*, April 2022
https://www.crisisready.io/wp-content/uploads/2022/06/The-Use-of-Human-Mobility-Data-in-Public-Health-Emergencies.pdf

[565] En France, des données d'Orange, sa solution FluxVision a permis de voir que 17% des habitants du Grand Paris auraient fui en province entre le 13 et le 20 mars.
Orange, « Pourquoi les données téléphoniques sont-elles précieuses pour lutter contre l'épidémie de Covid19 », Orange, 03/11/2020
https://www.orange.com/fr/actualites/2020/Avril/Pourquoi-les-donnees-telephoniques-sont-elles-precieuses-pour-lutter-contre-l-epidemie-de-Covid-19
UNTERSINGER, Martin, « Pourquoi les données téléphoniques aident à comprendre la pandémie de Covid-19 », *Le Monde*, 27/03/2020
https://www.lemonde.fr/pixels/article/2020/03/27/pourquoi-les-donnees-telephoniques-aident-a-comprendre-la-pandemie-de-covid-19_6034708_4408996.html

[566] POWER, Daniel, et al."Flowkit : unlocking the power mobile data for humanitarian and development purpose", *Flowminder*, Dial, 2019
https://www.flowminder.org/media/xrhp1tth/flowminder_flowkit_unlockingthepowerofmobiledata.pdf

[567]"The first use of mobile operator data for humanitarian operation : Haiti earthquake 2010",Flowminder
https://www.flowminder.org/what-we-do/population-distribution-and-mobility-analysis/disaster-management/the-first-use-of-mobile-operator-data-for-humanitarian-operations-haiti-earthquake-2010
BENGTSON, L, LU X., THORSON, A, GARFIELD, R, VON SCHREEB, J, "Improved Response to Disasters and Outbreaks by Tracking Population Movements with Mobile Phone Network Data: A Post-Earthquake Geospatial Study in Haiti", *PLOS Medicine* 8(8)2011. e1001083. https://doi.org/10.1371/journal.pmed.1001083

[568]TALBOT, David, "Cell-phone data might help predict Ebola's spread", *Technology Review*, 22/08/2014
https://www.technologyreview.com/news/530296/cell-phone-data-might-help-predict-ebolas-spread/

Global Pulse — plaident pour le partage de données de téléphonie mobile[569]. Pour accéder aux CDR, il a été nécessaire de négocier avec les gouvernements locaux et les compagnies téléphoniques de différents États. Or les cadres réglementaires sur ce sujet ne sont pas unifiés. D'où, comme le rapporte l'organisation DataPop alliance, la nécessité de négocier au cas par cas : « À l'heure actuelle, il n'existe tout simplement pas d'ensemble cohérent de réglementations ou de lignes directrices régissant le domaine de l'analyse des CDR. Les réponses aux demandes croissantes de CDR de la part des chercheurs ont généralement été ad hoc, accordées par les opérateurs télécoms sur la base de relations personnelles et d'autres arrangements. » [570] Concernant l'épidémie d'Ebola, les acteurs gouvernementaux ont finalement accordé la possibilité d'accéder à des données de CDR à des finalités de recherche[571], exception le Libéria. Ce pays s'est opposé aux demandes d'accès aux données mobiles, au motif qu'elles porteraient atteinte à la vie privée des personnes concernées. Et effectivement, pour le chercheur Sean Martin Macdonald, il ne fait aucun doute que ce type d'initiative contrevient aux lois relatives à la protection des données du Libéria, plus spécifiquement en matière de consentement des personnes concernées[572]. L'état d'urgence lié à l'épidémie d'Ebola n'exonérait pas le recueil de ce dernier pour le chercheur[573]. Sean Martin Macdonald regrette en outre une absence de discussion sur le caractère proportionné de cette mesure. D'autant que l'apport des CDR dans l'analyse de l'épidémie d'Ebola est discuté. Pour Susan Erikson, anthropologue spécialisée sur les sujets relatifs à la santé globale,

---

[569] FAST, Larissa, WAUGAMAN, Adele, « Fighting Ebola with Information: Learning From Data and Information Flows in the West Africa Ebola Response », 2016, Washington, DC: USAID
https://www.usaid.gov/sites/default/files/2022-05/FightingEbolaWithInformation.pdf
"Ebola and big data, call for help", *The Economist*, 23/10/2014 https://www.economist.com/leaders/2014/10/23/call-for-help "Why mobile data to prevent ebola has not yet been released", *The Economist*, 09/11/2014 https://www.economist.com/the-economist-explains/2014/11/09/why-mobile-data-to-prevent-ebola-has-not-yet-been-released

[570] "Right now, there is simply no coherent and comprehensive set of regulations or guidelines that govern the field of CDR analytics. Responses to growing demands for CDRs from researchers have typically been ad hoc, granted by Telcos on the basis on personal connections and other arrangements— or for data challenges at their will." LETOUZE, Emmanuel, VINCK, Patrick ,KAMMOURIEH, Lanah, "The law, politics and ethic of cell phone data analytics", *Datapop alliance*, April 2015, https://datapopalliance.org/wp-content/uploads/2015/04/WPS_LawPoliticsEthicsCellPhoneDataAnalytics.pdf

[571] WESOLOWSKI, A, BUCKEE, CO, BENGTSSON, L, WETTER, E, LU, X, « Containing the ebola outbreak - the potential and challenge of mobile network data »,*PLoS Curr*., 29/09/ 2014
VOGEL, Nicholas, THEISEN, Christopher, LEIDIG, Jonathan P., SCRIPPS, Jerry, GRAHAM, Douglas H., WOLFFE, Greg, « Mining Mobile Datasets to Enable the Fine-grained Stochastic Simulation of Ebola Diffusion », *Procedia Computer Science*, Volume 51, 2015, P. 765-774

[572] « En supposant qu'il soit légal pour les opérateurs de réseaux mobiles de collecter, d'utiliser et de conserver les données de localisation liées à des comptes d'utilisateurs spécifiques, les questions de droit qui se posent concernent le consentement éclairé de l'utilisateur avant la collecte et la justification du partage de ces données avec le gouvernement. En l'absence de consentement écrit, il est explicitement interdit aux opérateurs de réseaux mobiles de partager des informations d'identification avec quiconque autre que le gouvernement, ce qui rend illégal tout partage direct d'informations avec des tiers (comme les organisations internationales ou les ONG). »« Assuming that it is legal for mobile network operators to collect, use, and maintain location records attached to specific user accounts, the operative questions of law relate to informed user consent prior to collection and the justification of sharing those records with the Government. Absent written consent, mobile network operators are explicitly prohibited from sharing identifying
information with anyone other than the government – making all direct information sharing with third parties (like international organizations or NGOs) illegal. »
MCDONALD, Sean Martin, *Ebola : a big data disaster, privacy, property, and the law of disaster experimentation*, The Censer for internet & society Paper, 2016
FAST, Larissa, WAUGAMAN, Adele,"Fighting Ebola with Information: Learning From Data and Information Flows in the West Africa Ebola Response", Washington, DC: USAID, 2016.

[573] « L'obtention du consentement au point de collecte est à la fois une exigence légale dans le contexte libérien et une pratique commerciale qui a des précédents significatifs pour des moyens moins altruistes. Il ne fait aucun doute que l'intégration de clauses relatives à l'utilisation des données en cas d'urgence dans les contrats commerciaux et de service public est à la fois le moyen le plus simple et le plus légal de faciliter le partage des CDR, et qu'elle minimise pratiquement toutes les autres questions que la loi oblige à se poser. » "Obtaining consent at point of collection is both a legal requirement in the Liberian context and a commercial practice that has significant precedent for less altruistic means. There is no question that building emergency data use clauses into commercial and public service contracts is both the most straightforward and the most legal way to facilitate the sharing of CDRs, and minimizes virtually every other question that the law compels."
MCDONALD, Sean Martin, *ibid.*

il serait même limité[574]. Les CDR permettent de tracer les mouvements de populations, et peuvent apporter des éléments de connaissance pour des épidémies à propagation respiratoire (dont la COVID19). Mais ils ne seraient, d'après la chercheuse, que d'une utilité limitée pour le cas de l'épidémie d'Ebola, dont la propagation se fait par un contact direct et par échange de flux corporels (sang, salive). Pour faire simple, les données mobiles ne permettent pas de retracer avec précision les flux de propagation. Quant à Linus Bentgsson, membre de Flowminder, il défend ce type de méthode, mais il ajoute le fait qu'elles ne sont pas dépourvues de biais, concernant pour lui surtout la représentativité du taux d'équipement en téléphonie mobile, au modèle épidémiologique [575].Bien plus, pour Sean Macdonald l'utilisation d'analyse de statistiques téléphoniques pour ce type de cas en était encore au stade expérimental. Le recours à une méthode non éprouvée en contexte d'urgence va de pair avec un certain nombre de risques, notamment en matière de réidentification[576]. Ses craintes ont été partagées par différents acteurs, dont des compagnies téléphoniques locales. Plus généralement, ces dernières peuvent être réticentes à communiquer des données[577], du fait d'une absence de cadre législatif clair et unifié et de base de données centralisées réunissant les statistiques téléphoniques détenues par différentes compagnies[578]. Cela représente pour ces dernières « un risque juridique qu'elles ne sont pas toujours prêtes à prendre. Pour les partisans des projets de type « data for good », la résistance des compagnies téléphoniques est un obstacle à surmonter, et on peut dire de même sur les lois restrictives en matière d'accès aux données. Comme l'écrit la chercheuse en droit international Fleur Johns, ces dernières « sont considérées comme des défis, des contraintes, des obstacles et des

---

[574] ERIKSON, SL., "Cell Phones ≠ Self and Other Problems with Big Data Detection and Containment during Epidemics", *Med Anthropol Q*. Sep 2018, 32(3), p. 315-339.
ERIKSON, Susan, « Cell phones as an anticipatory technology: behind the hype of big data for ebola detection and containment » 2018, German Research Foundationhttps://lost-research-group.org/wp-content/uploads/2018/01/WP24_Erikson_180115.pdf

[575] « Même le Dr Linus Bengtsson, directeur exécutif de Flowminder, prend soin de nuancer la manière dont la transmission de virus affecte l'importance de la migration des données vers le mode "données". » « Even Dr. Linus Bengtsson, the Executive Director of Flowminder, is careful to nuance the significant way that virus transmission affects the importance of migration data to the data mode. » MCDONALD, Sean Martin, *Ebola : a big data disaster, privacy, property, and the law of disaster experimentation*, The Censer for internet & society Paper, 2016 https://raw.githubusercontent.com/cis-india/papers/master/C, IS_Papers_2016.01_Sean-McDonald.pdf
WESOLOWSKI, A, BUCKEE C., BENGTSSON L, WETTER E, LU X, TATEM AJ., "Commentary: Containing the Ebola Outbreak – the Potential and Challenge of Mobile Network Data*". PLOS,* 2014 Sep 29 . doi: 10.1371/currents.outbreaks.0177e7fcf52217b8b634376e2f3efc5e.
"What are the strengths and limitations of CDR data?", Flowminderhttps://www.flowgeek.org/what-are-cdrs/what-are-the-strengths-and-limitations-of-cdr-data

[576] "Le débat sur la meilleure façon de collecter, de partager et d'utiliser les CDR n'en est qu'à ses débuts. Le débat sur l'utilisation appropriée des données des réseaux mobiles, à ce jour, est largement constitué d'éléments de plaidoyer à perspective unique, chacun d'entre eux défendant un intérêt organisationnel ou commercial. Le débat institutionnel se concentre sur la promotion des intérêts du groupe principal, mais ne parvient pas à prouver que la modélisation des données basée sur les CDR crée des informations uniques et suffisamment exploitables pour justifier leur diffusion. ", " the debate about the best fit way to collect, share, and use CDRs is still in its very early stages. The conversation about appropriate use of mobile network data, as of now, Is largely comprised of single perspective advocacy pieces, each of which advance an organizational or commercial interest. The institutional debate focuses on advancing the interests of that group's primary constituency, but fails to prove where cdR based data modeling Create uniquely actionable enough insights to justify their release." MCDONALD, Sean Martin, Ebola : a Big data disaster, privacy, property and the law of disaster experiment, CSI Papers, 2016, p. 27
BERGTORA, SANDVIK, Kristin, LINDSKOV JACOBSEN, Katja, MCDONALD, Sean Martin, "Do no harm : a taxonomy of the challenges of humanitarian experimentation*", international Review of the Red Cross*, 2017, 99 (1), p.319–344.

[577] « Sur les marchés où les rentes des services de télécommunication sont élevées mais où les pouvoirs publics n'ont qu'une participation minimale, c'est-à-dire où les barrières à l'entrée sont importantes, ce qui se traduit par un nombre réduit d'opérateurs par rapport à la taille totale du marché, la résistance au partage des données pourrait être forte. Cette résistance devra donc être anticipée et résolue dès le début du partenariat, faute de quoi elle constituera un obstacle important à l'accès aux données de téléphonie mobile pour les statistiques officielles. « ,"In markets where there are high rents from telecommunication services but minimal government equity, i.e. significant barriers to entry resulting in fewer operators relative to total market size, resistance to records sharing could be strong. Therefore, such resistance will need to be anticipated and resolved at the beginning of the partnership, otherwise it will present a significant roadblock to accessing mobile phone data for official statistics."
UN Global working group on Big Data for official statistics, *Handbook on the use of mobile phone data for official statistics*, september 2019 https://unstats.un.org/bigdata/task-teams/mobile-phone/MPD%20Handbook%2020191004.pdf

[578] GERSTLE, Talia et al. , "Assessing the use of call detail records (CDR) for monitoring mobility and displacement",I*OM,* February 2021

problèmes à surmonter pour « aller de l'avant « ou préserver le « progrès ». Par exemple, l'un de nos informateurs chargé d'essayer de négocier des accords de partage de données au sein du réseau Global Pulse de l'ONU a fait remarquer que le « plus grand défi » pour les organisations engagées dans l'humanitaire numérique « est l'accès aux données — l'accès aux données et aussi la conformité réglementaire. »[579] Mais, dans certains cas, la « solution » est tout simplement de faire « sauter » les verrous juridiques ou de les contourner, et recourir par exemple à des courtiers en données[580], aux pratiques aux frontières du droit. Il s'agit par exemple de firmes comme Criteo ou Equifax qui commercialisent l'accès à des jeux de données personnelles collectées en ligne ou hors ligne par des firmes.

C'est aussi le cas de Bazze une startup aux pratiques décriées par des professionnels de la protection des données pour le peu de transparence quant à la provenance de ses données. Bazze est décrite comme un « data broker » qui donnerait « accès à des données de localisation "en temps réel"[581]. Pour Wolfie Christl, chercheur indépendant, les clients de Bazze pourraient avoir accès aux données de téléphonie mobile, des identifiants des appareils, des coordonnées GPS, et aussi des statistiques téléphoniques, des "call data records". L'Application Programming Interface (API) de Bazze donne une idée plus précise des données collectées[582] :

For every endpoint there is a sample response which will give you an idea of what the data looks like. There are a few different variations of this, but they all use similar fields. The data schema is as follows:

| Column | Description |
|---|---|
| advertising_id | Mobile device |
| advertising_id_type | Mobile device ID type |
| timestamp | Event timestamp in ISO format |
| latitude | Mobile device latitude in decimal format |
| longitude | Mobile device longitude in decimal format |
| altitude | Mobile device altitude in meters |
| ip_address | ipv4 |
| wifi_ssid | Wifi SSID that mobile device is connected to |
| wifi_bssid | Wifi BSSID that mobile device is connected to |
| country | Country in which mobile device is located at time of event, in ISO 3166-1 format |
| horizontal_accuracy | Horizontal accuracy of latitude and longitude coordinates in meters |
| user_agent | Mobile device web browser |
| publisher_id | Publisher ID of mobile application |
| iot_signals | Bluetooth devices that mobile device is connected to |
| bazze_device_id | Hash of the advertising_id |
| bazze_geohash | Geohash approximation of latitude and longitude coordinates, at 38.2m x 19m precision |
| bazze_mgrs | MGRS approximation of the record location, at a 1km precision |
| bazze_event_id | Hash of the entire data record |
| bazze_gps_country | Country in which mobile device is located at time of event, in ISO 3166-1 format |

Grâce à ces données, la startup affirme pouvoir localiser des personnes qui auraient visité une ambassade ou un site militaire. Wolfie Christl conclut que Bazze aide ses clients "à identifier

[579] "as challenges,constraints, barriers, and problems to be overcome in the course of "moving forward" or maintaining "progress." For example, one of our informants charged with trying to broker data-sharing arrangements within the UN Global Pulse network observed that the "biggest challenge" for organizations engaged in digital humanitarianism "is access to data—access to data and also regulatory compliance." JOHNS, Fleur, #*Help, digital humanitarianism and the remaking of international order*, Oxford University Press, p.180

[580]Courtier en données, Wikipedia, 16/07/2024, https://fr.wikipedia.org/wiki/Courtier_en_donn%C3%A9es

Uncovering the Hidden Data Ecosystem, https://privacyinternational.org/campaigns/data-brokers

[581] « access to "real-time" location data and a suite of other information, which Western governments can use to track foreign individuals in sensitive locations overseas. Called Bazze, the company markets a platform that can enable searches for people in embassies, consulates, and military bases, underscoring governments' growing reliance on data brokers to access vast quantities of intelligence on global citizens from commercial sources. » EMERSON, Sarah, « This startup sells access to data locating people at foreign military bases and embassies », Forbes, 22/02/2024 https://www.forbes.com/sites/sarahemerson/2024/02/22/bazze-data-broker-is-selling-data-that-can-locate-people-at-military-bases-and-embassies/

[582] https://bazze.io/docs/api/

et à suivre les individus d'intérêt" pour "aider le gouvernement américain et ses alliés". Couvrant les données de localisation mobile en "Afrique, au Moyen-Orient, en Asie, en Amérique latine et en Europe de l'Est".»[583]

Bazze aurait pour clients des services de renseignement et des forces armées, notamment le ministère de la Défense américain, et d'après un article du journal Forbes, des ONG humanitaires : « Les agences de défense et de renseignement sont la clientèle cible de Bazze, qui affirme avoir passé des contrats avec le ministère américain de la Défense et le ministère britannique de la Défense. Semwangu a refusé de donner des détails sur ces partenariats, mais a déclaré qu'"un exemple de cas d'utilisation consiste à identifier et à suivre les activités d'acteurs étrangers hostiles dans des pays étrangers". Les dossiers d'approvisionnement font état de plusieurs contrats avec l'armée de l'air américaine — dont un pour un outil qui "fournit une capacité de neutralisation pour identifier et suivre les acteurs malveillants" — bien qu'il ne soit pas clair quel pourcentage des fonds a été payé, le cas échéant. Un porte-parole du ministère de la Défense a déclaré à Forbes qu'il n'avait trouvé aucun contrat avec Bazze, et un porte-parole du ministère de la Défense a refusé de commenter les contrats de l'agence. Selon la société, elle a également travaillé avec des ONG humanitaires et des entreprises, qu'elle a refusé de nommer. »[584]

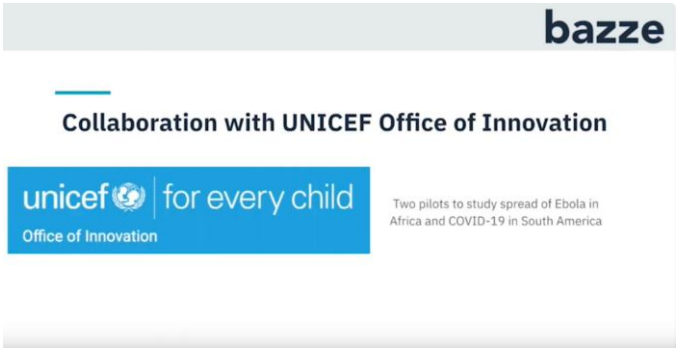
Il est possible de retrouver des traces de partenariats entre des ONG et Bazze sur Internet. Bazze a par exemple soutenu une série de conférences sur la cartographie humanitaire[585], une employée de Bazze y fait la promotion de la startup[586]. La présentation gomme évidemment toute référence pouvant évoquer le fait qu'une grande partie des clients de Bazze sont des acteurs liés au secteur de la défense. La vidéo promotionnelle fait mention d'un partenariat avec UNICEF pour des projets portant sur le suivi des épidémies d'Ebola et de Covid 19, au sujet duquel on ne dispose pas de plus de détails.

[583]" virtual ISR product helps DoD customers identify and track individuals of interest" to "help the US government and allies". Covering mobile location data in "Africa, the Middle East, Asia, Latin America and Eastern Europe"." https://x.com/WolfieChristl/status/1757776443814162891

[584] "Defense and intelligence agencies are Bazze's target clientele, and it claims to have contracted with the U.S. Department of Defense and U.K. Ministry of Defence. Semwangu declined to elaborate on these partnerships, but said that "one sample use case is to identify and track the activities of hostile foreign actors in foreign countries." Procurement records show several contracts with the U.S. Air Force — one for a tool that "provides stand-off capability to identify and track malicious actors — though it's unclear what percentage of the funds were paid out, if any. An MoD spokesperson told *Forbes* it could not find any contracts with Bazze, and a DoD spokesperson declined to comment on the agency's contracts. According to the company, it has also worked with humanitarian NGOs and corporations, which it declined to name." EMERSON, Sarah, « This startup sells access to data locating people at foreign military bases and embassies », Forbes, 22/02/2024https://www.forbes.com/sites/sarahemerson/2024/02/22/bazze-data-broker-is-selling-data-that-can-locate-people-at-military-bases-and-embassies/

[585] https://gg.cartong.org/fr/geong/2020/partenariats

[586]https://www.youtube.com/watch?v=0qQ0fNATVKM




**PROMOTION DU PARTENARIAT ENTRE UNICEF ET BAZZE[587]**

Enfin, une offre d'emploi récente d'UNICEF destinée à des data scientists mentionne la possibilité d'exploiter des données provenant de Bazze.

- Data exploration and analysis: find and promote interesting use cases for potential application of frontier data and technology, especially related to internal data sources or from private sector (e.g. Bazze), in projects with UNICEF colleagues and research partners.
- Deliverable: Collect UNICEF data gaps and needs from different divisions/programaatic areas/COs/ROs where frontier data and technology have the potential to contribute (e.g. migration, number of children in conflicts, etc.); Produce content that can be incorporated in the frontier data –use cases repository (in the form of slide deck for iterative refinements); Write a blogpost with a compelling story on the insights from the data analysis.
- Evaluate and support data requests from COs and ROs and divisions to access to different data sources as the WB data partnerships portal, other data and computational resources.

**ANNONCE D'EMPLOI D'UNICEF A DESTINATION DE « DATA SCIENTISTS » EVOQUANT LA POSSIBILITE D'EXPLOITER DES DONNEES PROVENANT DE BAZZE[588]**

Plus communément, la plupart des acteurs servant d'intermédiaires pour acquérir des données ne sont pas des courtiers en données, mais des GAFAM. Il se trouve que depuis 2017, Facebook propose un service proche facilitant l'accès à des données de mobilité. Les ONG n'ont plus à négocier avec plusieurs compagnies téléphoniques, parfois pendant plusieurs mois. Il suffit d'obtenir une simple licence, et comme le déclare Kalev Leetaru « contrairement aux enregistrements CDR, qui doivent généralement être obtenus de manière fragmentaire auprès de plusieurs fournisseurs dans chaque pays concerné, Facebook est en mesure de suivre la localisation en temps réel de ses utilisateurs dans le monde entier dans une seule base de données centralisée, quel que soit leur fournisseur de téléphonie mobile et même lorsqu'ils voyagent dans le monde entier. »[589]Précisons que Facebook a investi le champ de la cartographie depuis plusieurs années, d'abord en réalisant une carte de densité de population de l'Afrique[590]. L'objectif affiché était de repérer les besoins en connectivité et de lutter contre

[587] https://www.youtube.com/watch?v=0qQ0fNATVKM
[588] https://indevjobs.org/jobs/data-scientist-consultant-3
[589] « Contrairement aux enregistrements CDR, qui doivent généralement être obtenus de manière fragmentaire auprès de plusieurs fournisseurs dans chaque pays concerné, Facebook est en mesure de suivre la localisation en temps réel de ses utilisateurs dans le monde entier dans une seule base de données centralisée, quel que soit leur fournisseur de téléphonie cellulaire et même lorsqu'ils voyagent dans le monde entier. », "unlike CDR records, which must typically be acquired in piecemeal fashion from multiple providers across every country of interest, Facebook is able to track the real time location of its users globally in a single centralized database regardless of their cellular provider and even as they travel throughout the world." LEETARU, Kalev, "Are Facebook's disaster maps the Ultimate government surveillance tool in disguise?", *Forbes*,05/05/2019 Are Facebook's Disaster Maps The Ultimate Government Surveillance Tool In Disguise? (forbes.com)
[590] HEMPEL, Jessi, "Inside Facebook's ambitious plan to connect the whole world", *Wired*, 19/01/2016 https://www.wired.com/2016/01/facebook-zuckerberg-internet-org/

la fracture numérique ou plutôt de prospecter de nouveaux marchés et cibler de nouveaux usagers[591]. Pour ce faire, plusieurs partenariats ont été noués avec des acteurs impliqués dans la cartographie, parfois proche du logiciel libre comme OpenStreetMap et Humanitarian openstreetmap team (HOT)[592]. En 2017, Facebook lance le programme « Data for good » qui met à disposition d'ONG des jeux de données. Il s'agit soit des données économiques, soit des indicateurs portant sur la nature de liens d'interconnexion entre individus. Différents types de cartes sont proposés : des cartes de densité de population[593], de mobilité, de déplacement de population, de connectivité et de couverture des réseaux électriques[594]. Ce service est utilisé par plusieurs ONG. Facebook a noué des partenariats avec l'IFRC, Direct Relief et UNICEF, ainsi qu'avec NetHope[595]. Direct Relief s'est servi des cartes de mobilité pour coordonner des distributions d'aide lors d'incendies en Australie, pour évaluer des déplacements de population au cours du conflit ukrainien. Nethope a employé des cartes de connectivité afin de mettre en place des programmes de lutte contre la fracture numérique dans des pays en voie de développement[596]. Unicef les a utilisés pour mieux cibler des campagnes de vaccination au Pakistan[597]. Certains jeux de données sont partagés à des ONG après la signature d'une licence. D'autres données, moins sensibles, sont directement partagées sur la plateforme de l'Humanitarian Data Center d'OCHA[598]. Cette dernière permet le téléchargement de cartes de densité, de déplacement, d'index de connexion sociale ou de degré de richesse relatif. Elles sont constituées à la fois grâce à des données de localisation collectées sur le réseau social, et également d'autres types de données, comme des images satellitaires — obtenues par Facebook auprès d'entreprises spécialisées comme Maxmar. En effet, en postant une publication via un smartphone, un utilisateur émet de nombreuses informations, dont sa localisation, qui peut être réutilisée pour constituer une carte des

KILIC, Talip, BLANKESPOOR, Brian, DANG, HAI-ANH, MURRAY, Siobhan, PRYDZ, Beer, Espen, Sakamoto, Kiwako, "A first look at Facebook's high-resolution population maps", *World bank blogs*, 18/11/2016
https://blogs.worldbank.org/opendata/first-look-facebook-s-high-resolution-population-maps
MEIER, Patrick," The future of crisis mapping is finally here",*IRevolution*, 07/06/2017 https://irevolutions.org/2017/06/07/crisis-mapping-future/

[591] NOTHIAS, Toussaint, "Access granted: Facebook's free basics in Africa", *Media, Culture & Society*, *42*(3), p.329-348. https://doi.org/10.1177/0163443719890530

[592] PANNIER, Alice, « Sources d'influence, enjeux économiques et géopolitiques dans les logiciels open source », *IFRI*, décembre 2022 https://www.ifri.org/sites/default/files/atoms/files/pannier_influence_logiciels_open_source_2022.pdf

[593] VERHULST, Stefaan, ADITI, Ramesh, ANDREW, Young, ZAHURANEC, Andrew, "Where is Everyone? The Importance of Population Density Data: A Data Artefact Study of the Facebook Population Density Map", 2021.

[594]MAAS, Paige, IYER, Shankar, GROS, Andreas, PARK, Wonhee, MCGORMAN, Laura, NAYAK, Chaya, DOW, Alex, "Facebook disaster maps : aggregate insights for crisis response & recovery",Withe Paper – Social Media in Crisis and Conflicts Proceedings of the 16th ISCRAM N – València, Spain May 2019 https://idl.iscram.org/files/paigemaas/2019/1912_PaigeMaas_etal2019.pdf

[595]" Facebook data for good, Facebook data for good annual report", 2020
https://www.crisisready.io/wp-content/uploads/2021/01/Facebook-Data-for-Good-2020-Annual-Report-1.pdf

[596] Nethope, "Facebook data for good population density maps and how they are helping the nonprofit sector", 29/01/2021https://nethope.org/articles/facebook-data-for-good-population-density-maps-and-how-they-are-helping-the-nonprofit-sector/

[597] WICKS, Toby, "Unicef & Facebook put data to work for the world's most vulnerable children", *Forbes*, 09/06/2017 https://www.forbes.com/sites/unicefusa/2017/06/09/unicef-facebook-put-data-to-work-for-the-worlds-most-vulnerable-children/?sh=f39de5f4f2bf

[598]HDX une plateforme principale de téléchargement des données mise en place par the Humanitarian Data center, dédié à contribuer à une professionnalisation du traitement des données dans le secteur. Il vise également à améliorer la standardisation de la gestion de l'information, permettant de faciliter le partage d'information au niveau sectoriel. Leur site donne la possibilité d'accéder à différents jeux de données pouvant être utiles à l'action humanitaire. Ainsi, on peut y télécharger des fichiers Excel postés par l'OCHA sur le nombre de déplacés à Gaza d'octobre 2023 à décembre 2023. 238 organisations y participent, dont Meta, qui a posté 219 fichiers sur la plateforme à la date du 8 janvier 2024. La firme est loin d'être la plus grande contributrice, qui est la Banque mondiale, ou différentes agences Onusiennes, UNOSAT, Unesco, WFP, UNHCR, OIM, OCHA etc. Mais Facebook se situe tout de même dans une fourchette haute et son rôle de fournisseur de données n'est pas à négliger.

mouvements de population[599]. Théoriquement, il existe la possibilité de désactiver l'option de localisation de Facebook. Mais en 2019, l'entreprise reconnait qu'il est possible de suivre des utilisateurs même dans le cas où ils indiquent ne pas vouloir être tracés. Ceci est d'ailleurs précisé dans la politique de protection des données de Facebook[600]. Notons que l'entreprise encourage le fait d'être localisable afin de profiter d'une meilleure « expérience utilisateur » comme le déclare dans un article Paul McDonald, ingénieur chez Facebook[601]. La firme de Mark Zuckerberg est condamné en 2023 par les autorités de protection des données irlandaises et norvégiennes au motif que son système de localisation des usagers ne respecte pas le droit de la protection des données[602]. Le programme Data For Good est cependant maintenu — malgré différents scandales — dont Cambridge Analytica en 2018. Il connait même un certain succès[603], notamment lors de la pandémie de Covid 19. Laura McGorman la directrice du programme déclare ainsi : « Pendant la pandémie de COVID-19, nous recevions entre 5 et 20 demandes d'accord de licence de données par jour. » [604] À l'heure actuelle, le programme a noué des partenariats avec environ 650 organisations, et collabore avec la Banque mondiale, le Fonds monétaire international (FMI), l'organisation de coopération et de développement économique (OCDE), etc., [605] dans 70 pays, majoritairement occidentaux, comme indiqué dans la carte qui suit


**PAYS PARTENAIRES DU PROJET DATA FOR GOOD DE META[606]**

Les données de géolocalisation ne sont pas systématiquement des données sensibles, l'article 9 du RGPD qui récapitule l'ensemble des données sensibles ne les mentionne pas.

[599] Privacy international, ICRC, "The humanitarian metadata problem: doing no harm in the digital era", October 2018 https://privacyinternational.org/sites/default/files/2018-12/The%20Humanitarian%20Metadata%20Problem%20-%20Doing%20No%20Harm%20in%20the%20Digital%20Era.pdf

[600] « lorsque les services de localisation sont désactivés, nous pouvons toujours déterminer votre localisation grâce aux visites, aux évènements et aux informations concernant votre connexion Internet, par exemple. Des informations de localisation spécifiques, comme le signal GPS de votre appareil, et des informations de connexion, comme votre connexion Wi-Fi ou votre adresse IP (adresse de protocole Internet), nous aident à comprendre où vous vous trouvez »
https://www.facebook.com/help/278928889350358

[601] MCDONALD, Paul, "Understanding updates to your device's location setting", 9/09/2019 https://about.fb.com/news/2019/09/understanding-updates-to-your-devices-location-settings/

[602] MEAKER, Morgan, "Norway's privacy battle with Meta is just getting started", *Wired*, 15/11/2023 https://www.wired.co.uk/article/line-coll-norway-datatilsynet-meta
MILMO, Dan, O'CARROLL, "Facebook owner Meta fined euros1.2 bn for mishandling user information", *The Guardian*, 22/05/2023 https://www.theguardian.com/technology/2023/may/22/facebook-fined-mishandling-user-information-ireland-eu-meta

[603] CHENEY, Catherine, "What the Facebook scandal means for "data for good", *Devex,* 06/04/2018, https://www.devex.com/news/what-the-facebook-scandal-means-for-data-for-good-92425
SIEGFRIED, Kristy, "Surveillance for good? Facebook tracks disaster victims", *The New humanitarian*, 08/06/2017 https://www.thenewhumanitarian.org/special-report/2017/06/08/surveillance-good-facebook-tracks-disaster-victims

[604]"during the COVID-19 pandemic, we were getting between 5-20 data license agreement requests a day." HERDAGDELEN, Amaç, DOW, Alex, STATE, Bogdan, MOHASSEL, Payman, POMPE, Alex, "Protecting privacy in Facebook mobility data during the Covid-19 response",2020 https://research.facebook.com/blog/2020/6/protecting-privacy-in-facebook-mobility-data-during-the-covid-19-response/

[605] CHENEY, Catherine, "Facebook introduces disaster maps, *Devex,* 07/06/2017 https://www.devex.com/news/facebook-introduces-disaster-maps-announces-early-partners-90427

[606] « Data for good, Anual Report », Meta, 2020 https://dataforgood.facebook.com/dfg/resources/2020-Annual-Report

Malgré tout, le G29 a en 2011 reconnu le caractère sensible des données de localisation en raison des nombreux risques qu'elles posent pour les individus. Il n'est pas étonnant que les talibans aient cherché à avoir accès aux données statistiques téléphoniques de compagnies afghanes : ces dernières comprennent un certain nombre de métadonnées très utiles pour identifier les individus[607]. Il est donc crucial de les protéger de façon efficace, d'autant que les humanitaires opèrent dans des contextes volatiles[608]. Les données des cartes de Facebook ou des programmes de CDR sont dès lors anonymisées grâce à différentes techniques de statistique : ajout de bruit et techniques d'obfuscation, techniques de type « lissage spatial », technique de « confidentialité différentielle »[609]. Toutefois, il suffit de peu de points de données pour révéler l'identité des individus. Citons par exemple les travaux d'Yves Alexandre de Montjoye, qui dès 2013 alerte sur la facilité avec laquelle une personne peut être identifiée dans un jeu de donnée de localisation[610]. L'effet « mosaïque » permettant d'identifier un individu par croisement de métadonnées est bien connu [611]. Et comme le rappellent également les chercheurs Kumar Sharad et George Danezis, il est possible de retrouver un individu à partir des données de téléphonie mobile. Cela dit, pour Yves Alexandre de Montjoye il est nécessaire malgré tout de trouver le bon équilibre entre utilité et risque de réidentification : « Nous pensons que cela met trop l'accent sur un risque limité de réidentification et de préjudice peu clair, sans tenir compte des avantages sociaux de l'utilisation de ces données, tels qu'une meilleure gestion des épidémies ou une réponse plus éclairée du gouvernement après une catastrophe. Une attention particulière devrait être accordée aux cas où les données seront employées pour le bien public ou pour éviter de graves préjudices aux personnes. »[612] Il reste alors à déterminer quel degré de granularité d'information est à la fois pertinent et respectueux de la vie privée des individus. Il n'est pas nécessairement avantageux pour les ONG d'obtenir des données permettant un suivi individuel : « Jackman s'est notamment rendu compte qu'il n'était pas utile d'envoyer des données granulaires au niveau individuel. Les organisations voulaient des tendances plus marquées dans le temps, par exemple des données sur les quartiers envoyés toutes les 90 minutes environ. »[613] Et l'équipe de Meta affirme ne pas s'intéresser à l'analyse des mobilités d'individus, mais de populations : « Nous avons décidé que nous n'allions pas

---

[607] SABIN, Sam, VOGT, Heidi, "A enormously valuable trove : america's race against afghan data", *Politico*, 30/06/2021https://www.politico.com/news/2021/08/24/taliban-afghan-data-target-allies-506638

[608] GREENWOOD, Faine, "The crucial need to secure the location data of vulnerable populations", *Brookings*, 17/12/2021 https://www.brookings.edu/articles/the-crucial-need-to-secure-the-location-data-of-vulnerable-populations/

[609] POMPE, Alex, MORO, Esteban, MCKENZIE, Denise, "Disaster mobility data network meeting - data ethics & privacy", *CrisisReady*, 03/01/2022 https://www.youtube.com/watch?v=aW3tv4S1TUw&list=PL-GWPhSfpkzzTJKynxYTOIeq8-ixo4UXf

[610] DE MONTJOYE, Y-A, HIDALGO CA, VERLEYSEN, M, BLONDEL, VD. "Unique in the crowd: The privacy bounds of human mobility", *Sci Rep* 3, 1376 (2013).

[611]" Exploring The Mosaic Effect On HDX Datasets", Centre for humanitarian data, 20/07/2020, https://centre.humdata.org/exploring-the-mosaic-effect-on-hdx-datasets/.

[612] "Posture We believe this places too much emphasis on a limited risk of re-identification and unclear harm without considering the social benefits of using this data such as better managing outbreaks or informing government response after a disaster. Special consideration should be given to cases where the data will be used for significant public good or to avoid serious harm to people".de MONTJOYE, Yves-Alexandre, KENDALL, Jake, KERRY, Cameron, "Enabling humanitarian use of mobile phone data", *Brookings*, Issues in technology innovation, november 2014. https://www.brookings.edu/wp-content/uploads/2016/06/BrookingsTechMobilePhoneDataWeb.pdf
DE MONTJOYE, YA., GAMBS, S., BLONDEL, V. *et al.* On the privacy-conscientious use of mobile phone data. *Sci Data* 5, 180286 (2018). https://doi.org/10.1038/sdata.2018.286

[613] PETRONZIO, Matt, "Facebook launches "disaster maps" to help communities recover after crises", *Mashable*, 07/06/2017 https://mashable.com/article/facebook-disaster-maps-humanitarian-aid
"One of the biggest things Jackman realized was that sending granular, individual-level data wasn't helpful. The organizations wanted higher-level trends over time such as neighborhood-focused data sent every 90 minutes or so."

construire des outils pour la recherche et le sauvetage individuels, mais que nous allions essayer de construire des outils qui vous indiqueraient comment les populations dans leur ensemble sont évacuées à nouveau et, au niveau du quartier, si les gens s'abritent sur place ou non, parce que cela nous semblait être l'une des plus grandes lacunes. »[614]Cependant, le degré de granularité des données est ainsi mis en balance avec des impératifs de vie privée et le service serait même impacté d'après un rapport de l'ONG Direct Relief par des changements de politiques de protection de données de localisation de Facebook : « Tout au long des années 2021 et 2022, un pourcentage croissant d'utilisateurs de Meta ont cessé de partager leurs données de localisation, l'un des principaux flux de données utilisés par le programme Data for Good de Meta. Cela est dû en grande partie aux changements intervenus dans les systèmes d'exploitation des téléphones portables, qui demandent désormais aux utilisateurs de reconfirmer ou de réactiver leurs préférences en matière de partage de données sur une base quasi hebdomadaire. En conséquence, les données relatives à l'historique de la localisation sont devenues plus difficilement distribuées au sein de la base d'utilisateurs de Meta et les données n'ont plus la clarté granulaire qu'elles avaient auparavant. Par conséquent, les produits de données qui s'appuient fortement sur des trajectoires assez complètes de mouvements, tels que ceux utilisés dans des contextes d'intervention d'urgence ou de crise, seront affectés. » [615]Toutefois des données « non-personnelles » peuvent aussi être à risque[616], ainsi que les « données collectives »[617]. De façon plus générale, et pour revenir aux CDR, l'OIM ne collecte pas de données sur des exilés vénézuéliens pour son programme d'analyse des récurrences de trajectoires de mobilité à certains points de passages informels aux frontières, comme c'est le cas en Équateur : « Les données de CDR pourraient révéler l'emplacement et l'importance des personnes qui traversent à ces points de passage non

[614] "that's really powerful about Facebook data is that it's information at scale and we decided that we weren't going to be building tools for individual search and rescue we were going to be trying to build tools that told you about how populations at large we're evacuating again and a neighborhood level whether or not people were sheltering in place because that to us seemed to be one of the biggest gaps" Did data make a difference? Lessons from Facebook data for good in 2020, CrisisReady, 29/01/2021 https://www.youtube.com/watch?v=-F6CNTGYztk

[615] "throughout 2021 and 2022, an increasing percentage of Meta users have discontinued the sharing of their location history data, one of the primary data streams used by Meta's Data for Good program. This is largely due to changes in mobile phone operating systems, which now ask users to re-confirm or re-enable their data sharing preferences on a near weekly basis. As a result, location history data have become more thinly distributed across Meta's user base and the data lacks the granular clarity it once had. Consequently, data products that rely heavily on fairly complete trajectories of movement patterns, such as those used in emergency response or crisis contexts, will be impacted." BALSARI, Satchit, BUCKEE, Caroline, CHAN, Jennifer, SCHROEDER, Andrew, "the Use of Human Mobility Data in Public Health Emergencies", CrisisReady, April 2022
https://www.crisisready.io/wp-content/uploads/2022/06/The-Use-of-Human-Mobility-Data-in-Public-Health-Emergencies.pdf

[616] D'ailleurs la nouvelle politique de protection de données de l'ONU entrée en vigueur en mars 2024 comprend un article dédié aux données non personnelles sensibles. D'après le texte, ces dernières doivent être protégées au même titre que les données personnelles. L'organisation la décrit comme suit : par « donnée non personnelle à caractère sensible », on entend toute information, quelle qu'en soit la forme, qui, tout en ne se rapportant pas à une personne physique identifiée ou identifiable, peut, dans tel ou tel contexte sensible, exposer à un risque de préjudice certaines personnes et certains groupes, notamment les personnes et les groupes de personnes vulnérables ou marginalisées comme les enfants. » Circulaire du Secrétaire général Politique de protection des données et de confidentialité du Secrétariat de l'Organisation des Nations Unies
https://documents.un.org/doc/undoc/gen/n24/069/81/pdf/n2406981.pdf?token=5E8SbKIdOHd6goxvK8&fe=true
A contrario plusieurs documents législatifs visent à favoriser la circulation des « données non personnelles » par opposition à la protection de données personnelles. Il ne faut pas oublier que le RGPD a été assorti d'un vote du règlement (UE) 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne. MOURON, Philippe, "la libre circulation des données est devenue la cinquième liberté consacrée dans le droit de l'union européenne", *La Revue européenne des médias et du numérique*, N°49 hiver 2018-2019https://la-rem.eu/2019/03/la-libre-circulation-des-donnees-est-devenue-la-cinquieme-liberte-consacree-dans-le-droit-de-lunion-europeenne/

[617] LINNET TAYLOR, "Safety in numbers? Group privacy and big data analytics in the developing world", TAYLOR, L. , VAN DER SLOOT, B.; FLORIDI, L., (eds), *Group privacy : the Challenges of New data technologies*, Sringer, 2016

officiels, ce qui pourrait les mettre en danger. » [618] Et la chercheuse Linnet Taylor nous rappelle que la protection de la vie privée doit s'ancrer dans une analyse contextuelle qui n'est pas réductible à des techniques d'anonymisation reposant sur une méthodologie purement statistique[619]. De surcroit, malgré sa finalité humanitaire, il semblerait que ce projet relève d'une forme de « data colonialisme », au même titre que des programmes d'accès à Internet spécifiquement dédiés aux pays en voie de développement comme Free Basic, ou encore « Discover » [620]. Le programme « data for good » de Facebook contribue à légitimer l'exploitation de données et du capitalisme de surveillance, et au renforcement de monopoles informationnels et créer de fait une certaine dépendance en matière de connaissance[621]. Plus généralement, on peut dire que les initiatives de type « philanthropie informationnelle » risquent d'aboutir à un accaparement de la définition du bien commun [622], tout en posant une série de risques pour les individus en matière de vie privée. Et la notion même de philanthropie des données est problématique, comme le font remarquer Emmanuel Letouze, Patrick Vinck et Lanah Kammourieh dans un rapport de DataPopAlliance[623]. Selon eux, ce type de programme repose sur l'idée implicite que donner accès à des données est un acte de charité alors que les données appartiendraient en fin de compte aux individus. En ce sens, ce genre d'initiative ne bénéficie en effet pas aux premiers concernés : ni les ONG ni les bénéficiaires n'ont accès aux données des cartes proposées par Facebook. On peut donc opposer cartographie extractive et cartographie participative [624]. Le fil rouge de notre

---

[618]« CDR data might expose the location and magnitude of people crossing at these unofficial crossing points, which may put them at risk. »GERSTLE, Talia et al. , Assessing the use of call detail records (CDR) for monitoring mobility and displacement, IOM February 2021

[619] LATONERO, M., "Big Data Analytics and Human Rights: Privacy Considerations in Context". In, LAND, MK, ARONSON, JD, eds. *New Technologies for Human Rights Law and Practice*. Cambridge University Press; 2018, p.149-161

TAYLOR, Linnet, "No place to hide? The ethics and analytics of tracking mobility using mobile phone" *Environment & Planning D: Society & Space, 34*(2), 319-336

[620] ZEEVI, Yoav, "Facebook introduces discover : exploring new ways to support connectivity", Facebook, 05/05/2020 https://tech.facebook.com/engineering/2020/5/discover/

TOBIN, Meaghan, "How facebook discover replicated many of the free basics'mistakes", *Rest of world,* 08/06/2021https://restofworld.org/2021/facebook-connectivity-discover/

NOTHIAS, T. "Access granted: Facebook's free basics in Africa", *Media, Culture & Society*, 42(3),2020, p. 329–348.

TAYLOR, L., BROEDERS, D., "In the name of development: Power, profit and the datafication of the Global South", *Geoforum*, 64, 2015, p. 229–237.

Advox, "Can Facebook connect the next billion? "27/07/2017 https://advox.globalvoices.org/2017/07/27/can-facebook-connect-the-next-billion/

PEI, Lucy, OLGADO, Benedict Salazar, CROOKS, Roderic,"Market, Testbed, Backroom: The Redacted Internet of Facebook's Discover", In CHI *Conference on Human Factors in Computing Systems* (CHI '21), May 8–13, 2021, Yokohama, Japan. ACM, New York, NY, USA 13 Pages. https://doi.org/10.1145/3411764.3445754

KWET, Michael," Digital colonialism, The evolution of US empire", *TNI*, 04/03/2021 https://longreads.tni.org/fr/digital-colonialism-the-evolution-of-us-empire

[621]NGWENYAMA, OJELANKI, ROWE, Frantz, KLEIN, Stefen, ZINNER HENRIKSEN, Helle, " The Open Prison of the Big Data Revolution: False Consciousness, Faustian Bargains", and Digital Entrapment Information Systems Research 0 0:0, https://doi.org/10.1287/isre.2020.0588

MAGALHÃES, João Carlos, COULDRY, Nick, "Taking Away: Big Tech, Data Colonialism, and the Reconfiguration of Social Good", *International Journal of Communication*, 15(2021), p.343–362

[622] TAYLOR, L. "The ethics of big data as a public good: which public? Whose good? ", *Philos Trans A Math Phys Eng Sci*. 2016 28;374(2083)

TAYLOR, Linnet, BROEDERS, Dennis, "In the name of Development: Power, profit and the datafication of the global South", *Geoforum*, 64. P. 229-237

MCDONALD, Sean Martin, "Data Reiew Boards: Facebook, data governance and trusts in practice",*Digital Impact*, 03/04/2018 https://digitalimpact.io/data-review-boards-facebook-data-governance-and-trusts-in-practice/

[624] « Même des projets éminemment participatifs et mondiaux comme OpenStreetMap peuvent être sujets à des biais de représentation avec un Sud global sous-représenté dans la production de données, et des tensions entre contributeurs historiques du Nord et nouveaux usagers/contributeurs du Sud ne rentrant pas forcément dans la culture du projet. Cette dynamique est par ailleurs complexifiée par le fait qu'une forme de "décolonisation d'OpenStreetMap" a bien lieu par la production massive de données au Sud depuis quelques années… mais que celle-ci étant impulsée en grande partie par des multinationales cherchant à exploiter les données produites par les contributeurs locaux, elle peut aussi au contraire être vue comme néocoloniale. »

première partie a été le suivant : quels types de risques génère le rapprochement de l'humanitaire avec le secteur privé en matière de protection des données ? Les théories du capitalisme de surveillance nous donnent des éléments de réponse en mettant en lumière son caractère extractif, centré sur une économie de la donnée. Mais une part des risques est aussi associée avec sa dimension expérimentale, s'inscrivant dans des dynamiques coloniales. La thèse de l'humanitaire comme laboratoire peut être cependant nuancée. Certes, il existe des expérimentations technologiques, des partenariats avec des entreprises saisissant l'opportunité de développer un produit dans un cadre plus souple, même si cela va de pair avec un certain nombre de risques en matière de protection des données. Mais il faut prendre aussi en compte la diversité des contextes et des dynamiques locales. Et il faut aussi être attentif à la montée en puissance des discours visant à mettre en avant la nécessité d'une souveraineté numérique, notamment en Afrique. Aussi, les reconfigurations géopolitiques actuelles pourraient rebattre les cartes, rendant le terrain moins favorable pour les entrepreneurs occidentaux, mais peut être plus ouverts pour d'autres acteurs, par exemple de nationalité chinoise. L'agentivité des États reste discutée, ainsi que le poids et l'influence des « nouveaux entrants »[625], sachant que les revendications de souveraineté peuvent être instrumentalisées[626]. Mais pour le moment, et dans le cadre de notre thèse, nous enquêtons sur les acteurs occidentaux, ce qui implique alors de prendre en compte un autre facteur, qui permettrait d'atténuer les risques liés aux expérimentations technologiques, à savoir l'entrée en vigueur du RGPD.

Cartong, « Changer de perspective : pour une approche locale de la donnée, débats et défis de la localisation de l'aide et de la gestion de données », Janvier 2024 https://www.im-portal.org/Changer-de-perspective-pour-une-approche-locale-de-la-donn%C3%A9e
DOUG Specht,ed., *Mapping Crisis : Participation, Datafication and Humanitarianism in the Age of Digital Mapping*, London: University of London Press, 2020

[625] LETERME, Cedric, GAGLIARDONE, Igor, "vers un internet chinois en Afrique, pas si vite...", *CETRI,* 29/01/2021 https://www.cetri.be/Vers-un-Internet-chinois-en

[626] « Par ailleurs, ce nouveau récit de promotion d'une souveraineté numérique africaine soutenue par la Russie porte en lui les germes de stratégies plus offensives, notamment à l'égard des opérateurs et plateformes occidentales présents dans la région – au premier rang desquelles les entreprises françaises comme Orange. Présent dans de nombreux secteurs de l'économie ouest-africaine, le groupe français pourrait très bien se retrouver la cible de campagnes antifrançaises sur fond de dénonciation de la perpétuation d'un « néocolonialisme numérique » auquel la Russie pourrait apporter des solutions grâce aux entreprises de l'écosystème du Runet souverain. » LIMONIER, Kévin, "La "souveraineté numérique", nouveau vecteur de l'influence russe en Afrique francophone ?", *Le Rubicon*, 01/02/2024https://lerubicon.org/la-souverainete-numerique-nouveau-vecteur-de-linfluence-russe-en-afrique-francophone/
SOULE, Folashade, "Rivalités géopolitiques et partenariats numériques en Afrique, stratégies d'adaptation et défis", Etudes de l'IFRI, décembre 2023 https://www.ifri.org/sites/default/files/atoms/files/ifri_soule_partenariats_numeriques_afrique_2023.pdf

On l'a vu, une crise est, en tant que moments de suspension du droit, l'occasion pour des firmes d'expérimenter des technologies encore peu éprouvées, comme des drones ou des dispositifs biométriques. Mais cette conception de l'humanitaire peut être nuancée. La juriste Fleur Johns rappelle que le secteur est loin de flotter dans une zone de non-droit[627]. Mais cette dernière n'évoque pas le droit de la protection des données, alors qu'il permettrait, a priori, de nuancer cette image d'un secteur humanitaire comme laboratoire technologique. Il revient donc à ce chapitre de revenir sur le Règlement et sur la façon dont il encadre (ou non) l'innovation humanitaire. Précisons d'emblée que nous avons adopté dans le chapitre précédent une échelle internationale, sans nous restreindre à une zone spécifique. Or le RGPD est européen, ce qui implique de circonscrire notre terrain à des ONG opérant dans ce continent ? Ce n'est pas nécessairement le cas. Le RGPD a un champ d'application relativement large et se dote d'une portée extraterritoriale. Il concerne en effet théoriquement à tout acteur européen, qu'il agisse ou non dans cette zone géographique. Les humanitaires en mission sur le terrain devraient a priori s'y reporter, tant qu'ils dépendent de sièges situés dans ce continent[628]. Deuxième point, le RGPD a été érigé en texte de référence en matière de protection des données. Et l'on peut observer que les textes de droit souple (politique de protection de données, guides.) d'ONG ne devant pas nécessairement appliquer le Règlement (comme des ONG américaines ou des organisations internationales) s'en inspirent en partie. Par voie de conséquence, un grand nombre d'organisations humanitaires sont, directement ou indirectement, concernées le RGPD.

Pour en venir au vif du sujet, ce chapitre porte sur l'encadrement de l'innovation, et consiste donc en un contrepoint des lignes précédentes. On est donc partie de l'idée qu'avec l'entrée en vigueur du RGPD, on ne peut plus souscrire à la thèse de l'humanitaire comme laboratoire technologique. Il faut dire que le règlement a été présenté en tant que « big bang », une révolution législative, etc. [629] . Le règlement est donc d'application plus large que la Directive 95/46/CE sur la protection des données personnelles par sa portée extraterritoriale, reposant sur une plus grande responsabilisation des acteurs. Le texte parait pléthorique avec ses 99 articles, sachant que la Directive de 1995 n'en comptait « que » 34. Un bon nombre d'entrepreneurs l'ont alors accusé de freiner l'innovation, voyant dans le règlement un texte contraignant, allant à l'encontre de la liberté de création. Il est en effet parfois perçu comme

[627] "like other practices in the global digital economy, digital humanitarian initiatives are often characterized as taking place in lawless, ungoverned spaces. Nonetheless, a dense array of international, regional, national, and subnational laws, guidelines, and standards—both "hard" and "soft"—are implicated in developments in the global digital economy and have borne upon the development and deployment of the digital interfaces discussed throughout this book." , « comme d'autres pratiques de l'économie numérique mondiale, les initiatives humanitaires numériques sont souvent caractérisées comme se déroulant dans des espaces sans loi et sans gouvernance. Néanmoins, un large éventail de lois, de directives et de normes internationales, régionales, nationales et infranationales - à la fois « dures » et « souples » - sont impliquées dans les développements de l'économie numérique mondiale et ont influé sur le développement et le déploiement des interfaces numériques dont il est question dans cet ouvrage. » JOHNS, Fleur, *#Help Digital Humanitarianism and the Remaking of International Order*, Oxford University press, 2023, 178 p.

[628] THELISSON, Eva, « La portée du caractère extraterritorial du Règlement général sur la protection des données », *Revue internationale de droit économique*, 2019/4 (t. XXXIII), p. 501-533. https://www.cairn.info/revue-internationale-de-droit-economique-2019-4-page-501.htm

[629] ROSSI, Julien, « La structure argumentative d'un demi-siècle de politique européenne de protection des données à caractère personnel », *Politique européenne*, 2023/3 (N° 81), p. 54-85. https://www.cairn.info/revue-politique-europeenne-2023-3-page-54.htm

une série de mesures bureaucratiques, coercitives, dont l'application est un fardeau[630]. La communication des autorités de protection des données, comme la CNIL, met en avant au contraire un Règlement doté d'un cadre équilibré[631] ; laissant une marge de manœuvre à l'innovation technologique, tout en protégeant les personnes concernées[632].

C'est qu'il s'agit certes de protéger l'information, mais aussi d'assurer la circulation de ces dernières afin de soutenir l'innovation. Si on prend un peu de recul, il n'est pas étonnant qu'à l'époque la négociation de la Directive de 1995 ait été impulsée en partie par la DG Commerce. Cette dernière s'inscrit donc dans la lignée de la stratégie économique de l'UE ayant comme finalité le renforcement de sa compétitivité, la Stratégie européenne de Lisbonne[633] .

Ajoutons qu'une chercheuse comme Anu Bradford repose l'équation entre régulation et innovation, en rappelant que l'écosystème américain ne doit pas simplement son rang hégémonique a une réglementation souple en matière d'innovation et de protection des données. La Directive européenne de 1995 était déjà peu contraignante, ce qui n'a pas conduit à l'émergence d'acteurs aussi puissants. Ce sont d'autres caractéristiques de l'écosystème américain qui auraient selon elle permis l'ascension du secteur du numérique, et plutôt que le RGPD, elle pointe l'absence d'un marché européen, ainsi que de mécanisme de financement de l'innovation[634].

En tout cas, après un examen plus approfondi, le RGPD est plus « souple » qu'il n'y parait. Cela est en partie expliqué par le fait qu'il est le fruit d'intenses négociations entre différentes coalitions d'acteurs qu'a dépeintes Julien Rossi. Par exemple, l'objectif de la coalition des groupes d'intérêts industriels a consisté à tempérer le RGPD afin de préserver la liberté d'entreprendre[635]. Cette dernière a pu ainsi défendre l'idée de concentrer l'application du Règlement sur les données à haut risque. Cet argument est contesté par une deuxième

---

[630] Pour faire simple, le droit souple (ou soft law) est constitué de normes, standards, recommandations, lignes directrices, guides, etc. Alors que le droit dur est équivalent à un droit contraignant, dont le non-respect est sanctionné. Pour reprendre les précisions de Mireille Delmas Marty, l'anglais, qui confond les trois termes, oppose différentes sortes de *soft law* (le flou, le mou, le doux) au *hard law* (le précis, l'obligatoire et le sanctionné)
HACHEZ, Isabelle, « Balises conceptuelles autour des notions de "source du droit", "force normative" et *"soft law"* », *Revue interdisciplinaire d'études juridiques*, 2010/2 (Volume 65), p. 1-64. https://www.cairn.info/revue-interdisciplinaire-d-etudes-juridiques-2010-2-page-1.htm

[631]« La CNIL souhaite également répondre aux critiques – notamment celles de l'entrepreneur français Gilles Babinet –, qui estiment que le contrôle de la Commission bride l'innovation. "Il y a un débat sur 'la CNIL empêcheuse d'innover en rond'. Nous voulons déconstruire cet a priori. La CNIL s'est réorganisée pour accompagner l'innovation, avec l'intégration d'une douzaine d'experts techniques. [...] Cette direction des innovations et études a souhaité s'insérer dans les milieux qui portent l'innovation", tonne Isabelle Falque-Pierrotin. »
PEPIN, Guénaël, "Vie privée: la CNIL veut ménager protection et innovation", *Le Monde*, 24/04/2013
https://www.lemonde.fr/technologies/article/2013/04/24/vie-privee-la-cnil-veut-menager-protection-et-innovation_3164958_651865.html
ROSSI, Julien, « Protection des données personnelles et droit à la vie privée : enquête sur la notion controversée de " donnée à caractère personnel " » Science politique, Université de Technologie de Compiègne, 2020, tel-03155480

[632] FLORIDI, Luciano, « The End of an Era: from Self-Regulation to Hard Law for the Digital Industry », *Philos. Technol.* 34, 619–622 (2021). https://doi.org/10.1007/s13347-021-00493-0

[633] Le processus de Lisbonne constitue un des piliers de la politique économique de l'UE entre 2000 et 2010. Son objectif est de soutenir le développement de l'économie de connaissance et la compétitivité, et correspond donc à un prisme néolibéral de l'innovation.
VALLUY, Jérôme, « De l'histoire de l'informatique en expansion sociétale...au capitalisme de surveillance et d'influence (1890-2023), *Collection HNP, Terra HN édition*, 2023http://www.reseau-terra.eu/IMG/pdf/-30.pdf

[634] Bradford, Anu, The False Choice Between Digital Regulation and Innovation (March 7, 2024). Northwestern University Law Review, Vol. 118, Issue 2, October 6, 2024, https://ssrn.com/abstract=4753107 or http://dx.doi.org/10.2139/ssrn.4753107
BRADFORD, Anu, *Digital empires, the global battle to regulate technology*, Oxford university press, 2023, 608 p.

[635] « La coalition industrielle axée sur l'industrie publicitaire et l'industrie du crédit financier, favorable à un assouplissement des règles en matière de protection des données afin de favoriser une innovation technique perçue par ces acteurs comme favorable à la croissance économique en général et à la leur en particulier, mais aussi à l'intérêt des consommateurs désireux de telles innovations et de croissance. »
ROSSI, Julien, « Protection des données personnelles et droit à la vie privée : enquête sur la notion controversée de "donnée à caractère personnel" » Science politique, Université de Technologie de Compiègne, 2020, tel— 03155480

coalition d'acteurs, plus franchement en faveur de la défense du droit à la vie privée[636]. Le texte est donc le produit d'un certain nombre de compromis entre groupes aux intérêts parfois divergents, d'où le fait qu'il contienne des ambiguïtés et des points de flou. Or pour Mireille Delmas Marty, le flou d'un texte de loi est généralement comblé par la production de droit souple, à savoir des guides, recommandations, lignes directrices, standards, etc. Toutefois, le statut du droit souple est discuté parmi les juristes. Il permettrait, en conservant une marge d'interprétation, d'assouplir la rigidité du droit dur[637]. Mais son effectivité est également mise en cause. Le droit souple n'étant pas contraignant, comment garantir son application[638] ? Toujours est-il que l'opposition soft law/hard law ne doit pas être entendue de façon binaire, mais plutôt comme une forme de continuum. D'ailleurs, le RGPD, qui est théoriquement du droit dur en tant que Règlement, est caractérisé par une certaine part de flexibilité en son cœur. Cette dernière n'est pas simplement due au manque de précision de ses articles, mais à une « nouveauté » du RGPD qui, contrairement à la Directive de 1995, repose sur une logique de « compliance »[639].

Cette dernière consiste en une forme d'autorégulation par les organisations et non plus en un contrôle vertical par une autorité publique. D'après la juriste Marie Anne Frison Roche, ce type de mécanisme tend à être adopté lorsque les pouvoirs publics n'ont pas la force d'assurer l'effectivité d'une loi, et plus particulièrement en ce qui concerne ce qu'elle qualifie d'« objectifs monumentaux » : la lutte contre la corruption, contre le blanchiment d'argent, le terrorisme, et donc la protection des données[640]. La Directive de 1995 exigeait une déclaration au préalable par une entreprise à la CNIL en cas de traitement de données. Cette dernière le validait ou non. Le RGPD allège, en partie, le travail des autorités de protection des données. En l'occurrence, c'est au responsable de traitement de s'en assurer et de démontrer sa conformité juridique en cas de contrôle a posteriori par une autorité. Le rôle de cette dernière est maintenant d'accompagner les responsables de traitement dans l'effort de conformité, par la production de droit souple, référentiels, lignes directrices. Quant aux firmes, elles doivent documenter leur démarche de mise en conformité avec les règles auxquelles les infractions font l'objet de sanction. Elles peuvent être punies pour un manquement aux règles de droit, mais aussi de ne pas avoir prévenu de telles atteintes. Ceci exige la mise en place de mécanismes et de systèmes de suivis internes ainsi qu'une stratégie de prévention de risque, qui nécessite une application en amont de dispositifs de « compliance » : programmes de conformité, procédures d'alerte, cartographie des risques, etc. L'établissement d'une

[636] « La coalition de la « privacy community » (ou « privacy groups155 ») centrée sur l'association European Digital Rights (EDRi) et sur le Groupe de travail de l'article 29, favorable à des règles plus contraignantes de protection des données au nom de la protection des droits fondamentaux, et notamment des droits à la vie privée et à la protection des données à caractère personnel. »
ROSSI, Julien, *ibid*.

[637] DELMAS-MARTY, Mireille, *Le flou du droit*, PUF, Quadrige, 2004, 390 p.

[638] CASSELLA, S., V. LASSERRE, V., LECOURT, B. (dir.), *Le droit souple démasqué, Articulation des normes privées, publiques et internationales*, Pedone, Paris, 2018, 194 p.
SOREL, Jean- Marc, « Le rôle de la soft law dans la gouvernance mondiale : vers une emprise hégémonique », *Le Grand continent*, 21/03/2021 https://legrandcontinent.eu/fr/2021/03/21/role-de-la-soft-law-dans-la-gouvernance-mondiale-vers-une-emprise-hegemonique/

[639] ROSSI Julien, « La structure argumentative d'un demi-siècle de politique européenne de protection des données à caractère personnel », *Politique européenne*, 2023/3 (N° 81), p. 54-85. https://www.cairn.info/revue-politique-europeenne-2023-3-page-54.htm

[640]GAUDEMET, Antoine, « Qu'est-ce que la *compliance* ? », *Commentaire*, 2019/1 (Numéro 165), p. 109-114. https://www.cairn.info/revue-commentaire-2019-1-page-109.htm
FRISON-ROCHE,Marie-Anne (dir.), *La juridictionnalisation de la compliance*, Dalloz,2023 504 p.

évaluation des risques permet ainsi de réfléchir à des opérations permettant d'éviter ces derniers, selon le secteur d'activité de la structure[641].

Mais en quoi les mesures de compliance remettraient-elles en cause notre hypothèse initiale ? On était partie de l'idée que le RGPD permettrait d'encadrer l'innovation et de tempérer l'image d'un secteur humanitaire comme laboratoire technologique. On avait en tête un règlement contraignant, pouvant restreindre de façon claire les atteintes à la vie privée dues à un manque de cadre solide, venant combler le vide législatif entourant le numérique humanitaire. Or, on verra que dans leur mise en œuvre du RGPD, les ONG s'appuient encore, dans une certaine mesure, en raison des points de flous du Règlement, mais aussi, pour implémenter des mesures de « compliance », sur du droit souple. Cela pose évidemment question au regard des débats entourant ce dernier et sa force de contrainte. Et surtout, la démarche de « compliance », propre au RGPD, n'est pas dépourvue de limites. Tout d'abord, elle repose sur une forme de délégation du travail de contrôle de l'application du droit. Or l'humanitaire est traversé par de fortes inégalités de ressources financières et humaines. D'où un manque de compétence, renforcé par un déficit d'accompagnement par les autorités de protection des données. Ceci est flagrant si l'on s'intéresse à l'approche par les risques (et notamment les études d'impact de risque d'atteinte à la vie privée) qui va de pair avec les mesures de « compliance ». En effet, le RGPD et les autorités de protection des données ne leur procurent pas d'indicateurs clairs pour évaluer les risques et donc encadrer de façon rigoureuse les usages technologiques et l'innovation. Et pourtant, malgré tout ce que l'on vient de dire, le RGPD pourrait peut-être contenir des mesures permettant d'encadrer l'innovation : les approches de type « privacy by design » qui reposent sur la responsabilisation des ingénieurs. Cependant, on ne doit pas oublier de réinscrire cette démarche dans un contexte sociopolitique pour en comprendre les limites, et surtout ne pas déléguer totalement à l'outil technique le respect des principes de protection des données.

## Section 1 – Logique de « compliance » et RGPD

[641] CEPD, « Responsabilisation sur le terrain- Partie II : analyses d'impact relatives à la protection des données et consultation préalable », Juillet 2019, https://www.edps.europa.eu/system/files/2021-07/19-07-17_accountability_on_the_ground_part_ii_en_445_fr.pdf
EDPS, "Accountability on the ground Part I : records, registers and when to do data protection impact assessments", February 2018 https://www.edps.europa.eu/sites/default/files/publication/18-02-06_accountability_on_the_ground_part_1_en.pdf

Notre premier chapitre partait du principe que l'action humanitaire se déploie dans des contextes peu régulés, des crises, des guerres, en somme des moments de suspension du droit. Toutefois, ce tableau peut être nuancé.

Tout d'abord, en réaction aux critiques relatives au manque de redevabilité du domaine, s'en sont suivis dans les années 1990 une standardisation et régulation de l'aide. Elles ont donné lieu à l'édiction de normes et de droit souple, comme a pu le décrire Kristin Sandvik : « la bureaucratisation et la régularisation de l'action humanitaire s'effectuent principalement par la prolifération de normes non contraignantes résultant d'accords juridiques multilatéraux, de l'arbitrage international et de la capacité accrue des organisations internationales à élaborer des lois. »[642] Mais, toujours d'après Kristin Sandvik, s'il existe au sein du secteur un vaste corpus de « soft law », la gouvernance de l'espace humanitaire ne passe pas par du droit dur : « Cette ambivalence à l'égard de la réglementation juridique se retrouve dans l'ensemble de l'espace humanitaire. Alors que le secteur est fondé sur le droit international humanitaire et qu'il lutte depuis des décennies pour améliorer la responsabilité, les procédures juridiques jouent un rôle limité dans la gouvernance humanitaire. »[643]

Il est vrai que certains DPO ont pu faire le constat de ce qui leur parait être un « manque » de culture juridique, qui s'exprimerait donc aussi dans le champ de la protection des données : « *C'est vrai que la culture juridique dans le milieu des associations est parfois encore un peu faible… Donc ce qui m'a plu en fait, c'est d'avoir tout un terrain à construire et à sensibiliser. Voilà, c'est vraiment cet esprit de construction et de partir presque de zéro parfois… même si… des bonnes pratiques à faire. Il y a quand même beaucoup à faire. Et surtout dans le domaine humanitaire, où il y a de gros besoins d'encadrement juridique encore.* »[644]

Toutefois, toujours selon les personnes interrogées, on observerait une évolution sur ce point : « *C'est vrai que les ONG n'ont pas tellement de culture juridique, c'est simplement depuis quelques années que ça se renforce qu'ils ont de plus en plus tout simplement des services juridiques, donc c'est quelque chose qui, au départ… voilà on n'avait qu'un juriste par ONG, donc de plus en plus les ONG, se professionnalisent…* »[645]

Kristin Sandvik va dans le même sens. Ceci serait dû, pour la chercheuse, à l'émergence au sein de l'humanitaire d'un besoin plus fort de redevabilité qui manquerait à l'éthique : « Malgré — ou peut-être parce que — les humanitaires viennent de passer une décennie à élaborer une éthique des technologies humanitaires, il est aujourd'hui largement reconnu que

---

[642] « the bureaucratization and regularization of humanitarian action takes place mostly through the proliferation of soft norms resulting from multilateral legal agreements, international adjudication, and the increased law-making capacity of international organizations »
SANDVIK, Kristin, LOHNE, Kjersti, "Building a sociology of law for the humanitarian field", *Intlawgrrls*, 20/08/2017
https://ilg2.org/2017/08/20/building-a-sociology-of-law-for-the-humanitarian-field/

[643] « this ambivalence to legal regulation can be found across humanitarian space. While the sector is grounded in international humanitarian law and has for decades struggled to improve accountability, legal procedures play limited roles in humanitarian governance. Towards the mid-2020s, the humanitarian sector grapples with new challenges as humanitarian aid has become contested globally, with unprecedented efforts to control humanitarian work. Yet, even where the organizations are specifically dedicated to legal protection, such as with UNHCR's work on refugee status determination or the legal aid projects of the Norwegian Refugee Council, the organizations do not see law as intrinsic to their accountability objectives, or lawyers as necessary to run their multi-billion enterprise. » SANDVIK, Kristin, « The ambivalent juridification of the humanitarian space », *Verfassungsblog,* 31/01/2024 https://verfassungsblog.de/the-ambivalent-juridification-of-humanitarian-space/
SANDVIK, Kristin, JACOBSEN LINDSKOV, Katja, MCDONALD, Sean Martin, "Do no harm : a taxonomy of the challenges of humanitarian experimentation", *International review of the Red Cross*, 99 (1), 2017, p.319-344

[644] Entretien n°86, ONG22,DPO juriste, 27/10/2022

[645] Entretien n°86, ONG22, DPO juriste, 27/10/2022

la régulation de la transformation numérique est nécessaire dans un secteur où les cadres éthiques ne vont pas de pair avec de solides mécanismes de responsabilité. » [646]

On peut partir de son constat pour poser la question suivante : existerait-il au sujet de la numérisation de l'aide un mouvement de bascule du droit souple au droit dur ? Pour commencer, il est vrai que l'on constate que cette dernière a d'abord été accompagnée par la sortie d'un certain nombre de guides, rapports, etc. On peut en donner un premier aperçu dans le tableau qui suit :

| |
|---|
| **2010** : Publication du manuel de protection des données de l'OIM[647]. |
| **2011** : Réunion sur la protection des données en cartographie humanitaire lors de la « Crisis mappers Conference » en Suisse. L'événement est organisé par l'ONG World Vision et le collectif de cartographie Standby Task Force. Il portait sur la publication de cartes participatives lors du conflit syrien[648]. |
| **2013** : Publication du rapport « Aiding surveillance » par Privacy international. Ce dernier porte sur les risques en matière de protection des données dans l'humanitaire et le secteur du développement[649]. |
| **2014** : Lignes directrices de GSMA sur la protection de la vie privée dans l'utilisation de données de téléphonie mobile en réponse à l'épidémie d'Ebola[650]. |
| **2015** : Publication de la politique de protection de données d'Oxfam international[651]. |
| **2015** : Publication de la politique de protection de données de l'UNHCR[652]. |
| Publication d'une résolution sur la protection des données dans l'humanitaire lors de la 37ème Conférence internationale des commissaires à la protection des données et de la vie privée[653]. |
| Publication des règles de protection des données du CICR[654]. |
| **Janvier 2016** : Ouverture de l'office de protection des données du CICR ; modification des statuts du CICR pour y inclure une commission de contrôle indépendante à la protection des données. Publication des règles de protection des données du CICR[655]. |

[646] « Despite – or perhaps because – the humanitarians have just spent a decade elaborating on humanitarian technology ethics, it is today broadly acknowledged that regulation of digital transformation is necessary in a sector where ethics frameworks do not go hand in hand with robust accountability mechanisms. » SANDVIK, Kristin, « The ambivalent juridification of the humanitarian space », *Verfassungsblog,* 31/01/2024 https://verfassungsblog.de/the-ambivalent-juridification-of-humanitarian-space/

[647] IOM, "Data protection manual", 2010, 152 p. https://publications.iom.int/books/iom-data-protection-manual

[648] CHAMALES, George, BAKER, Rob,"Securing Crisis Maps in Conflict Zones. In Proceedings of the 2011" *IEEE Global Humanitarian Technology Conference, IEEE Computer Society*, USA, 2011, p. 426–430. https://doi.org/10.1109/GHTC.2011.47
"Security concerns for Libya crisis map standby Task force and UN OCHA", Openstreetmap, march 2011 https://wiki.openstreetmap.org/w/images/7/76/Security_Concerns_for_Libya_Crisis_Map.pdf

[649] HOSEIN, Gus, NYST, Carly, "Aiding surveillance, an exploration of how development and humanitarian aid initiatives are enabling surveillance in developing, countries", *Privacy International*, October 2013
https://privacyinternational.org/sites/default/files/2017-12/Aiding%20Surveillance.pdf

[650] GSMA, "Guidelines on the protection of privacy in the use of mobile phone data for responding to the Ebola outbreak", October 2014 https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2014/11/GSMA-Guidelines-on-protecting-privacy-in-the-use-of-mobile-phone-data-for-responding-to-the-Ebola-outbreak-_October-2014.pdf

[651]Oxfam, "Responsible program data policy", 2015 https://policy-practice.oxfam.org/resources/oxfam-responsible-program-data-policy-575950/

[652] UNHCR, "Policy on the protection of personal data of persons of concern to UNHCR", 2015 https://data.unhcr.org/en/documents/details/44570

[653] "Resolution on Privacy and international humanitarian action, 37th international conference of data protection and privacy commissioners", Amsterdam, 27 october 2015http://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-Privacy-and-International-Humanitarian-Action.pdf

[654]ICRC, "ICRC rules on personal data protection", February 2015 https://www.icrc.org/en/publication/4261-icrc-rules-on-personal-data-protection

[655] https://www.icrc.org/en/document/icrc-data-protection-independent-control-commission

**2017** : Publication du « Data protection handbook » par le CICR et le « Brussels Privacy Hub »[656].
**2017** : Publication par l'Harvard Humanitarian initiative du « Signal Code », un guide sur la protection des données en contexte de crise[657].
**Septembre 2020** : Publication de la seconde édition du « data protection Handbook » du CICR[658].
**Octobre 2020** : 42e conférence de la Global privacy Assembly (GPA) et adoption d'une résolution sur le rôle de la protection des données dans l'humanitaire. Création d'un groupe de travail sur le sujet[659].
**Juin 2021** : Création au CICR du « Global Advisory Board on digital threats during conflict »[660].
**2022** : Signature d'une résolution sur la protection des données par le conseil des délégués du CICR[661].
**2022** : Publication d'une nouvelle politique de Protection des données de l'UNHCR[662].

Remarquons également que si l'on a rapporté en début de chapitre des témoignages dépeignant l'humanitaire comme un secteur doté d'une « faible » culture juridique, cela ne signifie pas une absence de « sensibilité » pour la protection des données. Tout d'abord, on compte parmi les travailleurs d'organisations humanitaires des professionnels de santé, soit un corps de métier acculturé au secret médical. En outre, en raison de leur impératif de protection des populations[663], les personnels d'ONG peuvent être réceptifs aux risques numériques. D'autant qu'elles évoluent dans des contextes volatils et traitent des données sensibles, concernant des personnes potentiellement discriminées. Les entretiens avec des DPO confirment ces différents points :

[656] KUNER, Christopher, MARELLI, Massimo, "Handbook on data protection in humanitarian action, 2017 https://rm.coe.int/handbook-data-protection-and-humanitarian-action-low/168076662a
[657]GREENWOOD, Faine, HOWARTH, Caitlin, POOLE ESCUDERO, Danielle, RAYMOND, NAthaniel, SCARNECCHIA, Daniel, "The Signal code : a human rights approach to information during crisis, 2017
[658] KUNER, Christopher, MARELLI, Massimo (co-ed.), "Handbook on data protection in humanitarian action", 2020 https://www.icrc.org/en/data-protection-humanitarian-action-handbook
[659] « Résolution sur le rôle de la protection des données personnelles dans l'aide internationale au développement, l'aide humanitaire internationale et la gestion de crise, Adoptée le 15 octobre 2020 à l'occasion de la 42ème Conférence de l'Assemblée mondiale pour la protection de la vie privée »
https://globalprivacyassembly.org/wp-content/uploads/2021/01/FINAL-GPA-Resolution-International-Aid-FR.pdf
"Working Group on the Role of Personal Data Protection in International Development Aid", International Humanitarian Aid and Crisis Management Report, July 2022
https://globalprivacyassembly.org/wp-content/uploads/2022/11/2.2.h.-The-Role-of-Personal-Data-Protection-in-International-Development-Aid-International-Humanitarian-Aid-and-Crisis-Managment-Working-Group-English.pdf
[660] https://www.icrc.org/en/document/global-advisory-board-digital-threats
[661] "Safeguarding humanitarian data, background document", Council of Delegates of the International Red Cross and Red Crescent Movement, May 2022 https://rcrcconference.org/app/uploads/2022/05/16_CoD22-Safeguarding-Humanitarian-Data-Background-document-FINAL-EN.pdf
[662] UNHCR, "General policy on data protection and privacy, 2022, https://www.refworld.org/policy/strategy/unhcr/2022/en/124207
[663]MAHE, Anne-Hélène, « Qu'est-ce que la "protection" au CICR », *blog du CICR,* 28/09/2021, https://blogs.icrc.org/hdtse/2021/09/28/qu-est-ce-que-la-protection-au-cicr/
« Droit humanitaire (3/5) : MSF et la protection des populations », MSF, https://www.msf.fr/droit-humanitaire-35-msf-et-la-protection-des-populations
SOUSSAN, Judith, « MSF et la protection : une question réglée ?, discours et pratiques autour de la "protection des civils" », *CRASH*, Avril 2008 https://msf-crash.org/sites/default/files/2017-06/97590daa8b1b115332a0d77bc14d9113.pdf

« *On a eu Paris, qui est venu nous voir, qui est venu voir le siège, en disant qu'avec les lois antiterroristes, les contextes dans lesquels on travaille et le type de données qu'on a… on risque d'avoir des problèmes dans un futur très proche*. »[664]

« *Ce qui peut faire bouger les ONG ? C'est la dimension sécuritaire. C'est un prisme qui peut parler aux ONG, elles bougent quand il y a des questions d'espionnage des données par des groupes armés, des services.* »[665]

« *Ça prend bien au siège, il y a un intérêt pour le sujet, on a martelé le fait qu'il y a des responsabilités, avec des sanctions, mais je parle beaucoup d'éthique, oui c'est juridique, mais il y a beaucoup d'éthique et ça parle en raison du secret médical*. »[666]

« *Les gens sont assez sensibilisés, quand on leur parle de protection des données, c'est la protection des bénéficiaires, et ça c'est un argument qui fait écho ici.* » [667]

Mais on s'en souvient: Kristin Sandvik a pu faire le constat que malgré cette sensibilité et l'existence de soft law et de cadre éthique, le secteur était encore peu régulé[668]. Et il est vrai que les transpositions de la Directive 95/46/CE à l'échelle nationale avaient produit un paysage juridique fragmenté, protégeant inégalement les citoyens européens. Et surtout, elle laissait de côté un certain nombre d'ONG dont les terrains d'action se déployaient hors du continent. L'entrée en vigueur du RGPD aurait-il changé la donne ? Du fait de sa portée extraeuropéenne, il concerne un plus grand nombre d'ONG. En outre, une condition d'application du règlement est le fait qu'une organisation traite des données personnelles. On a déjà vu que le secteur était marqué par une quantification grandissante de ses activités. Cela dit, une bonne partie des données collectées par les ONG ne sont pas des données personnelles, mais des données statistiques, [669] qui sont partagées ensuite de façon anonymisée sur de nombreuses plateformes, comme celle gérée par l'Humanitarian Data center. Elles peuvent aussi être destinées aux bailleurs à des finalités de redevabilité. Les personnes engagées dans la collecte de ces données ne recueillent pas nécessairement l'identité légale des personnes. Cela ne signifie pas une absence d'enjeu éthique pour autant, la possibilité de ré-identification se pose toujours pour de tels jeux de données. L'idée est commune parmi les DPO d'ONG que le traitement de données non personnelles, comme des données démographiques ou géographiques, n'est pas sans risque, puisqu'elles peuvent suffire pour identifier des groupes parfois criminalisés[670]. Cependant, de telles données ne

[664] Entretien n°7, OI2, DPO, 11/12/2019
[665] Entretien n°9, ONG3, DPO, 19/12/2019
[666] Entretien n°17, ONG6,DPO, 31/01/2020
[667] Entretien n° 88, ONG24, DPO, 15/11/2022
[668] SANDVIK, Kristin, JACOBSEN LINDSKOV, Katja, MCDONALD, Sean Martin, "Do no harm : a taxonomy of the challenges of humanitarian experimentation", *International review of the Red Cross*, 99 (1), 2017, p.319-344
[669] « il s'agit d'évaluer leurs besoins, leur vulnérabilité, mais aussi leur résilience. Si des exercices annuels aussi appelés *population count* viennent recenser chaque ménage, des enquêtes sur la base d'échantillons sont également conduites régulièrement. Il s'agit d'enquêtes thématiques, liées aux secteurs humanitaires : abris, santé et hygiène, nutrition, etc. » MACIAS Léa, « Entre contrôle et protection : ce que les technologies de l'information et de la communication font au camp de réfugiés », *Communications*, 2019/1 (n° 104), p. 107-117. DOI : 10.3917/commu.104.0107. URL : https://www.cairn.info/revue-communications-2019-1-page-107.htm

[670]TAYLOR, L., FLORIDI, L., VAN DER SLOOT, B. (eds), Group Privacy : new challenges of data technologies, Dordrecht, Springer, 2017

sont pas couvertes par le RGPD, mais par des guides et des recommandations, du droit souple, produit notamment par l'Humanitarian data center, une organisation rattachée à l'OCHA[671].

Les ONG collectant de façon extensive des données statistiques sont des ONG très professionnalisées, dont les opérations respectent différents critères de standardisation. À l'autre bout du spectre, des ONG peu professionnalisées, dont les membres sont bien souvent des bénévoles, peuvent ne pas collecter de noms des bénéficiaires, voire ne pas demander leur identité, comme nous le raconte une enquêtée : « *Y'a des associations qui sont vraiment consciente de ce problème-là, y'en a qui demandent rien comme justificatif d'identité pour avoir accès à nos services qui sont du coup totalement gratuit et désintéressé. Or, nous, en fait, on va très facilement leur demander en fait une carte d'identité enfin des papiers*. »[672]

Il peut aussi arriver à de petites structures venant en aide à des exilés, de ne pas connaitre leur identité légale : « *c'est aussi quelque chose qui est susceptible d'être modifié en cours de leur parcours de migration parce qu'ils peuvent aussi changer d'identité donc et donc là cette question de données personnelles et de protection des données en fait c'est un peu étrange parce que pour eux, ils vont, pour la majorité d'ailleurs, se créer un autre prénom, en tout cas se faire appeler par un surnom qui deviendra leur prénom pour justement protéger… c'est une manière pour eux de protéger leurs données personnelles tout à fait okay…* »[673]

Pour notre enquêté, venant d'une petite ONG peu professionnalisée et militante, le fait de collecter des données identifiantes des personnes dépend de leur lien avec les acteurs étatiques : « *C'est surtout des associations qui sont contraintes… dont les activités sont bien plus ou moins proches en tout cas avec une forme de structure étatique ou gouvernementale…* »[674]

Il pourrait s'agir plus largement des bailleurs étatiques, qui au nom d'une redevabilité peuvent pousser à l'adoption de dispositifs biométriques, voire dans certains cas, la collecte de données anonymisées peut suffire, mais il peut arriver que des bailleurs étatiques exigent d'avoir accès à des données personnelles de bénéficiaires : « *On collectait des noms avant, dans nos opérations de téléphonie, de téléphonie humanitaire. Les gens viennent, font la queue et on leur donne quelques minutes d'appel par famille. Avant, on collectait des noms. Noms et prénoms. Le nombre de personnes de la famille, et un numéro de téléphone qu'on pouvait appeler. Ça permettait aux bailleurs de fonds de voir les résultats qu'ils attendaient.* » [675]

Sachant qu'on a pu faire le constat, dans nos entretiens auprès de personnes non professionnalisées dans la gestion de l'information, d'une équivalence entre la notion même de « donnée personnelle » à l'identité légale d'une personne. Or les données personnelles ne se limitent pas à de simples noms. Leur définition a fait controverse au sein des arènes dans

[671] Contrôle de la divulgation de données statistiques, OCHA, The Centre for Humanitarian Data, août 2019https://data.humdata.org/dataset/2048a947-5714-4220-905b-e662cbcd14c8/resource/64bb81f5-f21d-438d-8ad6-b7e94733c395/download/guidance-note-1-french-updated.pdf
[672] Entretien, ONG11, bénévole, 05/05/2020
[673]Entretien, ONG11, bénévole, 05/05/2020
[674] Entretien, ONG11, bénévole, 05/05/2020
[675] Entretien, ONG8, ingénieur, 31/03/2020

lesquelles le RGPD a été élaboré[676]. Rappelons simplement que selon le règlement, entré en vigueur, sont considérées des données personnelles, les informations suivantes : un nom, une photographie, une empreinte ou un scan d'iris, une adresse postale ou un email, un numéro de téléphone ou de sécurité sociale, un matricule d'employé, une adresse IP, un enregistrement sonore[677].

À titre d'exemple, une politique de protection de données de l'UNICEF précise qu'une donnée personnelle est définie par : « toute information concernant une personne identifiée ou identifiable ("personne concernée"). Une personne identifiable est une personne qui peut être identifiée, directement ou indirectement, par référence à :

i) un identifiant tel qu'un nom, un numéro d'identification, du matériel audiovisuel, des données de localisation, un identifiant en ligne, ii) un ou plusieurs éléments spécifiques propres à l'identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale de la personne ou iii) des évaluations de l'état et/ou des besoins spécifiques, par exemple dans le cadre de programmes d'assistance. La définition de ce qui constitue des données à caractère personnel est contextuelle et s'élargit, notamment en raison des progrès technologiques et des méthodes d'identification des personnes. »[678]

Et si une partie des données humanitaires relèvent de statistiques, d'un autre côté, les humanitaires collectent aussi un bon nombre de données personnelles. C'est par exemple le cas lors des différentes phases d'enregistrement des bénéficiaires. En effet des données basiques identifiantes peuvent être requises. Le terme de « données biographiques » est parfois utilisé pour décrire ce type d'information (ou « biodata » en anglais). Le type de donnée varie, mais généralement il s'agit de l'âge, du genre, d'informations de contact, de la taille du foyer et de son lieu, voire dans certains cas des données biométriques, et aussi des données de santé ou des données ethniques.

Selon certains témoignages, les identités légales des bénéficiaires ne sont pas systématiquement collectées, même si cela reste courant dans le cadre de la phase d'enregistrement des bénéficiaires. Citons par exemple ce rapport qui regrette le manque d'harmonisation de cette pratique: « tout d'abord, les noms des bénéficiaires sont collectés par pratiquement toutes les agences humanitaires. Cependant, les noms sont orthographiés différemment selon qu'ils sont enregistrés en anglais ou en somali, ce qui rend difficile la comparaison des noms entre les bases de données. Alors que les formulaires d'enregistrement de quelques agences (telles que le WFP et ACTED) prévoient des champs différents pour l'enregistrement du premier au quatrième nom, la plupart des formulaires d'enregistrement ne comportent qu'un seul champ pour l'enregistrement des noms, sans aucune instruction sur la manière dont ils doivent être enregistrés. Cela signifie que l'ordre

[676]ROSSI, Julien, « Protection des données personnelles et droit à la vie privée : enquête sur la notion controversée de "donnée à caractère personnel" » Science politique, Université de Technologie de Compiègne, 2020, tel— 03155480

[677] https://www.cnil.fr/fr/cnil-direct/question/une-donnee-caractere-personnel-cest-quoi

[678]« An identifiable individual is one who can be identified, directly or indirectly, in particular by reference to:
i) an identifier such as a name, an identification number, audiovisual materials, location data, an online identifier, ii) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual or iii) assessments of the status and/or specific needs, such as in the context of assistance programmes. The definition of what constitutes personal data is contextual and expanding particularly due to enhancements in technology and methods for identifying individualsUNICEF, Policy on personal data protection, 15/07/2020 https://www.unicef.org/supply/media/5356/file/Policy-on-personal-data-protection-July2020.pdf.pdf

dans lequel les noms sont enregistrés (premier, milieu et dernier) diffère d'une agence à l'autre. Alors que la plupart des agences humanitaires enregistrent quatre noms en raison de la similitude des noms en Somalie, d'autres n'en enregistrent que deux ou trois. De plus, les agences humanitaires telles que NRC et ACTED incluent le nom de la mère des bénéficiaires. »[679]

Dans certains cas, les ONG ne collectent pas des données nominatives, mais pour identifier les bénéficiaires « simplement » des numéros de téléphone[680], ou encore des « adresses » (dans certains camps, il existe des systèmes d'adressage des baraquements destinés aux bénéficiaires). Mais pour rappel, on a bien affaire à des données personnelles, puisqu'il s'agit de données pouvant identifier une personne concernée.

Ensuite, la collecte de données dépend du mandat de l'ONG. Par exemple, la gestion de camp de réfugiés repose sur une collecte extensive de données personnelles, comme le surligne un enquêté : « *pour les bénéficiaires de l'aide, c'est assez compliqué… C'est la jungle en fait je dirais, parce que ça dépend, c'est vraiment selon l'organisation… Si on regarde bien, il y a des organisations qui sont obligées de collecter des données personnelles, c'est indéniable. La gestion d'un camp de réfugiés ou d'un camp de déplacé implique l'identification des gens et la collecte de ses données et leurs stockages. C'est obligatoire. Une personne qui est prise en charge dans un camp, il est pas anonyme*. « [681] Un autre enquêté surenchérit : « *Dans des camps pour assurer la sécurité… Il faut au moins qu'il y ait un recensement des personnes, sinon comment on peut sécuriser l'endroit ? Y compris les… les bénéficiaires comme les personnels… Si on n'a pas l'identité des gens qui sont là, ça semblerait complètement anarchique, complètement hasardeux comme façon de faire.* » [682]

Ajoutons que les programmes médicaux donnent aussi lieu à une forte collecte de données personnelles, couplées d'informations sensibles. Cela dit, certaines ONG médicales ne mènent pas directement des programmes médicaux, et viennent en appui à des hôpitaux locaux. Elles ne collectent alors pas directement des données de santé, comme le précise un humanitaire qu'on a pu interroger sur le sujet :« *sur les programmes de traitement généraux, paracétamol, anti-inflammatoire, tout quoi. On ne distribuait pas nominativement des médicaments à des patients. On les distribuait à des pharmacies ou à des hôpitaux locaux qui les distribuaient ensuite à des patients. C'était eux qui géraient la confidentialité des patients, les*

[679] "First, recipients' names are collected by virtually all humanitarian agencies. However, names are spelt differently depending on whether they are recorded in English or Somali, making it difficult to compare names across databases. While the registration forms for a few agencies (such as WFP and ACTED) provide different fields for recording the first to fourth names, most registration forms have only one field for recording names, with no instructions on how they should be recorded. This means that the order in which names are recorded (first, middle and last) differs across the board. While most humanitarian agencies record four names due to the similarity of names in Somalia, others record just two or three. Also, humanitarian agencies such as NRC and ACTED include recipients' mothers' name."
Development initiatives, Harmonising registrations and identification in emergencies in Somalia, August 2019, https://devinit-prod-static.ams3.cdn.digitaloceanspaces.com/media/documents/Report_Harmonising-registrations-and-identification-in-emergencies-in-Somalia.pdf

[680] "Many humanitarian agencies use the phone numbers registered to receive assistance for identification because they are unique (there are no identical phone numbers), are linked to recipients' biodata and have a personal identification number (PIN) for security." Development initiatives, Harmonising registrations and identification in emergencies in Somalia, August 2019, https://devinit-prod-static.ams3.cdn.digitaloceanspaces.com/media/documents/Report_Harmonising-registrations-and-identification-in-emergencies-in-Somalia.pdf

[681] Entretien, ONG8, ingénieur, 31/03/2020

[682] Entretien, ONG5, responsable de programme medical, 26/07/2024

*intermédiaires des structures en fait. »* Sur les programmes de santé menés directement par les ONG, il est cependant nécessaire de conserver une trace des patients, notre enquêté est formel *: « lorsqu'on distribue des médicaments, à des patients, il faut savoir à qui le distribuer pour se prémunir du trafic de médicament, de la revente de matériel. En fait, on doit savoir à qui on donne les médicaments. Sinon c'est un puits sans fonds et ça peut susciter des trafics derrière. L'exemple du traitement antituberculeux… Il faut savoir à qui on donne les médicaments quoi ! Même sans suspecter de trafics… On ne peut pas dans ce type de traitement qui est lourd, extrêmement cher… On peut pas donner la seule responsabilité de l'identité au bénéficiaire lui-même, qui va se déclarer… Il va pas avoir les compétences médicales, de savoir quel médicament il a reçu, et puis il faut un check de la part de l'équipe médicale pour savoir pour savoir à qui ils donnent les traitements*. « [683] Ce responsable de programme de santé d'une ONG médicale ajoute que « *pour suivre certains traitements… comme des traitements antituberculeux, ça me semble évident qu'il faut leurs coordonnées, pour le rappeler, sinon tout le traitement, toute la démarche thérapeutique tombe à l'eau, donc il est évident que dans ce cas les ONG sont obligées de collecter les noms des patients, des bénéficiaires, ça semble évident. Ou au moins un système de codage qui permet de les retrouver facilement, mais il y a toujours moyen de réidentifier… Oui dans certains cas, il y a toujours moyen de pas noter le nom des patients. Mais dans d'autres, ça semble évident…* « [684]

Ajoutons qu'une partie des opérations recourent à des dispositifs de transfert monétaire, ce qui génère un bon nombre de données personnelles, nécessaire à la gestion des comptes bancaires des bénéficiaires (cf. chapitre 4). En outre, les programmes de Rétablissement de liens familiaux (RFL) génèrent des quantités extensives de données personnelles, à savoir des noms, les lieux de résidence et les coordonnées de personnes portées disparues et de leurs familles, d'enfants non accompagnés ou séparés de leurs proches, ou encore de détenus recevant des services du Mouvement de la Croix-Rouge et du Croissant-Rouge. D'ailleurs, lors d'une cyberattaque plus récente de la Croix-Rouge italienne se sont également des données personnelles, très sensibles, qui se sont retrouvées sur le darknet, à savoir des documents d'identités, des photographies, des formulaires de l'ONG… [685]

Et de surcroit le surligne le Global Privacy Assembly : « le traitement de données personnelles se fait dans le cadre de la mise en œuvre de nombreux programmes d'aide internationale au développement, dans l'aide humanitaire internationale et dans la gestion de crise, notamment en matière de consolidation de l'état civil et d'identification, sur lesquels reposent 12 des 17 objectifs de développement durable. »[686]

En outre, les ONG jouent dans certains cas le rôle de pourvoyeuses d'identité. Le marché de l'identité numérique, poussé par des acteurs comme Mastercard, est solide. De grands joueurs se sont positionnés sur ce sujet, comme l'UNHCR ou l'IFRC. Certains dispositifs d'identification sont dit « fonctionnels » : ce sont des documents n'ayant pas valeur de documents officiels,

[683] Entretien, ONG5, responsable de programme medical, 26/07/2024
[684] Entretien, ONG5, responsable de programme medical, 26/07/2024
[685] SEYDTAGHIA, Anouch, BUSSARD, Stéphane, « La Croix-Rouge italienne touchée par une fuite massive de données, le CICR enquête », Le Temps, 19/06/2024 https://www.letemps.ch/cyber/cybersecurite/le-cicr-a-nouveau-touche-par-une-fuite-massive-de-donnees
[686] Résolution sur le rôle de la protection des données personnelles dans l'aide internationale au développement, l'aide humanitaire internationale et la gestion de crise Adoptée le 15 octobre 2020 À l'occasion de la 42ème Conférence de l'Assemblée mondiale pour la protection de la vie privée https://globalprivacyassembly.org/wp-content/uploads/2021/01/FINAL-GPA-Resolution-International-Aid-FR.pdf

mais permettant d'avoir accès à des services au sein de l'écosystème humanitaire. De surcroit, le Norvegian Refugee Council par exemple ne fournit pas directement, mais assiste les bénéficiaires à obtenir des documents officiels, un service générant nécessairement des données personnelles[687].

Enfin, certaines ONG se sont spécialisées dans la fourniture de connectivité pour les bénéficiaires, ces dernières doivent aussi collecter des données. Les pratiques varient cependant beaucoup, selon les ONG : « *Maintenant côté bénéficiaire, on a un prénom, on demande aussi une initiale, mais en gros aujourd'hui on ne peut plus s'assurer que la personne est passée une seule fois. Ce n'est pas bien grave. D'autres organisations ont besoin de données beaucoup plus précises d'identification, ça dépend des ONG. «*[688] Dans certains contextes, il s'agit même d'une obligation légale : « *il y a des pays où… Si je prends l'exemple du Bangladesh, des Rohingya, là c'est même pire, c'est-à-dire que légalement, on se doit d'identifier les gens. Et à partir qu'une personne est identifiée comme Rohingya, on ne peut pas lui fournir de connexion internet, c'est interdit, c'est la loi. On risque de gros ennuis*. »[689]

Du fait de ces différents traitements de données, les ONG sont donc tout à fait concernées par l'obligation légale d'appliquer le RGPD, dont la mise en œuvre aurait nécessité d'après un de nos enquêtés un travail conséquent de responsabilisation des acteurs et d'encadrement des pratiques par le droit : « *C'était considéré comme normal et nécessaire d'avoir un poste de DPO. Mais à l'avènement du RGPD, il y a eu un gros travail de mise en conformité, d'avenants aux contrats, un certain nombre de choses ont été mises en œuvre, puis mises en pause avec le COVID, et on a repris le travail, ça a demandé une grosse réflexion sur les outils nécessaires à la gestion des données médicales. On est loin d'être un mauvais élève, mais par la quantité et la variété des données traitées, il y a forcément des éléments à prendre en compte.* »[690] Et il faut dire qu'on retrouve parfois dans nos entretiens l'idée d'un texte « bureaucratique », dont la mise en œuvre reste parfois en partie formelle : « *maintenant le côté RGPD dans la pratique est vu comme un processus administratif qui met des bâtons dans les roues, c'est un dernier élément à traiter, mais c'est en train de changer*. »[691]

Cependant, il n'est pas possible de parler de bascule de droit souple vers du droit dur. Comme on a commencé à le faire remarquer, plusieurs points font que le règlement est plus flexible qu'il n'y parait. Tout d'abord, nos enquêtés sont font face aux points de flou du règlement. Sans rentrer dans le détail de ces derniers, pour les DPO avec qui l'on a pu s'entretenir, ces ambigüités seraient expliquées par le fait que le texte a été pensé pour encadrer les entreprises privées et non pas des ONG. Toujours est-il que les autorités de protection des données pourraient éclairer les DPO. Un des rôles de la CNIL par exemple est d'accompagner la mise en conformité des organisations par la production de droit souple. Cela dit, il ressort de nos entretiens qu'elle ne remplirait pas ce rôle d'accompagnement pour les ONG. En l'absence de clarification de la part des autorités de protection des données, les ONG sont,

[687] Norwegian Refugee council, Legal and civil documentation response in Cameroon, April 2024 https://www.nrc.no/globalassets/pdf/reports/legal-and-civil-documentation-response-in-cameroon/factsheet---legal-and-civil-documentation-response-in-cameroon.pdf
[688] Entretien, ONG8, ingénieur, 31/03/2020
[689] Entretien, ONG8, ingénieur, 31/03/2020
[690] Entretien n°88, ONG24,DPO, 15/11/2022
[691] Entretien n°88, ONG24, 15/11/2022

semblerait-il, laissées avec leurs doutes, et renvoyées au texte de loi et à ses ambiguïtés, comme nous le confie un de nos enquêtés : « *moi j'échange beaucoup avec eux parce qu'ils ont une ligne spécifique pour les DPO, que j'utilise à foison, mais c'est rare qu'ils m'apportent une réponse claire, nos problématiques sont en marge de la législation, et la CNIL botte en touche. Elle se limite à la réglementation*. »[692]

Il n'y a pas de consensus sur la portée du RGPD parmi nos enquêtés. Le spectre d'application même du Règlement ne serait pas clair. Si on s'en tient au texte juridique, une délégation est liée au siège européen, qui a le statut de responsable de traitement, le RGPD devrait logiquement s'appliquer, surtout s'il s'agit de travailleurs européens et que des données peuvent être rapatriées au siège, situé dans le continent. Mais les ONG doivent gérer les interactions avec les droits locaux. Les choses se compliquent alors, et l'articulation des différents droits n'est pas toujours évidente, comme nous le raconte un DPO : « *on a beaucoup de projets à l'international. Quelle est la législation qui prévaut ? On est responsable de traitement, on est basé en France, et ayant des projets à l'international à mon sens c'est le RGPD qui prévaut. Mais si la législation locale vient en contradiction avec le RGPD, vu qu'on traite d'informations de personnes locales, quel est l'arbitrage qu'on doit faire ? Et là-dessus, la CNIL n'arrive pas à répondre*. »[693] Ajoutons un autre cas de figure : certaines ONG ont un fonctionnement plus décentralisé. Elles sont parfois composées d'antennes administrativement indépendantes du siège européen, mais impliquant des travailleurs humanitaires de nationalités différentes, dont certains sont européens. Il faut dans ce cas déterminer quel est le degré d'indépendance de la délégation, si le siège reste responsable de traitement ou non, question reconnue comme générant de l'incertitude[694]. Dans ce cas, l'« ONG-siège » n'est pas responsable de traitement, le RGPD ne serait pas applicable aux délégations. En effet, son article 3.2 indique qu'il s'applique pour des organisations hors Europe seulement si elles traitent des données de personnes se trouvant en Europe. Pour les délégations, l'application du RGPD n'est pas obligatoire, théoriquement. Les DPO d'ONG peuvent considérer que cela constitue un déficit de protection, et elles choisissent alors d'appliquer malgré tout le RGPD, ou du moins s'appuyer sur du droit souple : « *Puisque d'abord la conformité RGPD sur le terrain c'est quelque chose d'assez ambigu puisqu'il n'y a pas d'obligation stricto sensu d'appliquer le RGPD sur le terrain, parce que nos missions sont quand même globalement indépendantes… Et du coup, il n'y a pas de… comment dire. Donc ce sont des traitements qui sont déjà situés à l'extérieur de l'Union européenne. Donc appliquer le RGPD… c'est un peu compliqué. Donc voilà. Mais en tout cas on essaye au moins d'appliquer de grands principes du respect heu… Mais ça ne sera jamais une conformité… Aussi précise et rigoureuse que comme on l'a menée au siège (…). L'idée c'est plus d'appliquer des principes généraux du type RGPD que le RGPD en tant que tel. Et ça, c'est l'esprit de la plupart des ONG*

[692] Entretien n°88, ONG24, DPO, 15/11/2022
[693] Entrentien n° 88, ONG24, DPO, 15/11/2022
[694] « De plus, les sociétés privées et les administrations ont vu leur organisation se complexifier. Il est désormais très fréquent de se retrouver face à des groupes d'entités relativement autonomes s'échangeant régulièrement des données à caractère personnel. Il est donc devenu plus difficile d'identifier clairement qui doit être qualifié de responsable du traitement et qui est simple sous-traitant. » DELFORGE, A, 2018, » Les obligations générales du responsable du traitement et la place du sous-traitant. », Dans *: Le règlement général sur la protection des données (RGPD/GDPR): analyse approfondie*, Larcier, Cahiers du CRIDS, Numéro 44, 2018 p. 371-406
MENDOZA-CAMINADE, Alexandra, « Le rôle du sous-traitant en matière de données personnelles *»,* In : TISSEYRE, Sandrine (dir.), *Sécuriser la sous-traitance : quels nouveaux défis ?* Toulouse : Presses de l'Université Toulouse Capitole, 2019 , <http://books.openedition.org/putc/7141>

*qui travaillent sur le terrain. Et des guides repris par la Croix rouge hein. (…) Donc on essaye de mettre en pratique l'équivalent du Handbook.* »[695] Mais le recours au droit souple semble être un pis-aller pour l'enquêtée. D'ailleurs, sur la page d'un site web destiné à une formation spécialisée sur la protection des données humanitaires, il est spécifié qu' : « il n'a pas pour but de remplacer le respect des normes juridiques applicables ou des règles, politiques et procédures de protection des données qu'une organisation particulière peut avoir adoptées. Le manuel vise plutôt à sensibiliser les organisations humanitaires et à les aider à s'assurer qu'elles respectent les normes de protection des données personnelles lorsqu'elles mènent des activités humanitaires, en fournissant des conseils spécifiques sur l'interprétation des principes de protection des données dans le cadre de l'action humanitaire, en particulier lorsque de nouvelles technologies sont employées. »[696]

Notre propos n'est pas de détailler d'emblée l'ensemble des points de flou du texte. Certains seront évoqués au fil de la thèse (au sujet des analyses d'impact, mais également au sujet des bases légales du consentement et de l'intérêt légitime). Pour le moment, on se concentrera surtout dans cette section sur une autre point : l'approche par la compliance telle qu'elle est requise par le RGPD. On s'en souvient : dans le règlement les déclarations de traitement à la CNIL imposées par la Directive de 1995 sont remplacées par une démarche inspirée par l' « accountability » et par un contrôle a posteriori par l'autorité de protection des données. Une organisation n'a plus à déclarer ses traitements de données au préalable à une autorité. Au contraire. Elle a l'obligation de mettre en place des mesures techniques et organisationnelles appropriées pour prouver la conformité au Règlement en cas de contrôle a posteriori par une autorité. Ces mesures constituent une série de dispositifs de « reporting », de cartographie, de signalement. Cela implique une internalisation du contrôle du respect du droit, renversant la logique d'un contrôle vertical par une autorité externe aux entreprises. Par voie de conséquence, selon certains juristes, les protocoles de compliance marqueraient « la fin de la régulation, du moins son progressif remplacement. ». Et comme l'écrit le juriste Regis Bismuth : « la compliance ne repose plus exclusivement sur les leviers traditionnels du droit que sont l'interdiction et la sanction. Il ne s'agit plus en effet de réprimer la moindre conduite contraire aux règles applicables. Mais bien davantage. L'objectif est de développer des outils organisationnels (un plan de compliance, un plan de vigilance, etc.) destinés à prévenir et à gérer le risque de violation. »[697] C'est à l'entreprise de codifier les différents comportements susceptibles de caractériser des infractions. Pour ce faire, la firme peut édicter des codes de conduite. Ces derniers « ne se limitent pas à reproduire les définitions légales des comportements proscrits en droit interne ou international, ils définissent les lignes directrices adaptées aux spécificités de l'organisation et des activités concernées ». [698]

---

[695] Entretien n° 86, ONG22, DPO, 27/10/2022

[696]« It is not intended to replace compliance with applicable legal norms, or with data protection rules, policies and procedures that a particular organization may have adopted. Rather, the handbook seeks to raise awareness and assist humanitarian organizations in ensuring that they comply with personal data protection standards when carrying out humanitarian activities, by providing specific guidance on the interpretation of data protection principles for humanitarian action, particularly when new technologies are employed"
https://www.maastrichtuniversity.nl/events/data-protection-officer-dpo-humanitarian-action-certification

[697]BISMUTH, Régis, PASCAL, Hugo (dir.), « Les nouveaux défis de la compliance », *La Revue des juristes de sciences po*, Janvier 2019

[698] HARDY, Gaelle, "La compliance, une privatisation de la régulation? ", Dans : *La Privatisation; Revue de droit international d'Assas*, N° 5/Issue 5, 2022

Concernant le RGPD, entreprendre une démarche de compliance nécessite d'accomplir au sein d'une organisation un certain nombre de tâches, et documenter les traitements de données grâce à différents documents devant être transmis lors d'un éventuel contrôle. Ces documents permettent à une autorité de s'assurer que les mesures de conformités ont été prises. La CNIL en donne une liste indicative, que nous pouvons rappeler : le registre de traitement, les études d'impacts, les contrats noués avec les sous-traitants, les mentions d'informations aux personnes, les modèles de recueil du consentement des personnes concernées, les procédures mises en place pour l'exercice des droits[699].

Ce travail de compliance est porté en partie par le délégué à la protection des données (DPO), comme le rappelle l'article 39 du RGPD[700]. Sa nomination au sein d'une organisation est encouragée, voire requise dans les différents cas listés par l'article 37 du Règlement[701]. Le RGPD précise simplement qu'il doit être choisi en fonction de ses connaissances du droit à la protection des données. Il n'a pas nécessairement un profil juridique, des informaticiens peuvent remplir ce rôle.

Nos vingtaines d'entretiens avec des DPO nous ont donné un premier aperçu de ce type de profil professionnel. On a souhaité préciser cette première photographie d'un champ professionnel relativement récent. Pour ce faire, nous nous sommes rendue sur LinkedIn et on a sélectionné 34 profils de DPO d'ONG. On a choisi de recueillir les informations à la main. Le réseau s'est ouvert à la recherche et propose l'exploitation de données et métadonnées, grâce à des logiciels de « scraping », de collecte de « data »[702]. Nous n'y avons pas eu recours : notre échantillon est très limité (une quarantaine de profils). Et nous nous sommes contentées d'exploiter les données laissées volontairement visibles par les utilisateurs, et non pas des statistiques et indications calculées par la plateforme (les données par inférence)[703].

Plus précisément, on s'est concentrée sur les informations retraçant le parcours de la personne, sans nous intéresser aux autres indications, qu'on pouvait déduire d'une page LinkedIn, comme le degré d'intériorisation des codes de mise en valeur de soi sur le marché de l'emploi, le réseau d'interconnaissance, le degré de connexion d'un profil, etc. Pour être claire, deux informations nous ont intéressée : le domaine de formation (juridique, en science politique ou informatique), et la chronologie des parcours professionnels, à savoir la durée

---

[699] CNIL, « Documenter la conformité », 28/06/2018https://www.cnil.fr/fr/documenter-la-conformite

[700] Une des missions du DPO est de « Contrôler le respect du présent règlement, d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données et des règles internes du responsable du traitement ou du sous-traitant en matière de protection des données à caractère personnel, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant ». Article 39, règlement UE 2016/679

[701] Il est nécessaire de nommer un DPO dans les cas suivants : « a) le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle; b) les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées; ou c) les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9 ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10. »Article 37, Règlement UE 2016/679

[702] CHODORGE, Simon, « LinkedIn fait appel aux chercheurs pour devenir un nouvel observatoire de l'économie », *L'Usine Nouvelle*, 22/08/2018 https://www.usinenouvelle.com/editorial/linkedin-fait-appel-aux-chercheurs-pour-devenir-un-nouvel-observatoire-de-l-economie.N732094

[703]« Nouveau poste, obtention de fonds, publication de papiers scientifiques, participation à des conférences… La plateforme regorge de données, tantôt fournies, tantôt déduites statistiquement. Les premières correspondent à ce que les utilisateurs indiquent volontairement dans leur profil. Prénom et nom, le poste ou les postes occupés, etc. Les secondes, appelées "inférences", sont calculées par les algorithmes de la plateforme et valent cher aux yeux des publicitaires, des entreprises et des employeurs. » LOMBARDO, Eva, « Nos données LinkedIn peuvent nuire à la recherche d'emploi », *le Temps*, 08/12/2023 https://www.letemps.ch/economie/carrieres/nos-donnees-linkedin-peuvent-nuire-a-la-recherche-d-emploi

d'expérience sur un poste, la date de prise de fonction d'un DPO par rapport à l'entrée en vigueur du RGPD.

Le degré de fiabilité des informations se pose toujours sur les réseaux sociaux. Une personne peut être conduite à « falsifier » son profil, du moins à ajouter ou à supprimer des facettes de soi-même, qu'on ne juge pas nécessaire de valoriser. Sans rentrer dans ce niveau de détail, on a procédé à une vérification minimale, pour s'assurer au moins qu'il ne s'agissait pas de « faux » profil. On a avant tout croisé des informations, grâce à des requêtes sur des moteurs de recherche, et en notant si le profil était connecté ou non avec d'autres membres avérés d'une organisation.

De manière générale, on peut dire que les juristes restent majoritaires. Ils représentent 26 personnes sur les 34 fiches consultées. Une bonne proportion d'entre eux, 12 sur 34, est spécialisé en droit international ou en droit humanitaire. Parmi eux, deux personnes ont effectué une double formation en droit international et en droit du numérique. Ajoutons que 4 personnes supplémentaires ont suivi un parcours « droit du numérique », et qu'une seule personne est diplômée en droit de la protection des données. 4 personnes sont spécialisées en droit de la concurrence ou en droit de la propriété intellectuelle, et 3 personnes sont spécialisées en droit européen et en droit administratif. 6 DPO ont suivi un cursus en sciences humaines. 3 personnes sont diplômées en science politique et en relations internationales, une personne en économie, une personne en géographie et une personne en communication et en développement web. Ensuite, on notera que les DPO ayant une formation en science dure sont rares dans l'humanitaire. On compte simplement deux personnes ayant suivi ce type de formation. Enfin, deux DPO initialement informaticiens et ingénieurs ont obtenu un master en droit international ou en droit de la protection des données.

En ce qui concerne le détail de leurs parcours professionnels, une partie des DPO ont commencé leur carrière dans l'humanitaire. 13 DPO ont d'abord travaillé en tant que juristes, ou ont géré des programmes de protection, ont occupé des postes de direction ou sont spécialisés en gestion de données géographiques. Ce dernier profil est minoritaire. La plupart des DPO n'avaient pas de poste en lien avec la gestion de données. Et seule une personne faisait partie du service informatique d'une ONG avant de se reconvertir dans le domaine du droit de la protection des données et devenir DPO. En fin de compte, 14 personnes provenaient déjà du secteur humanitaire, soit la moitié environ des profils consultés. Une bonne partie des DPO d'ONG humanitaires se sont donc « reconvertis ». 9 personnes étaient au préalable DPO dans le privé. La fonction étant récente, seules deux personnes ont commencé leur carrière directement comme DPO dans l'humanitaire sans expérience antérieure. On compte tout de même 5 juristes n'ayant jamais été DPO ni travaillé au préalable dans l'humanitaire. Et enfin, simplement 3 personnes ont d'abord été ingénieurs ou informaticiens avant de devenir DPO dans l'humanitaire. Cette minorité de profils techniques est peut-être expliquée par une tendance à un recrutement en interne. Pour certains enquêtés, une connaissance de l'humanitaire est un prérequis à la fonction de DPO dans une ONG. D'autres enquêtés pensent surtout qu'il serait difficile de recruter des experts d'autres secteurs, notamment en raison d'une concurrence exercée par le secteur privé : « *Je dirais aussi que dans bien des cas de nombreux experts sont aussi dans le secteur privé. Google,*

*Microsoft, Apple ou Salesforce peuvent se permettre d'employer des experts en sécurité numérique ou en protection des données (…). MSF ou Oxfam sont mises au défi d'agir pareillement, vous savez que vous devez être compétitif, la communauté humanitaire doit faire face à la concurrence pour attirer ces experts dans un contexte de marché, et c'est un challenge permanent.* »[704] Et de manière générale, les ONG manqueraient de personnel, comme nous le déclare un DPO trois ans après l'entrée en vigueur du RGPD : « *On manque de personnel formé, on manque de fonds pour recruter ces personnes, et même quand ces personnes sont en place, c'est compliqué. (…) Nous on a 15 personnes. On est une grosse organisation certes, mais on est 15 personnes et on n'est pas complètement compliant, comme beaucoup de données échappent à une "Full protection", le HCR, il y a un DPO, un juriste et une assistante, ils sont 3, c'est incroyable.* »[705]

« *Ah oui… Oui, oui. Il faudrait plus de moyens ! Enfin, moi toute seule, je suis, je suis pas assez. Enfin, c'est déjà bien. On a dû créer un poste, parce que mon poste n'était pas créé, et donc mon poste c'est une création, pour l'ONG. C'est une ressource qui a dû déjà être négociée, assez difficilement. Mais c'est vrai que pour faire la conformité de l'ensemble de nos missions sur le terrain. Il faudrait être plusieurs. Il faudrait avoir des relais dans les missions, pour être 100 % conformes.* »[706]

Le manque de ressource financière peut également l'expliquer[707], comme le remarque un enquêté : *« Je ne dirai pas qu'il y a plus de fonds, il y a plus de visibilité, les donneurs sont plus conscients qu'il y a plus de besoins, surtout pour les bailleurs européens, il y a une visibilité forte, mais ça ne traduit pas sur des financements, il y a une croyance que même si le bailleur te demande d'être "compliant", tu as déjà fait ça et qu'il n'y a pas besoin de fonds supplémentaires*. »[708]

Ce déficit de moyens se retrouve également en matière de ressources humaines ainsi que de connaissance[709]. Il existe par conséquent un fort besoin de formation pour maitriser les différentes facettes de la protection des données, spécifiquement sur le plan numérique : « *On manque de compréhension des enjeux, les enjeux, ils ne sont pas simplement légaux, ils sont aussi techniques, nommer un DPO n'est pas suffisant, c'est qu'un côté de la pièce, il faut aussi avoir l'autre côté de la pièce, les équipes techniques capables de comprendre les enjeux,*

---

[704] « I do think that the collaboration between the technology sector and the humanitarian sector is necessary to meet the challenge, (…) Microsoft Google, Salesforce and you know all this organisations,so obviously the Silicon Valley organisations are instrumental and fundamental stackeholder in this process, but i would also say that many times many of the experts are also in the private sector, Google, Microsoft, Apple, or Salesforce can afford to hired digital security and data protection experts, in a way that MSF or Oxfam may be challenge to do so, right, you kwnow you have to compete, the humanitarian community has to compete for these experts in the open market, and that an ongoing challenge, you do have to do a partnership. » Entretien n°22, Ingénieur, consultant, 13/03/2020

[705] Entretien n°44, OI2, DPO, 07/03/2021

[706] Entretien n°86, ONG22, DPO, 27/10/2022

[707] CARTONG, « Les données programmes : le nouvel eldorado de la solidarité internationale ? Panorama des pratiques et besoins des OSC francophones »,14/09/2020 https://cartong.org/sites/cartong/files/2020_Etude_CartONG_Les_Donnees_Programmes_OSC_FR.pdf
STEWART, Shanon « Opinion : Information seurity needs to be a priority of international development », *Devex,* 13/01/2021 https://www.devex.com/news/sponsored/opinion-informationsecurity-needs-to-be-a-priority-of-internationaldevelopment-98861
ELLIOT, Vittoria, « Humanitarian organizations keep getting hacked because they can't spend to secure data », *Rest of the world*, 03/02/2022https://restofworld.org/2022/humanitarian-organizations-hack/
« Civil society is under attack. Severe cyber attacks that will cost lives »,*Nethope*, 03/06/2021 https://nethope.org/press-releases/civil-society-is-under-attack-severe-cyber-attacks-that-will-cost-lives/

[708] Entretien n°88, ONG23, DPO, 10/11/2022

[709] « Données programmes : le nouvel eldorado de la solidarité internationale ? Panorama des pratiques et besoins des OSC francophones », CartONG, 2020 https://cartong.org/sites/cartong/files/2020_Etude_CartONG_Les_Donnees_Programmes_OSC_FR.pdf]

*parce que jusque-là, l'équipe IT c'était l'IT vieille école quoi, maintenant les risques ont énormément évolué, et il faut être capable d'avoir dans son organisation des personnes qui sont capables, qui sont capables de comprendre les nouveaux risques, et capables de comprendre et de suivre l'évolution, la rapidité de l'évolution des technologies.* »[710]

Une question de recherche ouverte est relative aux racines et aux causes de ce désinvestissement. La fonction d'agent de compliance est plus généralement décrite comme une position fragile au sein d'institution, comme ont pu le montrer Antoine Vauchez et Caroline Vincensini, les démarches de conformité nécessite un investissement, qui n'est pas toujours facilement justifiable au sein des directions[711]. Concernant l'humanitaire, il est particulièrement difficile de démontrer aux bailleurs l'utilité (le « retour sur investissement ») des fonds destinés à la protection des données et à la cybersécurité. Les bailleurs sont souvent présenté de surcroit comme valorisant les dépenses allant sur le terrain, dédiées à des postes opérationnels. Il serait intéressant de voir si l'on assiste à une évolution allant dans le sens d'une prise de conscience de la nécessité de mieux financer ce sujet chez les bailleurs. On peut simplement à ce stade noter la création fin 2022 d'une bourse fléchée sur la cybersécurité en partenariat entre NetHope et USAID, le bailleur américain[712].

Cela dit, ce phénomène n'est pas spécifique à l'humanitaire. On peut lire par exemple dans un rapport de 2022 publié par l'Agence nationale pour la formation des adultes (AFPA) que « les DPO se sentent souvent en tension par rapport à un manque de moyens. Les réalités sont très différentes entre des DPO disposant de moyens importants en matière de temps, de formation, de budget et de ressources humaines et d'autres DPO arrivant difficilement à investir cette fonction. »[713] Selon des enquêtes de la Commission européenne[714], ou du Comité européen de protection des données (CEPD) a publié début 2024, ce manque de moyens perdurerait : « Même lorsqu'un DPO a été désigné, les enquêtes ont fait état de certaines préoccupations concernant les ressources mises à la disposition de ces agents. (…) Dans certains cas, comme l'indiquent les lignes directrices sur les DPO, il peut même être nécessaire de mettre en place une équipe de DPO, en fonction de la taille et de la structure

[710] Entretien n°44, OI2, DPO, CICR 07/03/2021

[711] "les normes de conformité obligent parfois une entreprise à renoncer à réaliser certaines transactions qui comportent un risque important de non-conformité, réduisant le volume des affaires. Les entreprises n'acceptent donc pas toujours facilement de contraindre leur activité économique au nom de la *compliance*. Marc Lenglet désigne ainsi les responsables de conformité – dont la position n'a rien d'évident – comme des « agents doubles », devant « entretenir d'excellentes relations avec le régulateur tout en accompagnant et en favorisant le business ». Les responsables de conformité ont beau plaider que les coûts financiers et surtout réputationnels d'éventuelles sanctions en cas de non-conformité seraient bien supérieurs aux gains découlant de ces transactions » VAUCHEZ, Antoine, VINCENSINI, Caroline, « Compliance La division public-privé du travail régulateur », In : *Le moment régulateur Naissance d'une contre-culture de gouvernement*, Paris, Presses de Sciences Po. Académique, 2024, p.321-348

[712] BRADLEY, Tony, « Closing the cybersecurity gap for nonprofit », *Forbes*, 27/06/2023 https://www.forbes.com/sites/tonybradley/2023/06/27/closing-the-cybersecurity-gap-for-nonprofits/
« démontrer le retour sur investissement de la sécurité informatique est un défi particulièrement grand pour les organisations dépendant de donateurs qui cherchent à voir un impact concret sur l'utilisation de leur argent autrement que par l'engagement d'un responsable de la sécurité informatique ». SEYDTAGHIA, Anouch, "Le CICR face à la tâche titanesque de protéger ses données numériques », *Le Temps,* 28/06/2024 https://www.letemps.ch/cyber/le-cicr-face-a-la-tache-titanesque-de-proteger-ses-donnees-numeriques

[713] « Evolution de la fonction de délégué à la protection des données », Direction de la prospective Afpa, 2022 https://travail-emploi.gouv.fr/IMG/pdf/synthese_dpo.pdf

[714]communication de la commission au parlement européen et au conseil, Deuxième rapport sur l'application du règlement général sur la protection des données, Bruxelles, le 25.7.2024, COM(2024) 357 final https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=COM:2024:357:FIN

de l'organisation. Malheureusement, ces ressources peuvent ne pas être allouées dans tous les cas. »[715]

En outre, selon une première enquête de 2019 sur les DPO français, plus d'un tiers d'entre eux estiment avoir des difficultés de maitrise du cadre légal, et 53 % estiment que seuls quelques points du RGPD leur échappent. Cela dit, la perception des compétences requises dépend du milieu professionnel : les juristes estiment que le métier de DPO nécessite un niveau de maitrise plus élevé en droit qu'en informatique[716]. Pourtant, le besoin de formation exprimé par les DPO concernerait surtout l'informatique et la cybersécurité. On peut sur ce point se référer à ce tableau tiré d'une enquête de la direction prospective métier de l'AFPA effectuée en 2019[717].

**Les principaux contenu(s) - thématique(s) cités sur lesquels les DPO souhaiteraient pouvoir être formés (plusieurs réponses possibles)**

| | |
|---|---|
| Connaissance dans le domaine de la sécurité informatique (chiffrement, authentification forte, traçabilité, tests de pénétration, attaques Dos, etc.) | 45,8 % |
| Réalisation des premières analyses d'impact | 42 % |
| Connaissance des systèmes d'information (base de données, Cloud, cookies, Machine learning, API, etc.) | 39,7 % |

BESOIN EN FORMATION DES DPO SELON L'ENQUETE DE L'AFPA [718]

De manière plus générale, le manque de compétence et de formation se creuserait avec l'accroissement de nouveaux profils de DPO : « Pour autant, ils restent nombreux à être peu ou pas formés, alors qu'ils proviennent de plus en plus d'environnement hors informatique et juridique. Ils sont également de plus en plus nombreux à exercer cette fonction à temps partiel et de façon assez isolée par rapport aux autres »[719]. Selon une enquête du CEPD publiée début 2024, les DPO ont pu acquérir plus d'expérience professionnelle. Mais l'autorité de protection de données s'inquiète toujours d'un défaut de formation continue mettant en cause la pleine application du cadre réglementaire. Ce dernier est en effet en évolution avec le vote de plusieurs autres textes de loi, comme le Digital service Act, digital markets Act, data governance Act, Artificial intelligence Act, etc. [720].

---

[715] « Even where a DPO was appointed, the surveys raised some concerns as to the resources that were being made available to those officers. (…) In some cases, as noted by the Guidelines on DPOs, it may even be necessary to set up a DPO team, depending on the size and structure of the organisation. Unfortunately, these resources may not be allocated in all cases" EDPB, "Coordinated enforcement action, designation and position of data protection officers", 16/01/2024https://edpb.europa.eu/system/files/2024-01/edpb_report_20240116_cef_dpo_en.pdf

[716] DGEFP, AFPA, « Mettre en œuvre le règlement général sur la protection des Données Comprendre et accompagner les entreprises et les salariés sur les enjeux d'emploi et de compétences », 2019, https://travail-emploi.gouv.fr/IMG/pdf/resultats-enquete-dpd-dpo.2.pdf

[717] AFPA, « Délégué à la protection des données (DPO), une fonction qui se développe, un métier qui se structure », 2020https://travail-emploi.gouv.fr/IMG/pdf/rgpd-metier-dpo-premiers-resultats-072019.pdf

[718] AFPA, ibid.

[719] AFPA, « Évolution de la fonction de délégué à la protection des données », 2022,https://travail-emploi.gouv.fr/IMG/pdf/synthese_dpo.pdf

DGEFP, AFPA, « Mettre en œuvre le règlement général sur la protection des Données Comprendre et accompagner les entreprises et les salariés sur les enjeux d'emploi et de compétences », 2019https://travail-emploi.gouv.fr/IMG/pdf/resultats-enquete-dpd-dpo.2.pdf

[720] DGEFP, AFPA, « Mettre en œuvre le règlement général sur la protection des Données Comprendre et accompagner les entreprises et les salariés sur les enjeux d'emploi et de compétences », 2019 https://edpb.europa.eu/system/files/2024-01/edpb_report_20240116_cef_dpo_en.pdf

Comment remédier à ce problème ? Pour pallier le manque de compétence dans le secteur de la solidarité internationale, une offre spécialisée d'enseignements a été ouverte à destination des DPO travaillant dans l'humanitaire. Cette dernière est organisée par l'Université de Maastricht, en collaboration avec l'ICRC, l'IFRC, OIM et l'UNHCR, l'OCHA. Ajoutons que le CEPD propose une autre solution : s'adresser aux autorités de protection de données. Mais ces dernières n'auraient qu'une connaissance très limitée du secteur humanitaire : « *On y allait… On allait voir la CNIL, on leur a expliqué, tout le monde était dépassé, même la CNIL n'arrivait pas bien à suivre, les débats qu'il y avait au niveau de l'UE n'avaient pas du tout pensé à l'action humanitaire, enfin, c'était vraiment un champ qui était délaissé de toute réflexion, il y avait déjà des craintes, au niveau de Facebook, parce qu'il y avait déjà eu plusieurs scandales, donc tout le monde parlait de protection des données sans trop savoir ce que c'était (…), personne n'avait pensé à l'action humanitaire.* »[721] Cette « absence » de retour des autorités de protection de données est confirmée par plusieurs entretiens auprès de DPO.

Comment alors concilier responsabilisation accrue et manque de moyens ? Une première solution est de mettre l'accent sur la mise en conformité[722] où le contrôle d'autorité est plus probable : « *Ça a déjà été un boulot considérable pour les activités du siège, et pour le terrain. Après on priorise aussi les actions en fonction du risque de sanction… La CNIL peut nous auditer au niveau du siège, mais va difficilement auditer nos missions sur le terrain. Donc on a dû prioriser notre champ d'intervention.* »[723]Et selon certains enquêtés, l'application du RGPD serait limitée au fait de « rassurer » les régulateurs, et donc strictement « formelle »[724], sans travail de fond : « *Parfois on se demande même si la prise de conscience des organisations sur la protection des données est due à l'envie de protéger les données ou à la peur de l'amende, sans voir qu'il existe un enjeu de protection des bénéficiaires*. »[725]

Selon ce dernier témoignage, le travail de conformité peut être motivé en partie par la peur de l'amende, mais on ne dispose pas de données sur le taux de contrôle des autorités de protection des données. Il semblerait d'après certains de nos entretiens que celui-ci serait faible, a priori. À vrai dire, il semblerait que de manière générale les autorités de protection des données ont des ressources inégales, longtemps restées insuffisantes[726]. Et donc, certains DPO semblent attendre que des acteurs — comme des bailleurs — jouent un rôle de contrôle et de contrainte : « *tant que les bailleurs ne bougent pas, ça commence un peu, tant qu'ils vont pas taper sur les ONG, enfin pas taper dessus, mais montrer que c'est un sujet important pour eux, ça ne bougera pas.* » [727] Il est vrai que le bailleur européen, l'European civil protection and humanitarian aid operation (ECHO), inclut dans ses contrats des points relatifs à la

[721] Entretien n°7, OI2, DPO, 11/12/2019
[722] Entretien n° 83, ONG1, DPO, 14/10/2022
[723] Entretien n°84, ONG 22, DPO, 27/10/2022
[724] Entretien n°83, ONG1, DPO, 14/10/2022
[725] Entretien n°44, OI2, DPO, 07/03/2021
[726] "Europe's governments are failing the GDPR", *Brave,* 2020 https://brave.com/static-assets/files/Brave-2020-DPA-Report.pdf
GAVOIS, Sébastien, "La Cnil accusée de ne pas veiller au respect du RGPD", *Next*, 06/02/2024 https://next.ink/126827/la-cnil-accusee-de-ne-pas-remplir-sa-mission-de-veiller-au-respect-du-rgpd/
« Dysfonctionnement systémiques des autorités de protection des données : le cas belge », *la Quadrature du Net,* 08/07/2021 https://www.laquadrature.net/2021/07/08/dysfonctionnements-systemiques-des-autorites-de-protection-des-donnees-le-cas-belge/
« Les GAFAM échappent au RGPD, la CNIL complice », *la Quadrature du Net*, 25/05/2021
https://www.laquadrature.net/2021/05/25/les-gafam-echappent-au-rgpd-avec-la-complicite-de-la-cnil/
[727] Entretien n° 9, ONG3, DPO, 19/12/2019

protection des données. Il faut aussi s'assurer de son effectivité, ce qui semble ne pas être le cas de toutes les clauses des bailleurs : *« Dans les guidelines pour l'"application form", il y avait bien un petit paragraphe sur le RGPD, il fallait que les organisations candidates puissent justifier de la mise en conformité de l'ONG avec le RGPD. J'ai posé la question j'ai demandé ce que ça signifie concrètement, ça veut dire qu'on doit auditer l'organisation ? Comment on peut justifier de ça, la personne que j'ai en face m'a dit, « écoute je ne sais pas trop », la personne que j'avais en face, c'était un gros groupe français de télécom, gros, me dit « écoute je sais pas trop, à mon avis, je vais demander, mais à mon avis tu as juste à certifier sur l'honneur que c'est bon », et effectivement il y a quelqu'un qui a répondu en disant que ça suffirait de certifier sur l'honneur qu'on était en conformité, il y a bien un paragraphe dessus, mais c'est parce qu'il le faut, ils se protègent, c'est du juridique, il n'y a rien à prouver*. »[728]

Cette section nous a permis de rendre compte d'une première limite de l'approche par la compliance. Elle fait en effet peser la responsabilité du contrôle de la mise en œuvre du Règlement en interne, et ce alors que les ONG manquent de ressources, à la fois en matière de finance et de connaissance, et d'autant que la fonction habituelle des autorités de protection des données ne serait pas effective, à la fois en tant que fonction d'accompagnement et de contrôle. Les DPO se retrouvent dans une posture ambiguë : ils manquent de ressources et de compétence, malgré une mise à l'agenda de la protection des données à l'échelle sectorielle, qui s'est traduite par la publication de guidelines et de rapports. Ajoutons que si un bon nombre d'organisations ont publié leur propre politique de protection de données, une part des guides normatifs ont été élaborées par des acteurs disposant d'une forte légitimité symbolique au sein du secteur, comme le CICR ou L'OCHA. Et s'il existe différents espaces d'échanges entre entrepreneurs de cause mettant en avant la nécessité d'une plus grande protection des données, ces espaces seraient restreints aux acteurs dominants du secteur, comme le regrette un DPO : « *le CICR (…) va mettre autour de sa table ses connaissances, ses potes quoi, ça reste restreint je trouve, trop restreint, ça manque, on a ne recherche on galère d'avoir des ONG à la table, on a des meetings ce sont que des acteurs onusiens, le HCR, UNICEF, le mouvement de la croix rouge, on galère d'avoir une ONG opérationnelle, qui est intéressée qui a les moyens de participer à ce type d'étude, on a du mal (…), ça serait super intéressant d'avoir un truc qui ne soit pas les grands qui se réunissent autour de la table, et puis les petits, qui ramassent les miettes et qu'on essaye de construire quelque chose.* » [729]

Mais notre point de vue est resté pour le moment général, on va préciser un peu ce premier tableau. On va décrire plus précisément le travail de « compliance ». Ainsi, on verra que s'assurer du respect du RGPD nécessite d'abord de choisir un prestataire qui ne représente pas de risques grâce à des études d'impact. De surcroit, le responsable de traitement doit s'assurer que le prestataire en question rentre dans une démarche de conformité. L'objectif est alors de garantir la responsabilisation de l'ensemble des acteurs, le responsable de traitement comme les sous-traitants.

[728] Entretien n°28, ONG8, ingénieur,09/04/2020
[729] Entretien n° 44, OI2, DPO, 07/03/2021

## Section 2 — Gestion de risque et « compliance » dans le RGPD

Rappelons que selon la Directive de 1995, un traitement de données doit être notifié à une autorité au préalable. Cette dernière doit ensuite trancher si le traitement représente ou non un risque élevé pour les personnes concernées. Or le considérant 89 du RGPD fait la critique de cette obligation, qui « génère une charge administrative et financière, sans pour autant avoir systématiquement contribué à améliorer la protection des données à caractère personnel. Ces obligations générales de notification sans distinction devraient dès lors être supprimées et remplacées par des procédures et des mécanismes efficaces ciblant plutôt les types d'opérations de traitement susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques, du fait de leur nature, de leur portée, de leur contexte et de leurs finalités. » Le RGPD met en place de tels mécanismes. Il fonctionne en effet selon un modèle de délégation du travail d'évaluation de la menace, comme le remarque Julien Rossi[730]. La chercheuse Karin Favro va dans le même sens : l'approche par les risques s'inscrit dans une démarche de « compliance ». Elle rappelle que selon le règlement, le responsable de traitement doit : « décrire systématiquement le traitement envisagé, sa finalité, de mesurer la nécessité et la proportionnalité des opérations de traitement, mais également d'évaluer les risques pour les droits et libertés des personnes concernées, et les dispositions projetées pour remédier aux risques. Sans cela, le responsable du traitement ne pourra pas rapporter la preuve que son activité est conforme à la réglementation. »[731] Et en conséquence, les études d'impact de risques font partie des documents à communiquer à une autorité pour attester de sa conformité au RGPD.

### § 1 — la notion de risque

Or, souvenons-nous que l'on a commencé à parler d'approche par le risque au sujet de la coalition de cause des groupes industriels, qu'a décrit Julien Rossi. Cette coalition a pu défendre l'idée que seuls les traitements à risque devraient être encadrés. Et donc, selon ce point de vue, le RGPD ne serait pas établi a priori. Au contraire. Il faut examiner au cas par cas les traitements et ne prendre des mesures de protection qu'en cas de risques réels et objectivés. Ce serait évidemment l'entreprise qui fixerait le seuil de risque[732]. Une telle démarche n'a pas été retenue. Le RGPD s'applique pour tous les traitements. Cela dit, de

[730]« La comparaison entre la place du "risque" dans la Directive de 1995 et dans le RGPD est utile pour comprendre la portée de ce qui est désigné, au sujet du RGPD, par le terme de "compliance". Le considérant 54 de la Directive 95/46/CE faisait en effet reposer le calcul de risque sur les épaules de l'autorité de contrôle. Les responsables du traitement avaient l'obligation de lui notifier leurs intentions de collecter et utiliser des données personnelles avant le début des opérations de traitement. (…) Or, désormais, avec le RGPD, c'est aux organismes concernés de déterminer eux-mêmes si l'un de leurs projets de traitements de données à caractère personnel présente un "risque élevé" ou non, et ils peuvent être sanctionnés en cas d'erreur. » ROSSI, Julien, « Protection des données personnelles et droit à la vie privée : enquête sur la notion controversée de "donnée à caractère personnel" » Science politique, Université de Technologie de Compiègne, 2020, tel— 03155480

[731] FAVRO, Karine, « La démarche de *compliance* ou la mise en œuvre d'une approche inversée », *LEGICOM*, 2017/2 (N° 59), p. 21-28. https://www.cairn.info/revue-legicom-2017-2-page-21.htm

[732] ROSSI, Julien, « Protection des données personnelles et droit à la vie privée : enquête sur la notion controversée de "donnée à caractère personnel" » Science politique, Université de Technologie de Compiègne, 2020, tel— 03155480

manière plus générale le droit de la protection des données reste influé par les approches par le risques, et ce bien avant le RGPD[733]. Le Règlement renforce toutefois ces dernière en intégrant l'obligation de mener des études d'impact et d'adopter des technologies incluant dès leur conception la protection des données (une méthode de type « privacy by design »). Et des mesures de protection supplémentaires sont donc requises si les études d'impact objectivent l'existence d'une vulnérabilité.

À ce stade, on doit préciser la définition des études d'impact de risque. Ces dernières sont des outils de connaissance, utilisés afin de circonscrire un risque, permettant d'établir le caractère prédictif d'un événement[734]. Notons qu'il est important de distinguer un risque (prédictible) et une menace (de l'ordre de l'imprévisible)[735]. D'où les questions suivantes : quels sont les outils et méthodologies utilisés pour établir la probabilité d'un événement ? Mais surtout comment et pourquoi dans certains cas ce qui est considéré comme un risque sort-il du champ du prédictible ? Ces questionnements se sont faits particulièrement pressants à partir des années 1980. À la suite d'accidents industriels majeurs (Tchernobyl, Three Miles Island etc.) a émergé un mouvement de contestation, notamment de militant de défense de l'environnement, dénonçant ces catastrophes. Et pour le sociologue Ulrich Beck la fin du XXe siècle correspondrait à l'avènement d'une « société du risque » : le progrès technique devient synonyme de menace[736]. Dans ce contexte, des méthodes de gestion de risque ont été progressivement élaborées pour anticiper un événement grâce à des indicateurs quantitatifs. L'analyse du risque est devenue une politique de management allant de pair avec la production d'un certain type de connaissance et d'outils : critères, audits, études d'impacts, etc. Et certains auteurs rattachent ce type de rationalité aux politiques de « New Management », comme ont pu le décrire Dominique Pécaud[737], ou Béatrice Hibou, liant bureaucratisation et idéologie néolibérale[738].

## §2 — les analyses d'impact relatives à la vie privée

Quant aux études d'impacts, elles proviennent originellement du droit financier, du droit alimentaire et de l'environnement. Elles ont d'abord été utilisées dans les années 1960 et

---

[733] GELLERT, Raphael, "We have Always managed risks in data protection law : understanding the simlarities and différences between the rights-based and the risk-based approach to data protection", Eur. Data Prot. L. Rev. 2016, 2(4), p. 481-492

[734] KERMISCH, Céline, « Vers une définition multidimensionnelle du risque. » *VertigO*, volume 12, number 2, september 2012.

[735] HACKING, Ian, *L'émergence de la Probabilité*, Paris : Seuil, Coll. Liber, 2002, 282 p.

[736] BECK, Ulrich, *La société du risque. Sur la voie d'une autre modernité,* Paris : Flammarion, 2008, 528 p.
BAYA LAFFITE, Nicolas (*et al.)* , « Gouvernement des risques par l'éthique et par les normes : perspectives critiques sur ces dispositifs et leurs évolutions », In: *Bulletin de veille scientifique*, 2011, n° 12, p. 136-142. https://archive-ouverte.unige.ch/unige:156141
LASCOUMES, Pierre, BARTHE,Yannick, CALLON, Michel, *Agir dans un monde incertain. Essai sur la démocratie technique,* Paris : le Seuil, 2001, 368 p.
BOUDIA, Soraya, « La genèse d'un gouvernement par le risque », dans : Dominique Bourg (éd.), *Du risque à la menace. Penser la catastrophe,* Paris : Presses Universitaires de France, 2013, p. 57-76.

[737] PECAUD, Dominique, *Risque et précaution, l'interminable rationalisation du social*, Paris : La dispute, 2005,313 p.
BOUDIA Soraya, DEMORTAIN, David, « Évaluation des risques », dans : HENRY, Emmanuel,(éd.), *Dictionnaire critique de l'expertise. Santé, travail, environnement,* Paris : Presses de Sciences Po, « Références », 2015, p. 133-140.
POWER, Michael , *The Audit Society*, Oxford University Press, 1997, 200p.

[738] Les politiques du new public management vont de pair avec « l'adoption d'un langage « de la rationalité et de l'efficacité, déjà anciennes, mais renouvelées par celui de la gestion, du management, du résultat et du risque, de l'*accountability* et de l'audit » HIBOU, Béatrice, *La bureaucratisation du monde à l'ère néolibérale*, Paris : La Découverte, 2012, p. 123

1970[739]. Puis, elles ont été transposées progressivement parmi les acteurs impliqués dans la protection des données à partir des années 1990 et inscrites dans le droit par l'article 35 du RGPD[740]. La fonction des études d'impact est simple. Si l'on reprend les mots du CEPD, une AIPD est « un processus dont l'objet est de décrire le traitement, d'en estimer la nécessité ainsi que la proportionnalité et d'aider à gérer les risques pour les droits et libertés des personnes physiques liés au traitement de leurs données à caractère personnel, en les évaluant et en déterminant les mesures nécessaires pour y faire face. » Tout ceci confirme qu'une AIPD permet de se conformer aux exigences du RGPD en matière de respect des droits et de démontrer que des mesures appropriées ont été prises. En ce sens, les AIPD s'inscrivent dans la démarche de redevabilité propre au RGPD. La CNIL décrit aussi les études d'impact comme outil de compliance : « Les AIPD sont un outil important au regard du principe de responsabilité, compte tenu de leur utilité pour les responsables du traitement non seulement aux fins du respect des obligations du RGPD, mais également en ce qui concerne leur capacité à démontrer que des mesures appropriées ont été prises pour assurer la conformité au règlement (voir également l'article 24) 5. Autrement dit, une AIPD est un processus qui vise à assurer la conformité aux règles et à pouvoir en apporter la preuve. »[741]Quant à la forme que peut prendre une AIPD, le paragraphe 7 de l'article 35 précise que l'analyse doit au moins contenir : a) une description systématique des opérations de traitement envisagées et des finalités du traitement ; b) une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités ; c) une évaluation des risques pour les droits et libertés des personnes concernées ; d) des mesures envisagées pour faire face aux risques.

Remarquons que si les analyses de menaces en cybersécurité portent sur des intrusions d'acteurs, sur des fuites de données et leur destruction, l'objectif d'une AIPD selon le RGPD est de prévenir les atteintes aux droits et libertés des individus au sens large. Le responsable de traitement doit ainsi inclure dans son analyse de potentielles violations de leur liberté de parole, de pensée, de circulation, de conscience et de religion.

Le G29 établit une ligne de démarcation entre approches par les risques limitées à une démarche de compliance[742], minimisant la protection des droits des personnes concernées :

---

[739]BAYA-LAFFITE, Nicolas, « Black-boxing Sustainable Development: Environmental Impact Assessment on the River Uruguay », In: VOSS, Jan-Peter, FREEMAN, Richard (ed.), *Knowing Governance. The Epistemic Construction of Political Order*, Palgrave Macmillan, 2016, p.237-255, 2016.

[740] WRIGHT, David, DE HERT, Paul (ed.), *Privacy impact assessment*, London : Springer, 2012, 523 p.

[741] 17/FR WP 248 rév. 01 «Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) »2016/679https://www.cnil.fr/sites/cnil/files/atoms/files/wp248_rev.01_fr.pdf

[742] It argued that "the risk-based approach is being increasingly an wrongly presented as an alternative to well-established data protection rights and principles" This requirement to provide for a uniform level of compliance, consistent with the rights-based nature of data protection, has been taken as an argument in favour of a strict separation between compliance issues and risk issues. Namely that full (legal) compliance with the GDPR should always take place, and risk calculations should only come on top of that.

« Le groupe de travail de l'art.29 a affirmé que « l'approche fondée sur les risques est de plus en plus souvent présentée, à tort, comme une alternative aux droits et principes bien établis en matière de protection des données »

Cette exigence d'assurer un niveau uniforme de conformité, cohérent avec la nature de la protection des données fondée sur les droits, a été considérée comme un argument en faveur d'une séparation stricte entre les questions de conformité et les questions de risque. En d'autres termes, le respect intégral (juridique) du GDPR devrait toujours avoir lieu, et les calculs de risque ne devraient venir qu'en sus. « GELLERT, Raphael, " Understanding the notion of risk in the General data protection regulation", Computer law & security review, 2018, N°34/2, p.279-288

GELLERT, Raphael, *The Risk-based approach to data protection,* Oxford University press, 2020, 304 p.

DEMETZOU, Katerina, " GDPR and the Concept of Risk", in : KOSTA, Eleni; PIERSON,Jo;SLAMANIG, Daniel ;FISCHER HUBNER, Simone;KRENN, Stephan, " Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data", 13th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Vienna, Austria, August 20-24, 2018,

« il n'est pas question d'affaiblir les droits des personnes à l'égard de leurs données à caractère personnel. Ces droits doivent être tout aussi forts même si le traitement en question présente un risque relativement "faible". L'extensibilité des obligations juridiques fondées sur le risque concerne plutôt les mécanismes de conformité. Cela signifie qu'un responsable du traitement des données dont le traitement présente un risque relativement faible ne devra peut-être pas faire autant d'efforts pour se conformer à ses obligations légales qu'un responsable du traitement des données dont le traitement présente un risque élevé. »[743]

Cela dit, le Comité européen à la protection des données (CEPD) reconnait que qualifier ce type de préjudice est un exercice difficile : « les risques pour les "droits et libertés" des personnes concernées sont difficiles à appréhender, car il n'y a pas de liens immédiats entre le traitement des données à caractère personnel et l'impact négatif que cela pourrait avoir sur les droits et libertés. Le traitement des données est considéré comme quelque chose d'éthique qui n'a pas d'impact direct sur la vie des personnes concernées, et si cela se produit, ce n'est que dans des cas limités et dans des circonstances exceptionnelles.»[744]

Deuxième remarque, les AIPD ne sont obligatoires que pour les traitements de données personnelles susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes concernées. Cette expression semble a priori floue : comment différencier un traitement représentant un risque « élevé » et un traitement représentant un risque jugé plus « acceptable » ? Le CEPD a publié des lignes directrices donnant quelques précisions. Il est recommandé de mener des AIPD dans le cas de décisions automatisées impliquant un effet juridique ou effet similaire significatif ; des cas de surveillance systématique ; des données sensibles ou données à caractère hautement personnel ; des données personnelles traitées à grande échelle ; des cas de croisement d'ensembles de données ; des données concernant des personnes vulnérables ; des cas d'usage innovant ou application de nouvelles solutions technologiques ou organisationnelles ; des cas d'exclusion du bénéfice d'un droit, d'un service ou contrat. La CNIL ajoute quatre cas nécessitant la conduite d'AIPD : les données biométriques et génétiques, les données de localisation, et des traitements effectués à finalité de surveillance de salariés.

Notons bien au passage que le G29 précise qu'il est recommandé de faire une AIPD dans le cas de technologies « innovantes » : « Le RGPD indique clairement (article 35 [1] et considérants 89 et 91) que l'utilisation d'une nouvelle technologie peut déclencher la nécessité d'effectuer une AIPD. En effet, l'utilisation d'une telle technologie peut impliquer de nouvelles formes de collecte et d'utilisation des données, avec un risque élevé pour les droits et libertés des individus. En effet, les conséquences personnelles et sociales du déploiement

[743] "there is no question of the rights of individuals being weakened in respect of their personal data. Those rights must be just as strong even if the processing in question is relatively 'low risk'. Rather, the scalability of legal obligations based on risk addresses compliance mechanisms. This means that a data controller whose processing is relatively low risk may not have to do as much to comply with its legal obligations as a data controller whose processing is high-risk" Article 29 WP, "statement on the role of a risk-based approach in data protection legal frameworks", 30/05/2014 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf

[744] « the risks towards the "rights and freedoms" of the data subjects is a concept difficult to be grasped, as there is no immediate connection between the processing of personal data and how adversely that could affect rights and freedoms. Data processing is seen as something ethereal that has no direct impact on the lives of the data subjects, and if so happens, it is only limited cases under exceptional circumstances. » EDPS, "Survey on data protection impact assessment under article 39 of the Regulation", case 2020-0066) https://edps.europa.eu/sites/edp/files/publication/20-07-06_edps_dpias_survey_en.pdf

d'une nouvelle technologie peuvent être inconnues. Une AIPD aidera le responsable du traitement des données à comprendre et à traiter ces risques. » [745]

Mais malgré l'existence de lignes directrices du CEPD, les chercheurs s'accordent sur le fait que le RGPD ne détaille pas la façon de caractériser un risque et sa probabilité ainsi que sa gravité. La manière de conduire une AIPD est aussi laissée à la discrétion du DPO et des contrôleurs de traitement. D'où une hétérogénéité des pratiques, en dépit de l'existence de référentiels méthodologiques. Ce flou laisse la porte ouverte à une utilisation purement formelle des AIPD, comme le précise Maxime Darrin : « N'oublions pas que l'AIPD s'insère, par principe, dans des procédures de conformité. En d'autres termes, sa réalisation n'a qu'une finalité probatoire : il s'agit d'une formalité administrative visant à démontrer la conformité de procédures internes à l'organisation concernée, ce qui a pour effet d'écarter l'obligation de publication des AIPD. Par conséquent, des méthodes hétérogènes d'évaluation d'impacts permettent d'offrir un certain blanc-seing à l'usage de technologies, alors même qu'elles sont contestables, tant dans leurs composantes qu'eu égard à la subjectivité d'analyse permise par leur laconisme ou leur opacité. »[746]

Il ressort de cette dernière réflexion la crainte que les opérations de gestion de risque puissent se réduire à un exercice de style, purement formel, servant en fin de compte de blanc-seing à des technologies portant potentiellement atteinte à la vie privée des personnes concernées. Et pour prendre le cas de la CNIL, cette dernière adopte une position d'accompagnement des start-ups afin de soutenir des « innovations responsables ». [747] Mais des associations comme la Quadrature du net lui reprochent de servir de caution éthique pour des projets qu'ils jugent attentatoires au droit à la vie privée. C'est le cas de la vidéo augmentée par exemple[748]. L'association critique l'approche de la CNIL, centrée sur l'évaluation des risques plutôt que sur le principe de nécessité[749].

---

[745] "The GDPR makes it clear ( art 35 (1) and recitals 89 and 91) that the use of a new technology can trigger the need to carry out a DPIA. This is because the use of such technology can involve novel forms of data collection and usage, possibly with a high risk to individual's rights and freedom. Indeed, the personal and social consequences of the deployment of a new technology may be unknown. A DPIA will help the data controller to understand and to treat such risks." Article 29, "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679", 04/04/2017 https://ec.europa.eu/newsroom/article29/items/611236/en

[746]DARRIN, Maxime, De MARCO, Estelle, KELLER, Jonhathan, ROSSI, Julien, « Sur les évaluations d'impact dans les politiques numériques », *La Revue européenne des médias et du numérique*, n° 64, Hiver 2022-2023 https://la-rem.eu/2023/06/sur-les-evaluations-dimpact-dans-les-politiques-numeriques/

[747] DENIS, Marie-Laure, « Innovation et protection de la vie privée : 45 ans d'histoire commune », *Servir*, 2023/1 (N° 519), p. 41-43. https://www.cairn.info/revue-servir-2023-1-page-41.htm

[748]« Caméras dites « augmentées » dans les espaces publics: la position de la CNIL », CNIL, 19/07/2022 https://www.cnil.fr/fr/cameras-dites-augmentees-dans-les-espaces-publics-la-position-de-la-cnil

« Le prétendu « encadrement » des dispositifs promis par la CNIL permettrait aux entreprises de la Technopolice d'utiliser les espaces publics et les personnes qui les traversent ou y vivent comme des « données sur pattes. » »Qu'est ce que la videosurveillance algorithmique », La Quadrature du net, 22/03/2022
https://www.laquadrature.net/2022/03/23/quest-ce-que-la-videosurveillance-algorithmique/

[749] La Quadrature du Net, "S'opposer à la vidéosurveillance automatisée", 11/03/2022 https://www.laquadrature.net/wp-content/uploads/sites/8/2022/03/Reponse-consultation-CNIL.pdf

LEVALLOIS-BARTH, Claire, KELLER, Jonathan, « Analyse d'impact relative à la protection des données: le cas des voitures connectées », Institut Mines-Telecom, Telecom Paris, 2021, https://cvpip.wp.imt.fr/files/2021/11/FINALRapportRechercheC3S_AIPD_VoituresConnectees_nov2021.pdf

Notons pour clore ce passage que plus généralement, d'autres modalités de régulation du risque existent, comme le principe de précaution[750]. Ce dernier est un principe général du droit de l'environnement, et l'on ne le retrouve pas dans le droit de la protection des données. On lui a reproché d'être délétère pour l'innovation[751]. Mais plusieurs acteurs, comme par exemple le comité d'éthique du CNRS, ont exhorté les industriels à l'appliquer au domaine numérique[752]. Et le juriste Raphaël Gellert conseille de s'y référer pour mener des évaluations de risque autres que des méthodes purement gestionnaires. Adopter le principe de précaution permettrait de mieux prendre en compte l'incertitude et « au lieu de gérer les risques, c'est-à-dire de rechercher le niveau de risque acceptable, "elle vise tout simplement à les éviter. » Et pour Raphaël Geller une approche précautionneuse nécessiterait de ne plus se contenter de méthodologies quantitatives et éprouvées et admettre que l'état d'un savoir ne permet pas de trancher dans l'immédiat sur l'adoption ou non d'une technologie.

### § 3 — les analyses d'impact relatives à la vie privée dans l'humanitaire

Les ONG traitent des données potentiellement sensibles de personnes qualifiées de vulnérables. Il parait logique de penser qu'elles sont amenées à réaliser des AIPD de façon régulière. D'ailleurs, l'exercice n'est pas dans l'absolu pour elles totalement nouveau. Il se trouve que les humanitaires ont une pratique éprouvée de la gestion de risque. Tout d'abord, à la suite des nombreuses attaques touchant le secteur, a dû être prise en compte la sécurité des travailleurs de la solidarité internationale. D'où une professionnalisation de la gestion de risque, et le développement d'outil d'analyse d'accidents sécuritaires, visant à anticiper leur occurrence [753] . En outre, certaines ONG, comme l'IFRC, se sont engagées dans des programmes de réduction du risque de catastrophe qui va de pair avec une série de dispositifs comme des systèmes d'alertes précoces et des IA dont la finalité est la prévision de l'advenue d'inondations, de tremblement de terre ou de cyclones[754].

Cependant, l'analyse des risques relatifs à la protection des données est nettement moins professionnalisée. De manière générale, la conception d'une AIPD est, d'après les entretiens

---

[750] BOURG, Dominique, SCHLEGEL, Jean Louis, *Parer aux risques de demain, le principe de précaution*, Paris : éditions du Seuil, 2001
GODARD, Olivier, « De l'usage du principe de précaution en univers controversé : entre débats publics et expertise », *Futuribles*, 1999, p. 37-60

[751] GRUMBACH, Stéphane, « Vers un principe de précaution numérique? » *Le Monde*,15/04/2013 https://www.lemonde.fr/idees/article/2013/04/15/vers-un-principe-de-precaution-numerique_3160109_3232.html

[752] DEPRIECK, Matthieu, FORTEZA, Paula, « Je propose d'instaurer un principe de précaution numérique », *L'Opinion*, 21/04/2020, https://www.lopinion.fr/politique/paula-forteza-je-propose-dinstaurer-un-principe-de-precaution-numerique
Comité d'éthique du CNRS, « Science, Risques et principede précaution », Avis n° 2021-41, https://comite-ethique.cnrs.fr/wp-content/uploads/2021/05/Avis-2021-41.pdf

[753] TAITHE, B, " Danger, Risk, Security and Protection: Concepts at the Heart of the History of Humanitarian Aid.", In: NEUMAN, M, WEISSMAN, F, (ed.), *Saving Lives and Staying Alive: the professionalisation of humanitarian securit*y. London: Hurst Publishers. 2016. p. 37-53
MARTY, Louise, « Manager les risques. La professionnalisation de la sécurité au sein des ONG », Mémoire de Master, Université Paris 1, Science politique, 2016. ⟨dumas-01560374⟩
BEERLI, Monique, "Saving the Saviors: An International Political Sociology of the Professionalization of Humanitarian Security", Thèse, Institut d'étude politique de Paris, Université de Genève, Sciences Politiques, Didier Bigo dir, Marco Giugni, 2017. https://www.theses.fr/2017IEPP0033

[754] BENBOUZID, Bilel, CARDON, Dominique, « Machines à prédire », *Réseaux*, 2018/5 (n° 211), p. 9-33. https://www.cairn.info/revue-reseaux-2018-5-page-9.htm
REVET, Sandrine, *Les coulisses du monde des catastrophes « naturelles ».* Paris : Éditions de la Maison des sciences de l'homme, 2018, 240 p.

avec des DPO, encore à affiner : « *La difficulté c'est que ça reste subjectif, on a peu de littérature claire qui permet d'identifier un niveau de risque de manière concrète, c'est une réflexion interne, propre à chaque organisation, c'est assez complexe de déterminer ce qui est un risque élevé, ou non. Nous ce qu'on aimerait, c'est avoir une matrice concrète et presque didactique, où on insère les éléments et ça va nous indiquer tout de suite si le risque est élevé ou pas, mais à chaque fois c'est une longue discussion pour établir le niveau de risque.* »[755]

Il existe cependant quelques guides mentionnant des pistes pour mener des AIPD dans l'humanitaire. Privacy International en collaboration avec le CICR, OCHA et UN Global Pulse a publié une note sur les études d'impact dans l'humanitaire[756]. Le document donne de premières indications pour conduire ce type d'étude et fait référence à plusieurs modèles d'AIPD : celui du CICR, de l'IFRC et de l'UN Global Pulse[757].

Sans surprise, les modèles d'AIPD varient selon les organisations. Ainsi Mercy Corps recommande de mener ce type d'étude dès qu'il est question de traiter des données personnelles : « Une évaluation relative à la vie privée est nécessaire chaque fois qu'un nouveau programme, un nouveau projet ou une nouvelle technologie implique la collecte ou l'utilisation de données personnelles ou sensibles. »[758] Son exemple d'analyse d'impact prend la forme d'un tableau à plusieurs entrées. Une première entrée concerne la nature des données : il est donc requis de spécifier le type de données collectées, leur qualité, leur finalité d'usage, leur modalité de stockage. L'évaluateur doit aussi s'assurer du respect du principe de minimisation et de la transparence du traitement. Une deuxième entrée est relative aux risques informationnels. Le responsable de traitement doit préciser la possibilité d'un dommage individuel ou organisationnel découlant d'une re-identification. La conformité du traitement au RGPD doit être documentée. Le tableau doit indiquer la base légale utilisée, la possibilité de retrait du consentement et la prise en compte des réponses aux demandes des personnes concernées. Autre point, les mesures de sécurité doivent aussi figurer dans l'AIPD, comme l'existence d'un entrainement du personnel et la possibilité de contrôler l'accès aux données. Notons enfin que le tableau comprend cinq cases permettant d'évaluer le degré de probabilité d'un risque. Il suffit d'y répondre positivement ou négativement, ou bien reconnaitre qu'il n'est pas envisageable de se déterminer sur ce point. Une dernière colonne concerne les mesures d'atténuation de risque à prendre.

Le modèle d'AIPD du CICR comprend 10 catégories : 1) Base légale (consentement ou autre) ; 2) finalité de traitement ; 3) principe de minimisation ; 5) qualité des données ; 6) durée de conservation des données ; 7) partage de données ; 8) mesures de sécurité ; 9) droits des individus ; 10) mesure de redevabilité auprès des personnes. L'AIDP évite l'effet « case à cocher ». Chacune de ces 10 catégories inclut une série de sous questions-posées de manière à obtenir des réponses qualitatives.

---

[755] Entretien n°88, ONG24, DPO, 15/11/2022

[756] Privacy International, "Assessing data management activities in the humanitarian sector : a guidance note", 27/ 07/2020 https://privacyinternational.org/news-analysis/4108/assessing-data-management-activities-humanitarian-sector-guidance-note

[757] "Guidance note series data responsibility in humanitarian action, Note #5 : data impact assessment" Privacy International, Humanitarian Data Centre, ICRC, https://privacyinternational.org/sites/default/files/2020-07/guidance_note_data_impact_assessments.pdf

[758]"A PIA is required anytime a new program, project, or technology involves the collection or use of personal or sensitive data." GITHUB, Mercy Corps, Data protection tools, https://github.com/mercycorps/DPP-guides/tree/main/Privacy-impact-assessment

Les différentes situations mentionnées par le CICR pouvant faire l'objet d'une AIPD reprennent dans les grandes lignes les recommandations des autorités de protection des données [759]. Trois cas de figure sont ajoutés par l'organisation humanitaire : l'utilisation de moyens de communication intrusifs, comme des textos, pour contacter des bénéficiaires ; la possibilité d'accès à des données de l'organisation par des gouvernements ; le partage de données entre organisations impliquées dans un programme d'aide humanitaire. Il existe d'autres divergences entre l'AIPD du CICR et de la CNIL. Concernant les risques de sécurité par exemple, le tableau de la CNIL ne précise tout d'abord pas leur nature (hacking, fuite humaine, etc.). Il se concentre plutôt sur le fait d'avoir pris ou non une série de mesures de prévention : chiffrement, cloisonnement des systèmes d'information, contrôle des logiciels malveillants. Ensuite, une analyse synthétique des risques doit être rédigée en prenant en compte trois facteurs : accès, modification, disparition. Leur nature, leur probabilité et leur impact doivent être spécifiés. Quant à l'AIPD du CICR, elle doit comprendre d'abord une description plus précise et qualitative du type des risques. Ces derniers sont évidemment liés aux situations humanitaires (conflits, personnes vulnérables, lois imposant l'accès à des données par des États). Autre particularité : en matière de risques réputationnels, le CICR est spécialement attaché aux principes humanitaires de neutralité, d'impartialité et d'indépendance. Leur atteinte entache selon l'organisation la confiance que les individus placent dans le CICR et remet donc en cause l'exercice de son mandat. Enfin, l'AIPD du CICR ne comprend pas de colonnes correspondant à l'évaluation quantitative et systématique du risque, à son degré de probabilité ou de gravité.

En revanche, pour l'organisme onusien Global Pulse l'estimation des dommages doit être à la fois qualitative et quantitative. La sévérité d'un dommage doit être d'abord décrite de façon qualitative. Il est rappelé que l'importance qu'on accorde à une atteinte à la vie privée dépend de facteurs socioculturels. L'ampleur d'un dommage doit être quant à elle calculée quantitativement grâce à un score allant d'un à sept. L'évaluateur doit ensuite déterminer en pourcentage le degré de probabilité d'occurrence du dommage (et non du risque), sachant que le document ne comprend pas de méthodologie pour calculer ce dernier[760].

Enfin, l'unité 510 de la croix rouge néerlandaise recommande d'inclure les AIPD dans un cycle plus global d'évaluation et de cartographie des usages numériques. Il est recommandé de commencer par effectuer une cartographie des technologies utilisées ainsi que des flux de données, puis de conduire l'analyse de risque à proprement parler, en essayant d'apprécier leur probabilité et le degré de sévérité et d'impact. Cette analyse doit être accompagnée d'un inventaire des mesures de protection et d'atténuations de risque. Dans un second temps, il est recommandé de procéder à l'estimation de la qualité des données (leur exactitude, leur complétude et leur pertinence). Enfin, l'évaluation doit comprendre une analyse de l'efficacité

[759] Le CICR préconise de réaliser une DPIA pour des données sensibles, des données concernant des personnes vulnérables, lors des traitements à grande échelle de données biométrique, pour des opérations de profiling, des décisions fondées sur un "traitement de donnée automatique", pour des technologies intrusives ou particulièrement sujettes à des failles (cloud, réseaux sociaux, géolocalisation, biométrie), la possibilité que des données puissent être accessibles pour des autorité, le fait d'avoir un impact négatif sur les individus, la possibilité que le CICR contacte des individus de façon intrusive ( SMS), la mise en place de système de surveillance, l'ouverture d'une nouvelle base de données, centralisant deux systèmes d'information séparés, ce qui peut conduire à un risque de réidentification ; utilisation de nouvelles finalités, plus intrusive, l'utilisation d'un nouveau système de gestion de données, un partage de données entre deux organisations.

[760] "Risks, Harms and Benefits Assessment Tool", UNGlobal Pulse, https://www.unglobalpulse.org/document/risks-harms-and-benefits-assessment-tool/

du traitement de données (rapidité de la gestion d'information, et balance entre la qualité des données et le coût relatif à leur collecte).

Le modèle d'analyse d'impact de risque en tant que tel comprend différents items à remplir : la nature du risque, la description de l'incidence (financier, réputationnel, ayant une incidence sur la vie des personnes). Une colonne est consacrée au degré de probabilité d'un risque, qui est évalué selon une échelle à trois niveaux : faible, moyen, élevé. Le niveau de risque doit être ensuite calculé en multipliant son degré de probabilité par le score d'impact. Enfin, une dernière colonne doit spécifier les mesures d'atténuation de risque à prendre. La complexité du modèle d'AIDP de l'unité 510 est peut-être due au fait que l'organisation s'est spécialisée dans des programmes de « réduction de risque de catastrophe » et développe des outils d'anticipation à partir d'IA. L'organisation possède une expertise en matière d'analyse de risque et propose un modèle holistique d'AIPD. Ainsi, l'étude d'impact doit prendre en compte 13 différents types de risque : (1) risques criminels, vol de données, hacking ; (2) risques relevant de facteur humain (conflits, grèves, censure) ; (3) risques liés à un endommagement d'infrastructure (coupure de courant, interruption des réseaux de communication, etc.) ; (4) risques causés par des catastrophes naturelles, pouvant affecter les services humanitaires ; (5) risques associés à une organisation tierce (fuite de données sur un serveur d'un sous-traitant) ; (6) risque réputationnel ; (7) risques dus à l'effet mosaïque, soit la réidentification et l'exposition d'individus résultant d'un croisement de base de données ; (8) risques découlant d'une mauvaise interprétation des données ; (9) risques venant d'un stockage décentralisé, concernant l'efficacité du traitement de données ; (10) risques provenant d'un manque de transparence (risque lié à des modèles de prédiction comprenant des biais ou à des données de mauvaise qualité) ; (11) risques associés à la révélation de données sensibles (informations ethniques, religieuses, géographiques, avérant des conflits entre les communautés) ; (12) risques dus à un manque de littératie numérique ; (13) risques industriels.

Ce modèle se veut exhaustif et inclut donc une gamme complète de risques. Les chercheurs Julia Zomignani Barboza et Paul De Hert proposent également un modèle d'AIPD holistique. La situation complexe des bénéficiaires (affectés par des conflits, des discriminations ethniques ou religieuses), fait que les AIPD ne devraient pas se limiter à l'évaluation de risque de violation du droit à la vie privée. Ces dernières devraient d'après eux inclure des éléments culturels et politiques[761]. Ainsi, certains DPO conseillent de ne pas se limiter à des descriptions techniques d'un traitement de données et d'inclure les perceptions des personnes concernées. Il serait nécessaire de concevoir des DPIA de façon plus inclusives : « *Nous, on peut les informer de certains risques, on va être au courant de certains risques, des data flow, des providers impliqués, et eux vont nous dire qu'il y a un autre risque et que si on partage nos données, pour une raison X ou Y c'est risqué, parce que chez nous il y a un groupe armé encore peu identifié qui agit contre notre minorité, c'est un risque qu'on n'a pas vu venir et il y a que les communautés qui pouvaient nous l'apprendre, parce que nous on est focalisé sur les risques*

[761]"Considering the possibly vulnerable situation in which migrants using these tools may find themselves, as well as the fact that ICT tools for integration are likely to interact with many of the above listed rights, it is only logical to extend the scope of the assessment to the reality, the concerns, and v needs of migrants and not limit it to an assessment of compliance with data protection rules."ZOMIGNANI BARBOZA, J., DE HERT, P. "Data Protection Impact Assessment : A Protection Tool for Migrants Using ICT Solutions.", *Social Sciences*, 10(12), 2021

*qu'on connait, sans prendre en compte les risques sur place, c'est pour ça qu'il est nécessaire d'aller sur place, et je pense que la communication doit être dans les deux sens, quand on informe les bénéficiaires des risques éventuels liés à la collecte des données, il faut aussi les entendre, et je pense que c'est pas fait encore, à une échelle importante*. *Ils savent ce qu'ils vivent, ils savent ce qu'ils encourent, nous, on a une vision partielle.* »[762]

Mais la mise en œuvre d'AIPD très détaillées nécessite des ressources financières et temporelles dont les ONG ne disposent pas systématiquement. Lors de nos entretiens, il nous a semblé que les ONG tentent au contraire d'alléger ce type d'étude d'impact. En effet, en raison du contexte sensible des crises humanitaires, il peut être très souvent requis d'en faire, soit une nécessité qu'il est souvent difficile de respecter : « *Si la question est de savoir si le traitement peut être à risque pour les droits fondamentaux, la réponse est toujours oui, donc on a tendance à faire plus souvent des DPIA, même si là aussi dans les faits on va appeler nos collègues pour leur dire qu'on va faire un DPIA presque tout le temps, mais dans les faits ça va pas être tout le temps un vrai DPIA, c'est-à-dire qu'on va pas toujours aller vers un DPIA complet*. » [763]

Ajoutons que le nombre conséquent d'AIPD à mener est aussi dû au caractère décentralisé de certaines organisations humanitaires. La fragmentation de leur système d'information complique leur cartographie et la possibilité de mener des analyses d'impact exhaustives : « *On souffre de ne pas avoir de solution tout à fait globale par rapport à d'autres organisations qui ont des systèmes d'enregistrement des bénéficiaires absolument centralisé, et, quel que soit le contexte, ils pourront avoir des modalités pour prendre pour collecter des données (…). Nous, on n'a pas vraiment ça, on a une certaine hétérogénéité dans nos systèmes pour gérer les bénéficiaires et à chaque fois on va faire un assessment du contexte et des risques.* »[764] Par voie de conséquence, certaines ONG choisissent de laisser les délégations locales se charger des AIPD, même si ces dernières n'ont pas toujours les compétences requises[765]. D'autres organisations tentent de simplifier leur système d'information : « *ce qu'on essaye de faire, c'est vraiment déjà de limiter le nombre d'outils utilisés, par exemple, au début, y avait énormément d'unités différentes, que ce soit la santé, ou la protection, qui commençaient toutes à utiliser des outils différents, on leur a dit, attendez, c'est trop compliqué, bah déjà nous on a une responsabilité, on doit en théorie savoir tout ce qui se passe en termes d'opérations, de traitement de données personnelles, donc ça devient compliqué quand on a 15 serveurs quand on a 15 opérations, providers, etc.*. » [766]

Une autre solution de simplification est d'en créer des versions allégées et adaptées au terrain. Ces dernières sont plus courtes et souples. Elles peuvent être utilisées en cas d'urgence et de contexte volatil dans le cadre de missions opérationnelles : « *Un data privacy impactment c'est bien c'est sympa, bon il faut le faire j'avoue de mettre ça entre les mains de quelqu'un sur*

[762] Entretien n°44, OI2, DPO, 07/03/2021
[763] Entretien n°93, OI2, DPO, 02/06/2023
[764] Entretien n°88, ONG24, DPO, 15/11/2022
[765] « Decentralised systems place responsibility for enacting DPIAs, or applying tool guidance, in the hands of programme officers who are frequently insufficiently equipped with the necessary technical literacy and resources. » The Engine Room, "Biometrics in the humanitarian sector, a current look at risks, benefits and organisational policies", July 2023 https://www.theengineroom.org/wp-content/uploads/2023/07/TER-Biometrics-Humanitarian-Sector.pdf
[766] Entretien n°7, OI2, DPO, 11/12/2019

*le terrain, c'est pas envisageable, il faut le rendre plus accessible, le vulgariser, s'assurer que des outils soient mis en place sur le terrain.* »[767]Ces AIPD devraient être réalisées de façon plus informelle, et sans en référer nécessairement au DPO, sauf en cas de doute [768]. Elles sont validées par le chef de mission de l'antenne: « *On en a des courts, adaptés au terrain, ce sont des listes de questions courtes à faire en fonction du contexte ; lors d'une ouverture d'une délégation en fonction du risque qu'elle soit proche ou non d'une zone de conflit. Ou en fonction de type de données, il faut beaucoup de bon sens, c'est selon le contexte.* » [769] On peut en quelque sorte dire, si on se réfère à Michel Callon ou à Pierre Lascoumes, qu'il s'agit d'acclimater des outils à un environnement particulier[770].

Une version courte reprend donc la structure globale d'une AIPD et doit comprendre une présentation minimale de la base légale utilisée, l'exposé du flux de données (type de données collectées, finalité d'usage, mode de stockage, etc.). Une évaluation des risques doit être menée (sa nature plus précise n'est pas décrite), des dommages potentiels doivent être mentionnés, et l'AIPD doit comprendre enfin des mesures à envisager pour les atténuer. Le modèle d'AIPD court du CICR laisse donc plus de latitude et reste nettement moins détaillé que sa version longue, même si l'on retrouve les grandes lignes.

La réalisation d'AIPD est de caractère facultatif. L'organisation ne contrôle pas leur usage : « *le (nom de l'organisation) avait une approche flexible, en théorie vous devrez faire un DPIA tout le temps, on vous accompagne si vous voulez, maintenant on ne va pas vous forcer, maintenant je pense qu'il y a beaucoup plus de personnes qui ont décidé de le faire, là où avant ils refusaient de le faire.* »[771] Il s'agit ici moins d'outil de redevabilité que d'aide à la décision. Une autre DPO ne croit pas à l'utilité d'une démarche incitative et facultative et propose de contractualiser leur usage : « *Les études d'impacts peuvent être imposées pour l'ensemble de nos programmes. Pour l'instant, ce n'est pas le cas. Mais j'aimerais qu'à l'avenir, ça le soit, que ce soit une obligation contractuelle de mener une étude d'impact. Donc ça peut venir de bailleurs, de partenaires, et de toute partie qui a la possibilité de nous imposer des études d'impacts*. » [772] Cette DPO s'interroge néanmoins sur la capacité de membres opérationnels à effectuer des AIPD, alors que leur connaissance de la nature des risques numériques peut être encore faible. « *Mais je pense que cette étude d'impact, il va falloir les mener, et les mener sur le terrain, ça va être assez compliqué, parce que ça demande des ressources et ça demande du temps, à la fois en ressources humaines et en compétences, donc il y a tout un volet de formation et de sensibilisation, parce qu'actuellement ce n'est pas mené, sauf quand on a une obligation de la part d'un bailleur de faire une étude des risques*. »[773] Ce point est d'autant plus crucial que le CICR indique qu'il est nécessaire de conduire des AIDP plus longues au moins dans trois cas de figure : lorsqu'une nouvelle technologie est utilisée ; dans le cas où les données sont particulièrement sensibles ; ou en cas de transfert de données (à des sous-

[767] Entretien n°9, ONG3, DPO, 19/12/2019
[768] Entretien n°84, ONG20, DPO, 14/10/2022
[769] Entretien n°7, OI2, DPO, 11/12/2019
[770] LASCOUMES Pierre, « Traduction », dans :BOUSSAGUET, Laurie, (éd.), *Dictionnaire des politiques publiques. 4e édition précédée d'un nouvel avant-propos.* Paris, Presses de Sciences Po, « Références », 2014, p. 632-640.
[771] Entretien n°91, OI2, DPO, 26/05/2023
[772] Entretien n° 86, ONG22, DPO,27/10/2022
[773] Entretien n°86, ONG22, DPO, 27/10/2022

traitants techniques, à d'autres organisations). En cas d'usage de technologies impliquant un risque d'intrusion (comme le cloud), le CICR conseille d'avoir recours à un consultant externe, doté d'une meilleure expertise. Cependant, le coût de ce type de prestation peut être assez conséquent. Et surtout, il est parfois difficile de trouver des personnes spécialisées sur ce genre d'opération ayant une connaissance du contexte humanitaire : « *Solidarités international a tenté de faire un appel d'offres pour une AIPD en Syrie, ils n'ont eu aucune offre valable. Ils ont eu aucune réponse du privé.* »[774]

Enfin, l'impact des AIPD est une question ouverte. Sont-elles prises en compte dans l'usage de tel ou tel outil ? Permettent-elles d'encadrer l'utilisation expérimentale de certaines technologies ? Certains DPO nous ont assuré que des dispositifs n'avaient pas été adoptés à la suite de DPIA. Sachant que ces dernières doivent être menées en amont pour éviter les coûts associés à un changement de modalité de traitement : « *On essaye d'identifier en amont… on essaye d'identifier ce qui n'est pas privacy by desing, et les prendre en compte. Cela permet d'éviter de changer d'outils, ça couterait trop cher*. »[775] Nous n'avons pas d'autres témoignages sur ce sujet dans nos entretiens. Mentionnons simplement le fait que dans un rapport d'Engine Room, on peut lire que leur technicité fait qu'elles peuvent être réduites à des procédures formelles, remplies de façon routinisées sans être prise en compte au niveau opérationnel[776]. Toujours est-il que le chercheur Aaron Martin fait le constat qu' "il existe peu d'exemples *publics* d'organisations humanitaires qui ont décidé de ne pas conclure un partenariat technologique ou de données à la suite d'une évaluation des risques ou d'une diligence raisonnable, ou qui ont mis fin à un tel partenariat à la suite d'une réaction de la société civile ou de préoccupations émergentes liées à des pratiques de surveillance nuisibles ou à des pratiques de blanchiment d'aide de la part des fournisseurs de technologie.»[777]

Pour conclure, les DPO n'incarneraient pas encore, pour les différentes autorités de protection de données, une posture d'expertise vis-à-vis des risques numériques, du fait d'un manque de ressources et de formation. Dans le même temps, les autorités de protection de données n'alloueraient pas suffisamment de ressources (notamment en matière de connaissance) pour les DPO humanitaires. Nos entretiens avec des DPO d'ONG confirment en partie ces difficultés, et s'ils revendiquent une plus grande conscience des risques numériques, les méthodologies de gestion de risque sont encore embryonnaires. Les DPO tentent malgré tout de construire des outils adaptés au terrain humanitaire. Il semblerait que les modèles holistiques d'AIPD sont difficilement mis en œuvre. Il est alors nécessaire de trouver un équilibre entre le fait qu'une AIPD soit suffisamment détaillée pour documenter les risques et ne pas se limiter à un

[774] Entretien n°9, ONG3, DPO, 19/12/2019
[775] Entretien n°17, ONG6, DPO, 31/01/2020
[776]"Étant donné que les DPIA sont des documents hautement techniques, ce manque de capacité institutionnelle limite actuellement la mesure dans laquelle ils peuvent être utilisés efficacement. Il y a un risque que les DPIA deviennent simplement une procédure - une paperasse que l'on remplit régulièrement sans influencer ou façonner de manière significative le déploiement des opérations technologiques." "Given that DPIAs are highly technical documents, this lack of institutional capacity currently limits the extent to which they can be effectively used. There is a risk that DPIAs will merely become procedural – a piece of paperwork that is routinely filled out without meaningfully influencing or shaping the rollout of technological operations."The Engine Room, "Biometrics in the humanitarian sector, a current look at risks, benefits and organisational policies", July 2023 https://www.theengineroom.org/wp-content/uploads/2023/07/TER-Biometrics-Humanitarian-Sector.pdf
[777]« there are scant public examples of humanitarian organizations deciding against a proposed data or technology partnership following a due diligence or risk assessment or discontinuing such a partnership following civil society pushback or emergent concerns related to harmful surveillance practices or aidwashing by technology vendors." MARTIN, Aaron, "Aidwashing surveillance : critiquing the corporate exploitation of humanitarian crises", *Surveillance & society*, 21 (1), 2023, p.96-102

exercice formel, mais tout en pouvant être mobilisée dans des contextes de crises et lors de situations d'urgence.

## Section 3 — Gestion de risque et sous-traitance

Conjointement à ce travail d'évaluation de risque d'un outil technique, il est aussi nécessaire de s'assurer du respect du RGPD par un prestataire en nouant une relation contractuelle entre responsable de traitement et sous-traitant[778]. Indiquons simplement que l'article 28 du RGPD stipule qu'un contrat est à inclure dans le dossier à fournir aux autorités en cas de contrôle puisqu'il permet de s'assurer que les différentes parties prenantes respectent le RGPD. La signature de ce dernier rentre par conséquent dans une logique de « compliance », comme le fait remarquer le juriste Loïc Brehin, qui indique également que « plus que permettre la conformité à une norme supérieure, le contrat peut contribuer à l'établissement et à la diffusion d'une norme. En lien avec la logique d'« accountability » prévaut une « démarche de corégulation » : les responsables et sous-traitants sont invités à définir eux-mêmes les mesures de mise en conformité qu'ils estiment les plus adaptées à leur situation et à en assurer le respect, en leur sein et dans le cadre de leurs relations contractuelles. Cette démarche s'inscrit dans le cadre plus large du « développement de […] normes de droit souple, caractéristique de la compliance. » [779] Il existe une certaine de latitude dans la forme que peut prendre ce contrat. Mais l'article 28 indique qu'il doit être mentionné, au minimum, que le sous-traitant ne traite les données personnelles que sur instruction du responsable de traitement ; qu'il s'assure que les personnes autorisées à traiter des données à caractère personnel s'engagent à en respecter la confidentialité ; qu'il s'assure de la sécurité des données des personnes concernées[780], aide le responsable du traitement à s'acquitter des demandes de droit d'accès aux données ; supprime les données personnelles à la fin de la relation de prestation (à moins que le droit de l'UE n'exige la conservation des données personnelles)[781]. Et surtout pour assurer un standard commun de protection, le 4 juin 2021, la Commission européenne a publié des clauses contractuelles types entre les responsables de traitement et les sous-traitants. Cependant, précisons que leur utilisation n'est obligatoire que pour les transferts de données à l'international. Il est recommandé de les employer pour des sous-traitants européens, mais cela reste facultatif. D'où de moindres contraintes pour les prestataires européens : « *dans le cadre de la sous-traitance la seule obligation c'est qu'on respecte l'article 28.3*[782] *du coup on a pas une exigence telle comme ceux qui encadrent les*

---

[778] MENDOZA-CAMINADE, Alexandra. *Le rôle du sous-traitant en matière de données personnelles* In : TISSEYRE, Sandrine (dir.). *Sécuriser la sous-traitance : quels nouveaux défis ?,* Toulouse : Presses de l'Université Toulouse Capitole, 2019, https://books.openedition.org/putc/7022?lang=fr

[779] BREHIN, Loïc, « Contrat et protection des données personnelles, étude des articles 26, 28 et 46 du RGPD », Mémoire de recherche, droit privé général, 2020, université Paris II-Assas

[780] Le RGPD stipule qu'un sous-traitant doit respecter l'art 32 qui précise que le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque).

[781]« Sous-traitance, exemple de clauses », CNIL, 04/10/2017 https://www.cnil.fr/fr/sous-traitance-exemple-de-clauses

[782] L'article 28.3 du RGPD stipule que : « Le traitement par un sous-traitant est régi par un contrat ou un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre, qui lie le sous-traitant à l'égard du responsable du traitement, définit l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, et les obligations et les droits du responsable du traitement. »

*transferts hors UE*. »[783] Certains DPO font le choix de les imposer malgré tout : « *les clauses contractuelles ne reprennent pas toujours les éléments contractuels obligatoires cités par le RGPD, j'ai vu très peu de prestataires utiliser les clauses types de la Commission européenne qui datent de plus d'un an, moi je les impose*. »[784] Cela permet d'assurer un standard commun de protection et d'éviter un décalage entre entreprises et ONG sur la perception des risques propres aux acteurs humanitaires : « *Avec les prestataires de services pour la dimension contractuelle, c'est pas évident, c'est une question complexe, parce que les prestataires de service ne sont pas toujours sensibilisés à la protection des données, voire n'ont pas de clauses spécifiques liées à la protection des données, quand on leur suggère une clause assez spécifiquement, ils sont pas tout à fait conscients de ce que ça représente, il faut faire toute une sensibilisation à la protection des données, ça nous permet de mettre de côté certains prestataires.* »[785] Mais à vrai dire, au regard de la place des prestataires non européens, du fait de la domination américaine sur le secteur numérique, l'application de clauses contractuelles types est bien souvent obligatoire. Et certains DPO font le choix d'imposer des mesures supplémentaires pour les prestataires non-européens : « *Les prestataires de niveau international (…) ils s'engagent à signer les clauses, mais elles ne sont pas suffisantes, il faut des garanties complémentaires, notamment pour les USA, qui sont pas évidentes à mettre en œuvre*. » [786]

Cela nécessite de pouvoir négocier des clauses contenant de solides garanties en matière de protection des données lors de la signature des contrats. Or, lorsqu'il existe des inégalités entre organisations et prestataires, imposer une logique de responsabilisation au sous-traitant reste ardu. Les DPO sont d'ailleurs quasi unanimes sur le peu de marge de manœuvre dont ils disposent pour marchander ces clauses contractuelles face aux GAFAM : « *On arrive bien à négocier avec les prestataires, avec les GAFAM, avec Microsoft, je ne sais même pas si on a une marge de manœuvre*. »[787] L'autorité de protection des données allemande a d'ailleurs critiqué les clauses contractuelles types de Microsoft, surtout relativement à sa suite logicielle 365[788]. Elles ne seraient pas suffisamment précises en matière de catégorie de données traitées, ainsi que sur leur finalité d'usage. Et elles laisseraient possible un partage de données avec des tiers de façon plus large que ne le permet le RGPD. Et la possibilité d'un partage de données vers les États-Unis reste un point important d'inquiétude, comme on le verra dans la deuxième partie au sujet de l'informatique en nuage et du Cloud Act. Les termes des contrats ne présenteraient pas un niveau de protection convenable, et comme le résume une DPO : « *Les organisations américaines utilisent les mots du RGPD, mais ne les définissent*

[783] Entretien n° 44, OI2, DPO, 07/03/2021
[784] Entretien n° 44,OI2, DPO, 07/03/2021
[785] Entretien n° 44, OI2, DPO, 07/03/2021
« Companies must "do no harm" in the humanitarian sector », *Privacy International*, 11/12/2018 [https://privacyinternational.org/news-analysis/2536/companies-must-do-no-harm-humanitarian-sector]
HUSSEIN, Pia, « Fit for the Future Series Interoperability: Humanitarian Action in a Shared Space », Ocha policy and studies series ,07/2015 [https://www.unocha.org/sites/dms/Documents/OCHA_TB13_Interoperability_online.pdf ]
[786] Entretien n° 44, OI2, DPO, 07/03/2021
[787] Entretien n° 88, ONG24, DPO, 15/11/2021
[788] AG DSK „Microsoft-Onlinedienste" Zusammenfassung der Bewertung der aktuellen Vereinbarung zur Auftragsverarbeitung, Datenschutzkonferenz, 24/11/2022 https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_zusammenfassung.pdf

*pas, les clauses confidentielles de boites américaines, c'est n'importe quoi. Elles peuvent mentionner : les données collectées seront notre propriété intellectuelle. »*[789]

Et donc malgré l'existence de ce cadre juridique, dépendre des sous-traitants reste un facteur d'insécurité pour certains DPO, d'où la tentation de recourir à des solutions développées en interne ou stocker ses données sur ses serveurs. Ceci représente un investissement que peu d'ONG peuvent se permettre : *« La situation idéale d'avoir de bout en bout le plus de données contrôlées par une seule organisation humanitaire, ça serait vraiment le but ultime, mais ça demande un investissement en temps et en argent qui est monstrueux, mais je pense que c'est nécessaire et je pense qu'on fait des "baby step" à ce niveau-là, progressivement on y va, le fait de ramener des "app" dans nos services, il y a beaucoup d'organisations qui essayent de ramener leurs données sur leurs propres serveurs, c'est déjà un premier pas pour contrôler les données, les ramener à la maison, l'idéal serait de pouvoir se passer un jour de parties tierces, maintenant à l'heure actuelle c'est impossible en termes de gouvernance, nous on est 25 000 dans le monde, on a déjà du mal, les 3/4 de l'humanitaire sont beaucoup plus petits ils ont aucune capacité de pouvoir se passer de gros providers*. »[790]

Cette section avait pour finalité de donner quelques exemples des difficultés d'ONG à réguler les risques liés à la sous-traitance, d'autant qu'il reste difficile d'assurer la transparence le long de la chaine des traitements de données, et se profile toujours le risque de détournement d'usage (« function creep » en anglais). Ce risque est favorisé par la porosité propre au capitalisme de surveillance entre les acteurs étatiques, dont les forces de l'ordre et les services de sécurité, et le secteur privé[791].

## Section 4 — Régulation de l'innovation et privacy by design

L'approche « privacy by design » propre au RGPD n'est pas en soi une mesure de « compliance ». Mais cette notion est dans le RGPD liée à l'« approche par le risque ». Il s'agit d'anticiper ces derniers, en adoptant un outil technique les minimisant d'emblée, et potentiellement grâce à une AIPD. Enfin, à titre plus général, la « privacy by design » s'inscrit tout à fait dans ce chapitre. Cette dernière repose sur d'autres présupposés que les pratiques expérimentales. Il ne s'agit plus de tester directement des technologies sur le terrain, mais d'anticiper en amont leur impact sur les sujets.

### § 1 — la notion de « privacy by design »

[789] Entretien n° 83, ONG1, DPO, 14/10/2022
[790] Entretien n° 44, OI2, DPO, 07/03/2021
[791] « Ces affinités électives ont soutenu l'exceptionnalisme de surveillance et contribué au terreau sur lequel la mutation du capitalisme de surveillance s'est développée jusqu'à sa pleine maturité. » ; « These elective affinities sustained surveillance exceptionalism and contributed to the fertile habitat in which the surveillance capitalism mutation would be nurtured to prosperity. »ZUBOFF, Shoshana, *L'Age du capitalisme de surveillance*, Paris, Zulma, coll. Essais, 2020, p.80.

Pour définir ce terme, on peut se référer aux travaux de Flora Fischer qui déplie l'ensemble des significations et traductions de l'expression « by design » : intention, dessein, conception, etc. C'est cette dernière acception qui nous intéresse. Comme l'explicite Flora Fischer il implique qu'une « intention éthique » soit inscrite dans un outil. L'idée est de maitriser de bout en bout les répercussions d'une technologie[792]. Il est clair que l'approche est préventive : elle suppose d'éviter tout risque de fuite informationnelle dès la conception du logiciel.

Plus précisément, l'expression « privacy by design » est formulée en 1995 dans un rapport conjoint de l'autorité de protection des données canadiennes et danoises portant sur les « privacy Enhancing Technologies »[793]. Le rapport explorait des pistes pour développer des services numériques exploitant moins de données personnelles tout en assurant les mêmes fonctionnalités. La notion est ensuite reprise par Ann Cavoukian, commissaire à la protection des données canadienne. Son principe de base est d'une très grande simplicité : un logiciel doit être développé de façon à respecter dès sa conception la vie privée des utilisateurs. Ann Cavoukian précise que le terme de « privacy by design » comprend sept facettes : (1) l'anticipation : il faut prévenir les atteintes à la vie privée avant qu'elles n'adviennent ; (2) La vie privée « par défaut » : il faut que le design de l'outil protège l'utilisateur sans action de sa part. À cette fin, il est nécessaire de limiter la collecte des données et respecter le principe de minimisation, ainsi que de restreindre les finalités d'usages des outils ; (3) intégré (« core design ») : la protection des données fait partie intégrante du système de l'outil et doit occuper une place essentielle de son développement ; (4) la compatibilité : les mesures de protection des données ne doivent pas empêcher la bonne marche d'autres fonctionnalités du logiciel ; (5) De bout en bout : les mesures de protection doivent être implémentées tout le long du cycle d'usage de l'outil ; (6)la transparence : l'outil doit rester transparent, il peut être audité de façon indépendante et les utilisateurs doivent en comprendre le fonctionnement ; (7) le respect de la vie privée des utilisateurs : un outil de type « privacy by design » doit prendre en compte l'utilisateur, permettre de recueillir son consentement et respecter l'ensemble des droits accordés par les réglementations en matière de protection des données (droit d'accès, rectification, etc.) [794]

La « privacy by design » a connu une certaine fortune au sein des organismes européens dédiés à la protection des données. La Directive de 1995 contenait déjà quelques éléments relatifs à cette dernière. Ainsi, l'article 46 requiert que la protection de données doive être envisagée dès la conception d'un traitement de données[795]. Le G29 se positionne aussi en faveur de cette notion : « ce principe devrait être contraignant pour les concepteurs et les producteurs de technologies, ainsi que pour les responsables du traitement des données, qui

---

[792] FISCHER, Flora, « L'éthique *by design* du numérique : généalogie d'un concept », *Sciences du Design*, 2019/2 (n° 10), p. 61-67. https://www.cairn.info/revue-sciences-du-design-2019-2-page-61.htm

[793] HES, R., BORKING, John, "Privacy-Enhancing Technologies: The Path to Anonymity", 1995, Registratiekamer, Information and privacy commissioner / Ontario, https://www.researchgate.net/publication/243777645_Privacy-Enhancing_Technologies_The_Path_to_Anonymity

[794] CAVOUKIAN, Ann,"Privacy by Design: The 7 Foundational Principles", Toronto, 2010, www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf.

[795] Art. 46 Directive 95/46/CE « considérant que la protection des droits et libertés des personnes concernées à l'égard du traitement de données à caractère personnel exige que des mesures techniques et d'organisation appropriées soient prises tant au moment de la conception qu'à celui de la mise en oeuvre du traitement, en vue d'assurer en particulier la sécurité et d'empêcher ainsi tout traitement non autorisé; qu'il incombe aux États membres de veiller au respect de ces mesures par les responsables du traitement; que ces mesures doivent assurer un niveau de sécurité approprié tenant compte de l'état de l'art et du coût de leur mise en oeuvre au regard des risques présentés par les traitements et de la nature des données à protéger. »

devraient être obligés de tenir compte de la protection technologique des données dès le stade de la planification des procédures et des systèmes informatiques. »[796]

Et le principe est entériné par l'article 25 du RGPD[797]. Ce dernier regroupe un ensemble de mesures à prendre pour garantir en amont d'un traitement de données la protection des personnes concernées. Dans le règlement, la « privacy by design » est interprétée de façon plus large que le choix d'une architecture d'un logiciel. Il s'agit de « concevoir » un traitement de données de bout en bout de manière à anticiper les risques pour les personnes concernées. Le responsable de traitement doit certes choisir un logiciel respectueux de la vie privée des utilisateurs, mais également prendre plusieurs mesures visant à penser une collecte de données en conformité avec l'esprit du règlement.

Pour ce qui concerne les mesures techniques, le CEPD donne des pistes à suivre : le fait d'utiliser des solutions techniques avancées ou mettre en place des formations de base pour le personnel d'une organisation[798]. Le DPO a donc l'obligation d'observer « l'état de l'art » technique en matière de protection des données. Et il doit s'assurer que les outils choisis sont dignes de confiance. Les textes juridiques ne mentionnent pas de technologies particulières permettant de respecter le principe de « privacy by design ». Toutefois, Carmella Troncoso regrette en 2011 que la plupart des textes réglementaires ne donnent pas de méthodologie plus claire sur les attentes en matière d'implémentation technique de la « privacy by design ». Mais, le texte se veut « neutre technologiquement parlant » afin d'éviter de devenir obsolète. En effet, au regard des progrès techniques, le risque est grand de se prononcer en faveur d'une technologie pouvant devenir à terme inefficace. Il est clair que les standards de chiffrement sont en évolution constante, entre autres en réaction aux développements de l'IA et de l'informatique quantique[799].

Quoi qu'il en soit, il est recommandé de mener des AIPD pour guider les choix du DPO. Les lignes directrices du CEPD associent donc directement « approche par les risques » et « protection des données dès la conception ». Il est aussi proposé de mettre en place des labels ou des certifications pour aider le DPO à se repérer dans l'offre technologique. Dès lors en 2023, la norme ISO 3700 relative à la « privacy by design » a été adoptée. Le CEPD recommande aussi l'adoption de « Privacy Enhancing Technologies » (PETS). Il n'y a pas de définition arrêtée de ces dernières. Ce terme désigne différentes technologies permettant d'atténuer les risques d'atteinte à la vie privée. Les PETS englobent donc différentes

---

[796] « this principle should be binding for technology designers and producers as well as for data controllers, they should be obliged to take technological data protection into account already at the planning stage of information-technological procedures and systems. »
JASMONTAITE,Lina,KAMARA, Irene, ZANFIR-FORTUNA, Gabriela, LEUCI, Stefano, "Data Protection by Design and by Default: Framing Guiding Principles into Legal Obligations in the GDPR", *European Data Protection Law Review*, Vol. 4, No. 2, 2018
BUTTARELLI, Giovanni, "Opinion 5/2018: Preliminary Opinion on Privacy by Design", 31/05/ 2018 https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary….

[797] « Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée » Art 25, Règlement 2016/679 https://www.privacy-regulation.eu/fr/25.htm

[798] MICHELAKAKI, Christina, BARROS VALE, Sebastiao, "Unlocking Data protection by design & by default: lessons from the inforcement of Article 25 GDPR", *The future of privacy*, May 2023 https://fpf.org/wp-content/uploads/2023/05/FPF-Article-25-GDPR-A4-FINAL-Digital.pdf

[799] EDPS, Opinion 5/2018, "Preliminary Opinion on privacy by design", 31/05/2018 https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf

techniques de chiffrement, comme le chiffrement homomorphique[800], le calcul multipartite différencié [801], la confidentialité différentielle [802], les preuves à divulgation nulle de connaissance, etc.[803] Au-delà des PETS, la « privacy by design » peut être envisagée jusqu'au cœur du réseau internet, le protocole IP/TP ne garantissant pas la protection des internautes, comme le rappelle le CEPD, d'où l'appel à développer d'autres types de protocoles, plus protecteurs, comme le protocole SCION réalisé par des ingénieurs suisses, que le CICR projette d'ailleurs d'utiliser[804].

Néanmoins, pour Alain Rallet, Fabrice Rochelandet[805], le terme « privacy by design » ne doit pas devenir un pur sigle et être utilisé en tant qu'argument commercial[806], comme le ferait la firme Apple[807]. D'autant que des intérêts économiques sont en jeu : les PETS constituent aussi un marché attractif, le marché du chiffrement homomorphique en Europe pèse lourd. Selon différents diagnostics, il est attendu qu'il croisse fortement et qu'il passe de 31 millions de dollars de bénéfices en 2019 à 66 millions de dollars de bénéfices en 2027[808].

En outre, il ne faut pas restreindre les approches de type « privacy by design » à une dimension strictement technique. L'ingénieure Carmela Troncoso elle-même rappelle qu'il est nécessaire de s'intéresser aux modalités d'usage d'un outil. Un système conçu de façon à respecter des principes de « privacy by design » ne peut pas être, bien entendu, utilisé à des finalités de surveillance. Les démarches de type « privacy by design » ne doivent pas mettre de côté la réflexion sur la nécessité et la légitimité de l'utilisation d'un certain système. Autre évidence, la conception d'un système technique respectueux de la vie privée doit prendre en compte le contexte sociopolitique et ne doit pas se limiter à un pur problème d'ingénierie[809], comme le prévient un de nos enquêtés : *« je trouve triste aujourd'hui (…) qu'on n'ait pas vraiment de moyens techniques d'obliger un "purpose limitation" et (…) avec les gens du cyber on va dire, ah ouais, vous avez tout ça et on va genre mettre du chiffrage et on va... On aura pleins de feuilles de route tout ce que vous voulez, mais la notion même de : mais pourquoi tu as besoin de ça et quel est le risque s'il est "disclose" ça rentre pas et donc ça c'est un problème*. » Selon

---

[800] https://www.cnil.fr/fr/definition/chiffrement-homomorphe
[801] https://www.cnil.fr/fr/definition/calcul-multipartite-securise
[802] https://www.cnil.fr/fr/definition/confidentialite-differentielle
[803] ARFOUI, Mehdi, TOUBIANA, Vincent, « Peut-on faire confiance aux PETs? Privacy Research Day", *LINC Cnil*, 14/06/2023 https://linc.cnil.fr/privacy-research-day-peut-faire-confiance-aux-pets
BABILLO, Maria, "Navigating privacy-enhancing technologies : key takeaways from the inaugural meeting of the global PETS network", *Privacy Forum*, 07/09/2023 https://fpf.org/blog/navigating-privacy-enhancing-technologies-key-takeaways-from-the-inaugural-meeting-of-the-global-pets-network/
[804] https://scion-architecture.net/
SEYDTAGHIA, Anouch, « Scion, l'internet ultra-sécurisé conçu en Suisse, décolle », *Le Temps*, 08/02/2023 https://www.letemps.ch/economie/finance/scion-linternet-ultrasecurise-concu-suisse-decolle
MARELLI, Massimo, "Opening an ICRC delegation for Cyberspace", *EJIL: Talk!,* 09/02/2023 https://www.ejiltalk.org/opening-an-icrc-delegation-for-cyberspace/
[805] RALLET, Alain, ROCHELANDET, Fabrice, ZOLYNSKI, Célia, « De la *Privacy by Design* à la *Privacy by Using*. Regards croisés droit/économie », *Réseaux*, 2015/1 (n° 189), p. 15-46. https://www.cairn.info/revue-reseaux-2015-1-page-15.htm
[806] GURSES, Seda, TRONCOSO, Carmela, DIAZ, Claudia, « Engineering Privacy by design », KU Leuven, IBBT, ESAT / SCD-COSIC, 2011 https://software.imdea.org/~carmela.troncoso/papers/Gurses-CPDP11.pdf
[807] BHUIYAN, Johana, "Apples says it prioritizes privacy, experts say gaps remain", *The Guardian*, 23/09/2022 https://www.theguardian.com/technology/2022/sep/23/apple-user-data-law-enforcement-falling-short
[808] RENIERIS, Elizabeth, "Why PETS ( Privacy-Enhancing technologies) may not always be our friends", *Adalovelace Institute*, 29/04/2021 https://www.adalovelaceinstitute.org/blog/privacy-enhancing-technologies-not-always-our-friends/
[809] GURSES, Seda, TRONCOSO, Carmela, DIAZ, Claudia, "Engineering Privacy by design", KU Leuven, IBBT, ESAT / SCD-COSIC, 2011 https://software.imdea.org/~carmela.troncoso/papers/Gurses-CPDP11.pdf

cet enquêté, Il ne faut donc pas « déléguer » totalement le respect de la vie privée à la technique[810].

Dernier point, les solutions « privacy by design » doivent, en outre, être relativement simples d'utilisation pour les usagers. À vrai dire, la « privacy by design » tend à mettre l'utilisateur hors de la boucle. Il peut être protégé. Mais dans ce cas, ce dernier ne garde pas nécessairement le contrôle sur les flux de données le concernant. C'est pour cela que certains chercheurs penchent donc pour des solutions de type « privacy by using ». On évoquera d'ailleurs ce point dans la dernière partie de cette thèse, consacrée aux droits des bénéficiaires et plus particulièrement au sujet des liens entre des dispositifs décentralisés (comme des blockchains) et l'autodétermination informationnelle.

## § 2 — la « privacy by design » dans l'humanitaire

L'approche « privacy by design » est peu discutée au sein du secteur humanitaire. Certaines politiques de protection des données d'ONG mentionnent ce principe. Mais la plupart du temps, le terme n'est pas précisément défini. Toutefois, certains guides sont plus détaillés. La politique de protection des données de l'IFRC prend la forme d'une « checklist ». Il est encouragé de choisir un logiciel parmi les technologies existantes (sans recourir nécessairement à des solutions innovantes) et respecter une série de critères prédéfinis[811]. OXFAM adopte une acception large du terme et le relie au sens qu'en donne le RGPD. Il s'agit de contrôler l'ensemble du cycle de traitement de données de manière à atténuer les risques : « Notre objectif est d'inclure le respect de la vie privée dès la conception tout au long du cycle de vie des données, ce qui nécessite de trouver un équilibre entre une planification minutieuse à chaque étape et une évaluation pratique des risques. » [812]

La politique de protection des données d'UNICEF mentionne aussi cette expression : « L'UNICEF doit intégrer la "protection des données dès la conception et par défaut" dans la planification, le développement et la prise de décision, et mettre en œuvre des mesures techniques et organisationnelles appropriées, telles que la minimisation des données et la pseudonymisation. » [813] UNICEF a ainsi annoncé une collaboration avec Apple pour développer un produit respectant des critères de « privacy by design », cette démarche s'inclut dans sa politique de partenariat avec le secteur privé[814].

---

[810] Entretien n°93, OI2, DPO, 02/06/2023

[811] Data Playbook, checklist 1", IFRC, https://preparecenter.org/wp-content/sites/default/files/checklist1data_technology060618.pdf

[812] « Our aim is to build privacy by design throughout the data lifecycle, which requires balancing careful planning at each stage with practical risk assessment. »OXFAM, "Going digital, privacy and data security under GDPR for quantitative impact evaluation", October 2019 https://oxfamilibrary.openrepository.com/bitstream/handle/10546/620884/cs-going-digital-gdpr-181019-en.pdf?sequence=1

[813] « UNICEF shall incorporate "data protection by design and by default" into planning, development and decision making, and implement appropriate technical and organizational measures, such as data minimization and pseudonymization » https://www.unicef.org/globalinsight/media/1286/file/%20UNICEF-Global-Insight-DataGov-data-use-brief-2020.pdf
NYST, Carly, GOROSTIAGA, Amaya, GEARY, Patrick , "Industry toolkit, children privacy and freedom of expression", UNICEF, 2018

[814] UNICEF, « Data governance for children : an emerging priority area for privacy professionals », 19/05/2022, https://www.unicef.org/globalinsight/stories/data-governance-children-emerging-priority-area-privacy-professionals

Le CICR a aussi interprété le terme de « privacy by design » en mettant l'accent sur sa dimension technologique et en le reliant à une démarche d'innovation. En effet, pour Massimo Marelli, DPO au sein de l'organisation, la protection des données exige de jouer sur les deux niveaux : sur le plan juridique et sur le plan infrastructurel. Les deux aspects doivent aller de pair, ce qui est raccord avec une approche de type « privacy by design ». Ainsi, la transformation numérique de l'organisation a eu comme principe directeur majeur la protection de la vie privée : « *Après ce qui a été très très intéressant, l'informatique au CICR, l'IT a toujours eu un rôle de support à nos opérations. On n'est pas une société technologique. On ne crée pas des logiciels. Elle était réduite à ce qui est nécessaire, mais pas tellement plus. On allait pas investir des millions pour avoir l'application la plus jolie, et ce qui a malheureusement aussi signifié qu'on avait pas de recherche sur les nouvelles technologies. Quand on a eu cette accélération de la digitalisation, poussée par différents éléments, il fallait être présent sur ces questions… Pourquoi vous faites pas de drones, pourquoi vous ne faites pas d'IA ? Ces questions-là on les avait, mais on n'avait pas la capacité d'y répondre parce qu'on n'avait pas d'investissement dans ce domaine. Et la personne de la protection des données s'est dit, bon bah si on ne peut pas justifier l'investissement IT, on va pouvoir le justifier du point de vue de la protection des données*. »[815]

Or, selon Massimo Marelli les outils pouvant respecter les exigences du CICR en matière de vie privée ne sont pas encore commercialisés : « Il se peut que ces produits ne soient pas disponibles sur le marché à l'heure actuelle et qu'ils doivent être achetés dans le cadre de partenariats de recherche et de développement avec des universités et d'autres partenaires, pour être ensuite convertis en solutions durables. » [816] Pour développer des outils technologiques répondant à ses besoins, le CICR a donc noué différents partenariats avec des universités et des entreprises afin de développer des outils numériques. Le CICR travaille ainsi avec des écoles d'ingénieur suisses, celle de Lausanne et de Zurich[817]. Plusieurs projets sont menés sous la houlette de Carmela Troncoso, une ingénieure très engagée en matière de « privacy by design »[818]. Enfin, un centre de recherche a été ouvert au Luxembourg, baptisé « Délégation pour le Cyberespace ». Cette dernière se veut être un « espace sûr », avec pour : objectif « d'explorer et de comprendre plus avant ce que la neutralité, l'impartialité et l'indépendance signifient dans un contexte numérique et comprendre comment ils sont liés aux débats en cours sur la "souveraineté numérique". Il s'agit de créer un terrain d'essai neutre, impartial, indépendant et exclusivement humanitaire (ou "souverain") et sûr où le CICR peut mener des activités de recherche et de développement (…) et où il peut s'engager en toute sécurité dans le dialogue et les débats opérationnels nécessaires, sans les risques liés

[815] Entretien n°93, OI2, DPO, O2/06/2023

[816] « these may not, at present, be available from the market, and may need to be procured as part of research and development partnerships with academia and other partners, to be then converted into sustainable solutions. » MARELLI, Massimo, PERRIG, Adrian, "Hacking humanitarian : mapping the cyber environment and threat landscape", ICRC, Humanitarian Law & Policy,07/05/2020https://blogs.icrc.org/law-and-policy/2020/05/07/hacking-humanitarians-mapping-cyber-environment/

[817] ETH Zurich, « Engineering at the service of humanitarian aid », 10/12/2020 https://ethz.ch/en/news-and-events/eth-news/news/2020/12/cooperation-icrc.html

[818] GURSES, Seda, TRONCOSO, Carmela, DIAZ, Claudia, "Engineering Privacy by design", KU Leuven, IBBT, ESAT / SCD-COSIC, 2011 https://software.imdea.org/~carmela.troncoso/papers/Gurses-CPDP11.pdf

aux contextes opérationnels "réels". »[819] Au-delà des principes propres au RGPD, mentionnons simplement que le CICR, en tant qu'organisation internationale, explore différentes solutions pour transposer ses immunités et privilèges dans le domaine numérique. Différents pilotes sont en cours : emblèmes digitaux, développement de solutions de type logiciels libres, mais aussi d'un pilote de dispositifs d'identification biométrique. On examinera rapidement ces deux derniers projets.

Tout d'abord, le CICR explore en effet présentement les potentialités des logiciels libres et open sources en matière de « privacy by design ». Au contraire des GAFAM, le modèle économique des logiciels libres ne repose pas centralement sur l'exploitation des données des utilisateurs. Et en matière de protection de la vie privée, ils sont, dans une certaine mesure, considérés comme sûrs. En tout cas, ces derniers sont audités par une communauté. Par voie de conséquence, les failles seraient plus facilement détectables et corrigées. Massimo Marelli rappelle d'ailleurs ce point : « De telles dépendances comportent divers risques : si le vendeur fait faillite, il ne peut plus fournir de support pour ses produits ou de correctifs pour remédier aux vulnérabilités découvertes. En outre, le fournisseur peut soudainement modifier ses politiques et ses tarifs au détriment du client, voire cesser de fournir ses produits et services sous la forme d'une sanction numérique. »[820] En outre, la sécurité de ce type de logiciel est discutée et ne fait pas consensus. Plusieurs cas de failles ont été recensés : en 2014, la faille Heartbleed, détectée dans la librairie OpenSSL, avait touché de nombreux sites web, dont Facebook, Google et Twitter. En outre, la nature collaborative de l'open source est certes gage de sécurité, mais tout dépend de l'implication de la communauté de codeurs dans un projet. S'ils sont peu investis, des failles peuvent passer longtemps inaperçues. Et d'un autre côté, le fait de rendre visible le code peut signifier que des hackeurs peuvent en exploiter les défauts.

L'adoption de solutions de type logiciel libre n'est pas encore à l'ordre du jour, d'après nos entretiens, pour le moment, l'organisation en reste à un stade « exploratoire ». Un partenariat a été noué avec le CERN afin de creuser la possibilité de recourir à ce type de logiciel. L'institution défend en effet l'usage de logiciel libre, en raison de motifs éthiques et financiers : le coût des licences Microsoft est prohibitif. Et le centre de recherche nucléaire développe en interne des alternatives aux GAFAM. Plus profondément, il existe au CERN une longue tradition en matière de logiciel libre et « open source »[821]. Et récemment, le CERN a conduit le projet « MALT », dont l'acronyme signifie au départ tout simplement : Microsoft Alternative. Le projet a par la suite été renommé « Microservice Architecture on Libre

[819] « Considering the complexity and novelty of the above objectives, as well as the potentially wide-ranging implications of 'getting it wrong', the objective is to further explore and understand what neutrality, impartiality, and independence mean in a digital context, and if and how this connects with ongoing debates on 'digital sovereignty'. It involves creating a neutral, impartial, independent and exclusively humanitarian (or "sovereign") and secure testing ground where the ICRC can carry out Research and Development (R&D) (…) and in which it can safely engage in necessary operational dialogue and debates without the risks attached to 'real' operational contexts. »MARELLI, Massimo, "Opening an ICRC delegation for Cyberspace", *EJIL: Talk!*, 09/02/2023 https://www.ejiltalk.org/opening-an-icrc-delegation-for-cyberspace/

[820]« Such dependencies bear various risks: if the vendor goes out of business, it can no longer provide support for its products or patches to address discovered vulnerabilities. Also, the vendor can suddenly change its policies and pricing to the detriment of the customer, or even stop delivering its products and services as a form of digital sanction "MARELLI, Massimo," The SolarWinds hack : lessons for international humanitarian organizations", *International review of the Red Cross*, Vol 104, number 919, 2022 https://international-review.icrc.org/sites/default/files/reviews-pdf/2022-06/Selected-Articles-International-Review-of-the-Red-Cross-No-919.pdf

[821]DUSSUTOUR, Chloé, « CERN, an international organisation paving the way for the use of open source software in research, OPENSOURCE Observatory, European Commission, 24/09/2020 https://joinup.ec.europa.eu/collection/open-source-observatory-osor/document/cern-international-organisation-paving-way-use-open-source-software-research

Technology ». Et effectivement, de manière générale, les logiciels « open sources » constitueraient une échappatoire à l'écosystème extractif des GAFAM et du capitalisme de surveillance[822]. Cela dit, Nick Couldry ne les mentionne cependant pas dans son ouvrage « The Costs of connection ». Sortir du « data colonialisme » requiert un changement plus profond que l'adoption de solutions techniques. Et pour le chercheur « Décoloniser les données signifie parler maintenant à partir de la position des colonisés informationnels et imaginer un avenir commun pour l'humanité au-delà du projet contemporain de réduire la vie humaine aux flux d'input/output. »[823] Et surtout, dernière limite, l'écosystème du logiciel libre et de l'open source est investi par les acteurs privés, Microsoft, Twitter, Facebook, etc. Beaucoup de solutions sont hybrides. En bref, tout dépend du modèle économique du projet [824].

Évoquons maintenant un deuxième projet du CICR. L'organisation a mis au point un dispositif d'identification biométrique respectant la vie privée dès sa conception. Ce projet étonne. En effet, à l'inverse de l'UNHCR, le CICR collecte des données biométriques de façon moins systématique. Et la politique de protection de données biométriques du CICR publiée en 2019 est relativement restrictive. Elle préconise un stockage décentralisé, contrairement à l'UNHCR qui est connu pour ses bases de données biométriques pléthoriques. Leur collecte doit être limitée au mandat du CICR et dans des cas bien circonstanciés : pour l'identification des morts (ADN, reconnaissance faciale), pour son service de rétablissement de liens familiaux (photographies) ; pour des documents de voyage du CICR destinés à des personnes dépourvues d'identité afin de leur permettre de revenir dans leur pays d'origine[825] (recueil d'empreintes). Toutefois, les programmes de distribution d'aide ne font pas partie de son mandat originel. Mais la collecte de données biométriques est alors dans ce cas justifié par l'efficacité de ce type de solutions et le fait qu'elles assurent un gage de redevabilité[826]. En

---

[822] SODERBERG, Johan, *Hacking capitalism, the Free and open source software movement*, New York, London: Routledge, 2008, 252 p.

[823] « Recent infrastructures of connection have facilitated new forms of collectivity, but this does not mean that we must accept the forms of exploitation that are indissolubly tied to the data relations associated with those infrastructures. If we disown the corporate dream that the world's rich diversity can and must be ordered for profit, we may find that other forms of connection are possible."
« Decolonizing data means speaking now from the position of data's colonized and imagining a common future for humanity beyond the contemporary project to reduce human life to the inputs and outputs of data processing." COULDRY, Nick, MEJIAS, Ulises, *The costs of connection*, Standford university Press, 2019, 352 p.

[824] « De nombreux projets de biens communs numériques reposent sur des logiciels libres, dont les modèles commerciaux peuvent être très divers. Il peut s'agir de configurations à double licence où la distribution est ouverte pour les organisations à but non lucratif et payante pour d'autres, comme MySQL, ou de services de conseil ou de distribution et/ou de services de licence d'un logiciel libre ou d'un modèle de licence, comme RedHat. Ils peuvent également être hybridés avec des logiciels propriétaires4 par le biais de développements verticaux utilisant des logiciels libres comme base sur laquelle des logiciels propriétaires sont construits (par exemple, Google avec le soutien du noyau Linux). Il existe également des arrangements horizontaux dans lesquels les sociétés/entreprises s'impliquent dans des projets de logiciels libres, comme l'application WebSphere d'IBM qui permet aux utilisateurs de créer leurs propres applications à l'aide du logiciel libre Apache. « , "Many digital commons projects rely on FLOSS, of which business models can be very diverse. They can involve dual-licensing configurations where distribution is open for non-profits and payable for others, such as MySQL, or consulting services or distribution and/or licensing services of an open-source software or licensing model, such as RedHat. They can also be hybridized with proprietary software4 through vertical developments using open-source software as a base upon which proprietary software is built, (e.g., Google with Linux core support). Alternatively, horizontal arrangements exist where corporations/businesses involve themselves in open-source projects, such as IBM's WebSphere application which enables users to build their own apps using the Apache open-source software."FRION, Louise, "Digital commons as alternative systems of value", Science po, May 2022https://www.sciencespo.fr/public/chaire-numerique/wp-content/uploads/2023/06/15-juin-DIGITAL-COMMONS-policy-brief-Louise-Frion-1.pdf
« Les communs numériques sont-ils condamnés à devenir des "communs du capital" ?, *Scinfolex*, 24/06/2018https://scinfolex.com/2018/06/24/les-communs-numeriques-sont-il-condamnes-a-devenir-des-communs-du-capital/

[825] "The Emergency travel document", The International committee of the red cross, 2018

[826] « Après mûre réflexion, le CICR a conclu qu'il était possible de tirer parti des gains d'efficacité et d'efficience de l'authentification biométrique, ainsi que de la responsabilité de bout en bout dans ses distributions d'aide, tout en minimisant les risques pour ses bénéficiaires.", "After careful consideration, ICRC concluded that it was possible to leverage the efficiency and effectiveness gains of biometric authentication, as well as end-to-end accountability in its aid distributions, while also minimizing the risks to its beneficiaries." HAYES, Ben, MARELLI, Massimo, "Reflecting on the International committee of the Red Cross's biometric policy : minimizing centralized databases", 09/2023 https://ainowinstitute.org/wp-content/uploads/2023/09/regulatingbiometrics-hayes-marelli.pdf

effet, en raison de leur caractère irrévocable, les données biométriques permettent une meilleure traçabilité de l'aide et répondent ainsi aux exigences de transparence des bailleurs. Et ce projet — encore au stade de pilote — résulterait en partie de fortes pressions (de la part des bailleurs) pour recueillir ce type de données : « *Maintenant, il y a des pressions, maintenant nous ce qu'on est parvenu à faire, c'est limiter encore une fois les risques, donc de toute façon on va prendre des risques, toutes les organisations humanitaires demain vont prendre des risques, et on aura des accidents, y aura des problèmes, ce n'est qu'une question de temps, soit y en a eu et on est pas encore au courant, donc tout ce qu'on peut faire, c'est limiter les risques, donc ce qu'on a fait avec la biométrie, c'est qu'on a décidé d'autoriser le biométrique, mais sous une forme particulière. »*[827]

La politique sur la biométrie du CICR impose en effet d'adopter une approche « privacy by design ». Ceci pose question. En effet, comment la biométrie, fondé sur l'identification de traits physiques d'une personne, soit une technologie très invasive, peut-elle être conçue de manière à respecter la vie privée des sujets ? Il se trouve qu'il existe des travaux cherchant à répondre à cette question. Les scientifiques explorent plusieurs pistes. Tout d'abord, une solution serait de revenir sur le caractère irrévocable des données biométriques : « L'une des idées consiste à modifier les données biométriques, avec l'aide d'autres données, afin de générer un modèle révocable. »[828] Une autre piste serait de réduire le degré de granularité des données biométriques. L'objectif est de révéler le moins d'information possible sur la personne : « Ces méthodes suppriment des parties de l'échantillon biométrique (par exemple, en découpant une image en blocs et en rejetant la plupart des blocs), ou obscurcissent les données biométriques en les déformant ou en y ajoutant du bruit. Ces transformations font que les données stockées et traitées ne peuvent pas être entièrement liées aux données d'origine. »[829]

Ces solutions ne sont pas encore pleinement matures, comme le reconnaissent les scientifiques[830]. Et le conseiller du CICR en « data protection by design » Justinas Sukaitis reconnait que la recherche en la matière est encore balbutiante : « Le domaine de la biométrie s'est considérablement développé au cours des deux dernières décennies grâce aux améliorations apportées à la reconnaissance, à l'acquisition d'images et à l'intégration de nouvelles technologies. Bien que des travaux importants aient été réalisés sur le sujet (…), la biométrie n'a guère progressé dans l'évaluation des problèmes de confidentialité et de sécurité liés à l'authentification des personnes. » [831]

---

[827] Entretien n°93, OI2, DPO, 02/06/2023

[828] "One idea "is to transform biometrics data, with the help of other data, to generate a template that is revocable." GRAF NARBEL, Vincent, SUKAITIS, Justinas, "Biometrics in humanitarian action : a delicate balance", *Humanitarian Law & Policy, ICRC blogs*, 02/09/2021https://blogs.icrc.org/law-and-policy/2021/09/02/biometrics-humanitarian-delicate-balance/

[829] « These methods remove parts of the biometric sample (e.g. cutting an image into blocks and discarding most of the blocks) or obfuscate the biometric data by distorting it or adding noise to it. These transformations make it so that the stored and processed data cannot be linked to the original one entirely. " GRAF NARBEL, Vincent, SUKAITIS, Justinas, ibid.

[830] MEDEN, Blaz et ali, "Privacy-enhancing face biometrics : a comprehensive survey", IEE Transactions on information forensics and security, vol.16, 2021 https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9481149

[831] "The field of biometrics has vastly expanded over the last two decades with improvements in recognition, image acquisition and integration of new technologies. Though significant work has been made regarding biometric template protection, biometrics have barely improved on assessing privacy and security challenges related to authenticating individuals."
SUKAITIS, Justinas, "Building a path towards responsible use of biometrics : a proposal for security and data privacy evaluation of biometric systems", Master Thesis, EPFL, ICRC, 2021

Et à l'heure d'aujourd'hui, il n'existerait pas selon le CICR de solution disponible et prête à l'emploi répondant aux exigences de l'organisation[832]. Le CICR conduit donc son propre projet de recherche en partenariat avec l'école polytechnique de Lausanne (entre autres avec les chercheuses Boya Wang et Carmela Troncoso) et le Centre de sécurité de l'information de l'organisme de recherche germanique de Helmholtz (avec le chercheur Wouter Lueks). Le pilote a pour objectif de répondre à des contraintes a priori contradictoires. Il faut d'abord s'assurer que seule la personne éligible reçoit de l'aide, avant tout afin de pouvoir communiquer cette information pour des audits de bailleurs, tout en collectant le moins possible de données de bénéficiaires. Le CICR fait en outre le choix d'un système décentralisé de stockage. Les données sont conservées par un système de « token », gardé par le bénéficiaire. Le CICR n'y aurait pas accès selon l'organisation[833].

Ce dispositif n'est pas encore testé en conditions réelles. Il reste donc à savoir quel sera le cadre éthique accompagnant sa mise en œuvre. Citons simplement Justinas Sukaitis, conseiller en « privacy by design » au CICR : « il reste encore des étapes importantes à franchir pour ce système, car même si la théorie et les expériences en laboratoire sont valables, nous devons réaliser l'étude de faisabilité de notre côté, car nous ne testons jamais sur des personnes dont la vie peut être affectée par un bug de dernière minute. »[834] Le produit en est encore actuellement au stade de pilote. Et quand bien même le marché des PETS est en expansion, comme on a pu l'indiquer, d'après nos enquêtés il reste encore difficile de trouver des partenaires commerciaux pour ce type de solutions : *« et ça les grosses sociétés, à un moment donné elles vont dire écoutez c'est super, nous sur la biométrie je me souviens de session avec de gros fournisseurs lorsqu'on a des appels d'offres que ce soit des agences de police aux frontières et qu'on arrive et qu'on est en compétition avec toutes ces entreprises. Et on arrive avec notre solution en disant que notre solution est certes plus chère, mais ça protège les individus, pour ce genre de client, c'est pas vraiment ce qui paie, donc c'est vrai qu'on a du mal à aller au-delà des pilotes et des prototypes.* »[835]

Pour conclure, il nous semble que la démarche du CICR, comme le formule un enquêté, résulte d'un compromis : « *Cela étant, cette vision du biométrique que nous on a choisi, on ne collecte pas de données, ça n'a pas fait plaisir à tout le monde, évidemment en interne, ça n'a pas satisfait, parce que ça ne règle pas le problème de la duplication, parce que l'intérêt du biométrique c'est aussi d'éviter de donner deux fois de l'aide à quelqu'un, les donneurs n'aiment pas trop, ça n'empêche pas ça parce que du coup on n'a pas accès aux données, on ne peut pas faire de "cross-match", pour être sûr que la personne n'a pas reçu deux fois de l'aide, et puis ça ne plait pas aux autorités, parce que les autorités aimeraient bien qu'on ait accès aux données et qu'on puisse leur transmettre, mais bon c'est comme ça, c'est un*

---

[832]"For Graf Narbel, the key issue is the responsible use of biometrics, something he argues is impossible with the tools currently available. ICRC", « Pour Graf Narbel, la question clé est l'utilisation responsable des données biométriques, ce qui, selon lui, est impossible avec les outils actuellement disponibles. «, "The Biometrics Minefield*", InspiRed*, 26/02/2021 https://blogs.icrc.org/inspired/2021/02/26/the-biometrics-minefield/

[833] WANG, Boya, LUEKS, Wouter, SUKAITIS, Justinas, GRAF NARBEL, Vincent, TRONCOSO, Carmela, "Not Yet another digital ID : Privacy-preserving humanitarian aid distribution, 2023, https://doi.org/10.48550/arXiv.2303.17343

[834]"Nonetheless, there are some significant steps ahead for this system as, even though the theory and lab experiments hold, we need to do the feasibility study on our end as we never test on people whose lives may be affected by a last minute bug." EPFL, « Safe Aid: protecting privacy in humanitarian operations », 26/05/2023 https://actu.epfl.ch/news/safe-aid-protecting-privacy-in-humanitarian-operat/

[835] Entretien n°93,OI2, DPO, 02/06/2023

*compromis qu'on a dû faire*. »[836] Ces paragraphes donnent une première idée des rapports de force entre bailleurs, défenseurs de l'innovation numérique et professionnels de la protection des données.

Et surtout, ce type de solution biométrique ne satisferait pas pleinement les bailleurs ni plus largement les défenseurs de la vie privée. Effectivement, un dispositif biométrique est invasif de façon inhérente. Et « Privacy by design » ou non, il reste inscrit dans un rapport de pouvoir : les bénéficiaires peuvent difficilement refuser la collecte de leurs données quand bien même les politiques de protection de données les y autorisent[837]. Le CICR aurait-il pu s'opposer plus franchement aux pressions existantes des bailleurs ? D'autres ONG — dont les contraintes et moyens diffèrent — ont fait le choix de ne pas recourir à des dispositifs biométriques : « *Nous avons dit au siège que nous ne voulions pas recueillir de données biométriques parce que nous ne disposons pas des ressources et de la technologie suffisantes pour nous assurer que nous pouvons le faire d'une manière sûre.* »[838] Toujours est-il que la marge de décision dépend de configurations spécifiques à chaque ONG, en fonction des moyens dont elle dispose en matière de négociation face aux bailleurs, de ressources financières et de réseau d'acteurs universitaires et privés prêts à s'investir dans un projet humanitaire. Or, le CICR malgré son statut international traverse une crise économique. Certes, le numérique est présenté comme un moyen d'améliorer l'efficience, mais à l'avenir, l'organisation aura-t-elle toujours les moyens d'investir dans des programmes de recherche ambitieux en matière de « privacy by design » [839] ? Parmi d'autres potentiels exemples, un projet du CICR de transfert monétaire reposant sur une blockchain a dû être ainsi suspendu pour un temps pour raison financière[840]. Mais dans une déclaration récente à la presse, une porte-parole de l'organisation assure que la cybersecurité restera une priorité à l'avenir. En tout cas, il reste aussi à convaincre les Etats donateurs de renforcer le financement de la cybersécurité et la protection des données. Ce sujet est à l'agenda de 34ème Conférence internationale de la Croix-Rouge et du Croissant-Rouge devant avoir en Octobre 2024[841].

---

[836] Entretien n°93, OI2, DPO,02/06/2023

[837] HAYES, Ben, MARELLI, Massimo, "Reflecting on the International committee of the Red Cross's biometric policy : minimizing centralized databases", 09/2023 https://ainowinstitute.org/wp-content/uploads/2023/09/regulatingbiometrics-hayes-marelli.pdf
POLICY on the processing of biometric data by the ICRC, 28/08/2019

[838] "we have said to the headoffice that we don't want to collect biometric data because we dont have enough ressources and technology to make sure that we can do this in a secure maner." Entretien 21, ONG7, DPO, 27/02/2020

[839] ENDERLIN, Serge, « Le Comité international de la Croix-rouge traverse la plus grave crise de son histoire », *Le Monde*, 05/06/2023 https://www.lemonde.fr/international/article/2023/06/05/le-comite-international-de-la-croix-rouge-traverse-la-plus-grave-crise-de-son-histoire_6176176_3210.html
« En difficulté, la Croix Rouge internationale va encore couper dans ses effectifs », *Les Echos*, 11/09/2023 https://www.lesechos.fr/monde/enjeux-internationaux/en-difficulte-la-croix-rouge-internationale-va-encore-couper-dans-ses-effectifs-1977188
« Le point sur la situation financière du CICR », CICR, 04/04/2023 https://www.icrc.org/fr/document/le-point-sur-la-situation-financiere-du-cicr

[840] « The HTS prototype has been fully developed and is now ready for field testing. Unfortunately, plans to test it in the field with an ICRC delegation have been put on hold due to the institution's challenging financial situation. Nonetheless, the research team remains hopeful that a solution can soon be found with a delegation or with another humanitarian agency. »
'Le prototype HTS a été entièrement développé et est maintenant prêt à être testé sur le terrain. Malheureusement, les plans visant à le tester sur le terrain avec une délégation du CICR ont été suspendus en raison de la situation financière difficile de l'institution. Néanmoins, l'équipe de recherche garde l'espoir qu'une solution pourra bientôt être trouvée avec une délégation ou avec une autre agence humanitaire.'
« humanitarian token solution : digital cash assistance that preserves privacy »27/06/2023,InspiRED,
https://blogs.icrc.org/inspired/2023/06/27/humanitarian-token-solution-digital-cash-assistance-preserves-privacy/

[841] SEYDTAGHIA, Anouch, "Le CICR face à la tâche titanesque de protéger ses données numériques », Le Temps, 28/06/2024

Pour conclure, on s'est donc intéressée aux rapprochements de l'humanitaire avec le secteur privé dans le cadre de sa numérisation. Les entreprises privées ont investi le secteur via des partenariats innovants. Des sociétés de drone ont pu mener des programmes de livraison de médicament, des firmes ont pu tester leurs produits de scan d'iris. En outre, les États où interviennent les ONG sont parfois des États qualifiés de failli, dont les régulations plus fragiles ménageraient pour les firmes la possibilité de mener des expérimentations dans un cadre plus souple. Mais cela ne signifie pas que les enjeux de souveraineté ne se posent pas pour les ONG, et cela est d'autant plus le cas si l'on prend en compte le contexte sécuritaire dans lequel s'inscrit l'aide humanitaire et les exigences de contrôle des ONG par les États, spécifiquement en matière de contre-terrorisme, comme on le verra dans la partie qui va suivre.

Réduire l'humanitaire à un laboratoire technologique serait simplificateur. Les ONG ont mis en place un cadre éthique encadrant les usages numériques. Il s'agit cependant de textes non contraignants. Et l'application du RGPD reste, lors de la rédaction de cette thèse, partielle malgré une certaine sensibilité à la protection des données dans le secteur. Et surtout, les DPO se heurtent aux difficultés générées par l'approche par la compliance propre au règlement. Les DPO n'incarneraient pas encore, pour les différentes autorités de protection de données, une posture d'expertise vis-à-vis des risques numériques, du fait d'un manque de ressources et de formation. Dans le même temps, les autorités de protection de données n'alloueraient pas suffisamment de ressources (notamment en matière de connaissance) pour les DPO humanitaires. Nos entretiens avec des DPO d'ONG confirment en partie ces difficultés, et s'ils revendiquent une plus grande conscience des risques numériques, les méthodologies de gestion de risque sont encore embryonnaires. Les DPO tentent malgré tout de construire des outils adaptés au terrain humanitaire. Il semblerait que les modèles holistiques d'AIPD sont difficilement mis en œuvre. Il est alors nécessaire de trouver un équilibre entre le fait qu'une AIPD soit suffisamment détaillée pour documenter les risques et ne pas se limiter à un exercice formel, mais tout en pouvant être mobilisée dans des contextes de crises et lors de situations d'urgence. Mais au-delà du manque de moyens, il est nécessaire de rappeler les difficultés de mener des analyses de risques viennent aussi de la complexité des systèmes d'informations, interconnexion des systèmes, des situations de crises volatiles, et surtout d'un manque de transparence, caractéristique en un sens des acteurs dominants du numérique, particulièrement en ce qui concerne des GAFAM[842].

Par ailleurs, il est pour les DPO difficile de négocier des clauses suffisamment solides du fait de la position dominante de certains acteurs, surtout lorsqu'il est question des GAFAM. Une manière d'atténuer ce risque est de réduire leur nombre ou d'adopter une approche de type « privacy by design ». Cette dernière nécessite toutefois des ressources qui manquent dans

---

https://www.letemps.ch/cyber/le-cicr-face-a-la-tache-titanesque-de-proteger-ses-donnees-numeriques
SEYDTAGHIA, Anouch, BUSSARD, Stéphane, "La Croix-Rouge italienne touchée par une fuite massive de données, le CICR enquête », le Temps, 19/06/2024
https://www.letemps.ch/cyber/cybersecurite/le-cicr-a-nouveau-touche-par-une-fuite-massive-de-donnees

[842] MASURE, Anthony, « Résister aux boîtes noires. Design et intelligences artificielles », Paris, Puf, *Cités*, n° 80, décembre 2019, anthonymasure.com/articles/2019-12-resister-boites-noires-design-intelligences-artificielles
PASQUALE, Frank, *The black box society : the Secret Algorithms that control money and information*, Harvard University Press, 2015, 320 p.
ZUBOFF, Shoshana, *L'Age du capitalisme de surveillance*, Paris : Zulma, 2020, 864 p.

un secteur humanitaire toujours plus sollicité par la multiplication des crises. Enfin, adopter une démarche de type « privacy by design » ne suffit pas si les rapports de pouvoir, propres à l'humanitaire, restent inchangés. Par exemple, il ne faut pas oublier que les bailleurs de fonds favorisent plutôt la transparence et la traçabilité des financements que les outils garantissant l'anonymat des bénéficiaires.

## Partie II — Recomposition des souverainetés étatiques et protection de la vie privée des bénéficiaires dans l'espace numérique humanitaire

### Introduction de partie

On va maintenant s'intéresser à la manière dont l'exercice des souverainetés étatiques affecte l'espace humanitaire et ses avatars numériques, plus spécifiquement en matière de protection des données. Comme on l'a vu dans notre introduction, la définition « classique » de la souveraineté met l'accent sur la maitrise d'un territoire et d'une population. Sachant que cette maitrise se joue aussi au niveau informationnel : un Etat doit disposer de données sur sa

population, qui qui doit être rendue lisible et transparente[843]. En outre, l'exercice de la souveraineté rend nécessaire le contrôle des moyens de communication et des modalités de la diffusion de l'information ou de son absence de diffusion. Le secret est ainsi constitutif de la figure du souverain absolu[844].

Or, il est admis que l'exercice de la souveraineté territoriale et informationnelle est remis en cause du fait de la numérisation de nos sociétés. L'espace numérique a en effet été initialement pensé comme étant hors du contrôle des États, selon une première conception libertarienne des réseaux, défendue par John Barlow qui y voit un espace équivalent à la haute mer[845]. Et a priori, l'espace numérique ne peut pas être défini comme un territoire. Il est caractérisé par une forte réticularité et par l'interconnexion de serveurs à l'international[846]. Et comme on l'a dit, des acteurs privés, et notamment américains, y occupent une place prépondérante[847]. Ajoutons que la perte de maitrise de cet espace se joue à plusieurs niveaux : à la fois au niveau des infrastructures, au niveau des data centers, des câbles sous-marins[848], et même des réseaux satellites[849]. Elle se joue aussi au niveau informationnel, et concerne le contrôle des données et des communications au travers de plateformes applicatives. Enfin, elle concerne aussi les différents attributs de puissance d'un Etat, lui permettant de garder la main sur un territoire, mais aussi sur une population. Ce pouvoir se traduit par différentes opérations de mise en donnée de ses citoyens (via des opérations de recensement, de délivrance de dispositifs d'identité). Cette fonction tend aussi à être en partie déléguée à des acteurs privés (des entreprises développant et commercialisant des dispositifs d'identité numérique, parfois décentralisés, ambitionnant de redonner aux usagers une forme d'autonomie, et reposant par exemple sur des blockchains).

---

[843] SCOTT, JAMES C., *L'œil de l'État : moderniser, uniformiser, détruire*, Paris : la Découverte, 2021, 546 p.

[844] DAHO, Grégory, GUITTET, Emmanuel-Pierre, POMAREDE, Julien, « Les territoires du secret : confidentialité et enquête dans les mondes pluriels de la sécurité. Introduction », *Cultures & Conflits*, 2020/2 (n° 118), p. 7-17. https://www-cairn-info.ezproxy.utc.fr/revue-cultures-et-conflits-2020-2-page-7.htm

LAURENT, Sébastien- Yves, *État secret, État clandestin : essai sur la transparence démocratique*, Paris : Galimard, 2024, 360 p.

CHRETIEN-GONI, Jean-Pierre, « Institutio arcanae - Théorie de l'institution du secret et fondement de la politique » in LAZZERI, Christian, REYNIE, Dominique, (sous la dir.), *Le pouvoir de la raison d'État*, PUF, 1992, 266p.

DIJSTELBLOEM H., PELIZZA, A., "The state is the secret. For a relational approach to the study of border and mobility control in Europe", in de Goede M., Bosma E., Pallister-Wilkins P. (eds.), *Secrecy and Methods in Security Research: A Guide to Qualitative Fieldwork*, Londres: Routledge, 2019, p. 52-56.

[845] John Barlow, militant d'un internet indépendant du contrôle des États, et marqué par les théories libertariennes, est connu pour sa déclaration d'indépendance du Cyberespace, dont le passage suivant est le plus cité : « Gouvernements du monde industriel, vous géants fatigués de chair et d'acier, je viens du Cyberespace, le nouveau domicile de l'esprit. Au nom du futur, je vous demande à vous du passé de nous laisser tranquilles. Vous n'êtes pas les bienvenus parmi nous. Vous n'avez pas de souveraineté où nous nous rassemblons. » John Perry Barlow, « A Declaration of the Independence of Cyberspace », 8 février 1996 (en ligne : www.eff.org).

[846] « *L'espace numérique dispose de toutes les caractéristiques d'un espace lisse : fluidité, spontanéité, a-directionnel, sans forme et non cartographiable. "Dans l'espace strié on ferme une surface, et on la répartit suivant des intervalles déterminés, d'après des coupures assignées ; dans le lisse on se distribue sur un espace ouvert, d'après des fréquences et le long des parcours (logos et nomos)". Les espaces lisses sont des espaces libres, sans ordre ni juridiction, comme les déserts, glacés ou chauds, et les mers ; l'internaute est un nomade, un navigateur. Les espaces striés, quant à eux, sont des espaces conquis, partagés et exploités ; les stries sont celles que laisse dans la terre le labour des paysans. »* AUDREY, Hérisson, « Le cyberespace, cet espace de confrontation à part entière », *Stratégique*, 2017/4 (N° 117), p. 231-246. https://www-cairn-info.ezproxy.utc.fr/revue-strategique-2017-4-page-231.htm

[847] COELHO, Ophélie, *Géopolitique du numérique : impérialisme à pas de géants*, Ivry sur Seine : les éditions de l'Atelier, 2023, 272 p.

MHALLA, Asma, *Technopolitique : comment la technologie fait de nous des soldats*, Paris : éditions du Seuil, 2024, 288 p.

[848] MOREL, Camille, *Les câbles sous-marins*, Paris : CNRS éditions, 2023, 200 p.

[849] « Spatial : la souveraineté européenne menacée », *Le Monde*, 29/12/2022 https://www.lemonde.fr/idees/article/2022/12/29/spatial-la-souverainete-europeenne-menacee_6156017_3232.html

Or, comme on l'a dit, les États tentent de rétablir une forme de souveraineté dans ce milieu mouvant et pluriel[850]. Et de fait, envisager la projection d'un État sur un milieu numérique nécessite tout d'abord de repenser la définition d'un territoire et la forme que peut prendre ce type de milieu, d'où la nécessité de recourir à des notions et concepts permettant de le formaliser. Ainsi, le terme de cyberespace, venant de la science-fiction[851], est parfois utilisé au niveau stratégique et régalien, et au sein du milieu académique. Lui est parfois préféré celui de « datasphère ». Le terme de « datasphère » insiste sur sa représentabilité, lié à son ancrage physique (et donc cartographiable) : « la datasphère peut se concevoir comme la représentation d'un nouvel ensemble spatial formé par la totalité des données numériques et des technologies qui la sous-tendent, ainsi que de leurs interactions avec le monde physique, humain et politique dans lequel elle est ancrée. »[852]

Plus généralement, les description du cyberespace en font un milieu composé de 3 couches :

— Une première couche est formée par l'infrastructure physique (les ordinateurs, les box de fournisseur d'accès, disque dur, etc., les différents moyens de transmissions, câbles, les serveurs, les routeurs, les satellites, etc.). Elle est constituée par tous les périphériques d'accès et les infrastructures nécessaires à son fonctionnement et englobe les fournisseurs d'accès Internet, ainsi que les centres de données. Cette strate, de par sa dimension physique, est plus facilement localisable, et s'ancre clairement dans un territoire.

— Une seconde couche est qualifiée de couche logique ou logicielle. Elle est constituée de langage machine et de protocoles qui permettent aux ordinateurs de communiquer les uns avec les autres. Elle englobe donc tous les services permettant d'assurer la transmission de données entre un expéditeur et un destinataire.

Sachant que certains analystes divisent cette couche en 2 sous-couches :

— une couche de « l'infrastructure logique », qui « comprend tous les services qui permettent d'assurer la transmission des données entre deux points du réseau », et qui repose sur un commun (comme le protocole TCP/IP) et sur des services comme le routage, le nommage, ou l'adressage.

— une couche des applications, qui permet « à tout un chacun d'utiliser l'Internet sans rien connaître à la programmation informatique : Web, e-mail, réseaux sociaux, moteurs de recherche, etc.

---

[850] COUTURE, Stephane, TOUPIN, Sophie, What does the notion of "sovereignty" mean when referring to the digital?, *New media & society* 2019, Vol. 21(10) p.2305–2322 sagepub.com/journals-permissions

[851] C'est tout d'abord un auteur de science-fiction , William Gibson, écrivain phare du mouvement cyberpunk, qui serait à l'origine du terme. Dans un roman publié en 1983, le Neuromancien, il décrit un espace tridimensionnel, généré électroniquement, une matrice dans lequel les personnages entrent en se connectant par ordinateur. Le cyberespace peut être considéré comme une représentation mentale des données stockées au cœur des systèmes informatiques. Il décrit le cyberespace comme une « hallucination consensuelle vécue quotidiennement par des dizaines de millions d'opérateurs dans tous les pays »

[852] DOUZET Frédérick, « Du cyberespace à la datasphère. Enjeux stratégiques de la révolution numérique », *Hérodote*, 2020/2-3 (N° 177-178), p. 3-15. https://www.cairn.info/revue-herodote-2020-2-page-3.htm

— Enfin, la dernière strate est une couche sémantique ou cognitive en rapport avec le contenu informationnel. En clair, il s'agit de l'ensemble des messages passant par l'Internet (le contenu des conversations, des publications, etc.).

Pour préserver sa souveraineté, un État doit donc pouvoir maîtriser les réseaux, les communications électroniques et les données, publiques ou personnelles. En somme, il lui faut opérer une transposition des attributs de sa puissance dans le cyberespace. [853] Retrouver une souveraineté passe par des tentatives de reterritorialisation du Web[854], par des politiques de relance industrielle — par le soutien au cloud souverain, à la puissance de calcul (les supercalculateurs), l'IA, etc., par l'arme du droit ainsi que par une politique de cyberdéfense[855], quand bien même les opérations de « gendarme » du cyberespace, de garant de la sécurité et sureté des internautes mobilise un écosystème d'entreprises et d'acteurs privés. Sachant que les représentations de cette souveraineté, ses discours, les possibilités de les mettre en œuvre varient grandement en fonction des États. L'Europe n'a évidemment pas la même conception de la souveraineté que la Chine, la Russie ou des États africains.

Or l'espace humanitaire s'est construit en relation avec les souverainetés étatiques et ne peut donc qu'être affecté par ces évolutions. Pour rappel, l'espace humanitaire désigne un espace *symbolique* dont l'accès permet la réalisation d'une assistance fondée éthiquement, de façon indépendante et impartiale[856]. Pour rappel, on peut à nouveau citer la définition qu'en donne Rony Brauman : « L'espace humanitaire [est un] espace symbolique hors duquel l'action humanitaire se trouve détachée [de son] fondement éthique et qui se constitue à l'intérieur des repères suivants : accès, dialogue, indépendance, impartialité. Ceci implique d'une part la liberté de dialogue, la possibilité de parler librement avec les gens au service de qui on travaille, sans subir de pression systématique de quiconque. C'est une question élémentaire de dignité qui ne va pourtant pas d'elle-même. Il faut d'autre part la liberté de mouvement et d'évaluation des besoins, dans toute la mesure où les conditions pratiques le permettent, bien sûr. Condition importante pour éviter de devenir un instrument de propagande, un ornement dans la vitrine de tel chef de guerre ou telle faction ou groupe politique. » [857]

L'espace humanitaire garantit donc une liberté de mouvement et d'accès aux bénéficiaires et d'interaction et de dialogue avec les acteurs en place. Le préserver signifie s'assurer du maintien d'une relative autonomie face au contrôle de l'État, de son territoire et de ses

[853] DOUZET Frédérick, « La géopolitique pour comprendre le cyberespace », *Hérodote*, 2014/1-2 (n° 152-153), p. 3-21, https://www.cairn.info/revue-herodote-2014-1-page-3.htm
DOUZET, Frédérick, « Editorial, Du cyberespace à la datasphère. Enjeux Stratégiques de la révolution numérique », *Hérodote*, 2020/2 n° 177-178, p.3 -15, https://www.cairn.info/revue-herodote-2020-2-page-3.htm
[854] CATTARUZZA, Amael, « Frontières du cyberespace. Elements de réflexion sur la territorialisation d'Internet, in : DANET, D, CATTARUZZA, A,(dir.), *La Cyberdéfense, quel territoire, quel droit?,* Economica, 2014, p. 21-33
[855] MHALLA, Asma, *Technopolitique : comment la technologie fait de nous des soldats*, Paris : éditions du Seuil, 2024, 288 p.
[856] THURER, Daniel, "La pyramide de Dunant : réflexions sur l'"espace humanitaire", *Revue internationale de la Croix-Rouge*, Vol. 89, n° 865, Sélection française 2007, p. 51-66
[857]BRAUMAN,Rony, *Humanitaires, le dilemme, Entretien avec Philippe Petit*, Paris : Textuel, 1996, p. 43.

populations. Cet espace n'est pas donné : il est mouvant et contextuel. Il dépend du statut des ONG et il reste le fruit du rapport de pouvoir et de négociations[858].

Or, on assisterait à un éclatement des souverainetés, entrainant une complexification de l'espace humanitaire. Ce dernier est maintenant discuté avec différents groupes d'acteurs : des acteurs étatiques certes, mais aussi des groupes armés non étatiques, des groupes « terroristes » ou groupes indépendantistes, voire des groupes de hackeurs. Sa défense serait-elle plus difficile à garantir ? Pour de nombreux acteurs de la solidarité internationale, cela est indéniable. On assisterait à une réduction de l'espace humanitaire, ce qui se traduit par des difficultés accrues pour accéder au terrain, notamment pour des motifs sécuritaires du fait d'une multiplication d'attaques armées ciblant spécifiquement des humanitaires. De surcroit, la réduction de l'espace humanitaire va de pair avec une perte d'indépendance des ONG, découlant d'un regain de contrôle des ONG par les États sur leur territoire[859].
On partira de ce constat pour faire l'hypothèse que la réduction de l'espace humanitaire complexifie le contrôle de l'information et donc la protection des données des ONG. Cette hypothèse soulève un certain nombre de questions. En effet, comment l'exercice de la souveraineté des États se traduit-il sur le plan informationnel ? Dans quels cas le partage de données avec des États est-il perçu comme un risque pour les bénéficiaires en matière de vie privée ? Comment les ONG y font-elles face ? Comment négocient-elles ce qui peut être qualifié d'espace humanitaire informationnel et numérique ?
Notre troisième chapitre tentera de donner de premiers éléments de réponse à ces questions. En clair, il sera consacré aux échanges de données avec des acteurs étatiques. Ces derniers ont lieu tout le long d'un programme humanitaire, on se concentrera donc sur les échanges de données entre les ONG et les « États hôtes ». Il faut donc décrire les différents flux et partages d'informations existants. Il faut revenir sur la façon dont ils sont perçus, comme étant légitimes ou comme facteur de risque, notamment s'ils sont associés à différentes formes de violence d'État. Notre hypothèse est qu'une partie de ces échanges et circulations d'information met en jeu l'indépendance des ONG et qu'il existe une tension entre confidentialité et accès à un terrain de crise. Et dans ce cas, nous chercherons à déterminer comment les humanitaires ont la possibilité de s'y opposer, ou non. Pour ce faire, les ONG tendent à mettre en avant l'importance des principes humanitaires, ou à en appeler aux privilèges et immunités d'organisations internationales. Sachant que la numérisation de l'aide complexifie d'autant plus leur application, comme on le verra au sujet de l'informatique en nuage.

---

[858] Coordination Sud, « Protéger et garantir un espace humanitaire pour les populations civiles et les acteurs et actrices de la solidarité internationale, stratégie humanitaire de la République française », Novembre 2023 https://www.coordinationsud.org/wp-content/uploads/2023_Recommandations-SHRF-commission-humanitaire_VF.pdf
AUDET, François, « L'acteur humanitaire en crise existentielle. Les défis du nouvel espace humanitaire », *Etudes internationales*, vol. 42, no 4, 2011, p. 447-472

[859] "Sous l'influence d'intérêts politiques et économiques, voire de bureaucraties autoritaires, la surveillance et le contrôle d'activités humanitaires dans les pays frappés par les crises ont considérablement augmenté. Sans aucun doute, selon l'expérience de MSF, "nous faisons face à une augmentation des contextes où les États font valoir leur souveraineté, nous empêchant l'accès aux terrains d'intervention, complexifiant aussi la conduite des opérations et, dans certains cas, entravant notre mission de soignants. Dans la pratique, cela se traduit souvent par un "contrôle administratif accru", ainsi que "des négociations complexes pour MSF concernant l'accès aux populations". MCLEAN, Duncan, « Les conséquences humanitaires d'une réaffirmation de la souveraineté de l'État », *Alternatives humanitaires*, n°9, 2018, https://www.alternatives-humanitaires.org/fr/2018/11/13/les-consequences-humanitaires-dune-reaffirmation-de-la-souverainete-de-letat/
MCLEAN, Duncan, HOFMAN, Michel, » Droit international humanitaire, souveraineté des États et érosion du consensus humanitaire : la fin de l'humanitarisme ? », *Alternatives humanitaires*, 2023 https://www.alternatives-humanitaires.org/fr/2023/07/22/droit-international-humanitaire-souverainete-des-etats-et-erosion-du-consensus-humanitaire-la-fin-de-lhumanitarisme/

De surcroit, les Clouds et plus globalement le processus de numérisation de nos sociétés participe aussi à la recomposition des souverainetés étatiques. Ce phénomène est aussi lié à l'entrée en scène d'une série d'acteurs non étatiques, des entreprises évidemment, comme les GAFAM, mais aussi d'autres groupes plus informels, comme des hackers. L'implication de cybercombattants dans des conflits contemporains s'inscrit dans un long mouvement de contestation du monopole de la violence des États du fait de la multiplication de conflits intraétatiques — à l'encontre de groupes terroristes par exemple — et l'implication d'acteurs privés dans la conduite de la guerre, comme des hackers donc.

Nos deux chapitres suivants 4 et 5 sont donc liés aux répercussions en matière de vie privée de ces formes de conflictualités et de leurs répercussions dans l'espace numérique. Le chapitre 4 sera consacré aux conséquences du contre-terrorisme sur la protection des données des ONG. Le sujet a déjà fait l'objet d'une riche littérature scientifique. On se concentrera pour notre part sur un sujet qui nous a paru être peu traité : les implications en matière de vie privée pour les ONG de la lutte contre le financement du terrorisme et leurs répercussions numériques. Différentes coalitions de cause se sont formées pour faire entendre la nécessité de ménager une exception humanitaire au sein du cadre juridique formé par les mesures de contre-terrorisme. Enfin, dans le chapitre 5, on s'intéressera à d'autres menaces au sein de l'espace numérique : les cyberattaques. On assiste en effet à une sécuritisation du cyberespace par les États. Réagir aux cyberopérations devient un enjeu de défense des intérêts nationaux, et maintenir une présence régalienne forte sur le terrain numérique est présenté comme une nécessité. Les ONG sont également victimes des nouvelles formes de conflictualités et des « cyber-opérations » liées aux « guerres informationnelles ». Et les ONG tentent alors de préserver l'espace humanitaire — et de défendre leur liberté d'agir et d'intervenir auprès des populations sans être pris pour cible, tout en défendant la vie privée des bénéficiaires.

## Chapitre 03 — Protection des données et ONG face à la recomposition des souverainetés, des « États faillis » à l'extraterritorialité de l'informatique en nuage

### Introduction de chapitre

Autour de l'écosystème humanitaire gravitent un certain nombre d'acteurs avec qui les ONG interagissent : des Casques bleus et organisations onusiennes, des bailleurs de fonds, des acteurs étatiques relevant d'une échelle locale ou nationale, des militaires, des membres de services de sécurités et des forces de l'ordre, des entreprises, des prestataires techniques, des groupes armés non étatiques, etc. D'où une forte circulation d'information pour coordonner l'ensemble des membres précités. Sachant qu'on se concentrera ici sur les échanges de données avec des acteurs étatiques. Ces derniers ont lieu tout le long d'un programme humanitaire, de leur élaboration jusqu'à la toute fin d'une mission (des audits peuvent encore être envoyés à des bailleurs gouvernementaux). Or il existerait une pression croissante à communiquer aux acteurs étatiques des données détenues par des ONG, comme nous l'a confié un de nos enquêtés : « *on a une pression de plus en plus importante pour fournir de plus en plus de données, désagrégées ou non, ça dépend du type de demande, ce sont des demandes qui peuvent arriver à différents niveaux, qui peuvent être inscrits dans un contrat pour du financement, ça peut être des demandes qui peuvent être Adhoc ou encore des demandes par exemple le Royaume-Uni, en échange du financement nous a demandé tous la liste de tous les Syriens qu'on avait parmi les bénéficiaires.* »[860] Ce type d'échange est lié à une pression accrue à plus de transparence et de redevabilité émanent de bailleurs, comme l'a très bien démontré Larissa Fast[861]. Elles proviennent également d'« États hôtes ». À ce sujet, les mécanismes de partages d'information sont multiples. Une ONG peut transmettre des données à l'hôpital local partenaire, qui peut éventuellement les envoyer au ministère local de la Santé. Une ONG doit parfois tout simplement communiquer aux gouvernements en place la liste des personnels qu'elle emploie, voire des bénéficiaires de ses programmes d'aide. Somme toute, les requêtes d'acteurs étatiques sont parfois perçues comme étant tout à fait légitimes. Dans un rapport sur ce sujet, Lynda Raftree liste les partages d'informations qu'elle qualifie de « légitime » : le partage de données avec un gouvernement dans le cadre d'un programme social ; le partage de données afin d'éviter la duplication des interventions entre les ONG et les actions gouvernementales, par exemple lorsqu'un État assiste une population précédemment aidée par des agences humanitaires ; les échanges de données relatifs aux soupçons de corruption concernant des ONG, le gouvernement souhaitant dans ce cas procéder à un audit ; les échanges de données permettant de respecter les recommandations mondiales du Groupe d'action financière sur le blanchiment de capitaux (GAFI)[862]. Cela dit, nous verrons dans la suite de la thèse que l'action du GAFI pose lourdement question en matière de protection des données. Ce qui représente pour les ONG une « ligne rouge » en matière de requête de données de la part d'acteurs étatiques est donc fluctuant et dépend des rapports de pouvoirs en place. Car comme l'écrivent Sean Martin Mcdonald et Ben Gansky : « L'échange et l'utilisation de données, en tant qu'acte, tout en contenant un échange "matériel", sont indissociables de l'économie politique et des relations de pouvoir qui définissent le bien-fondé de cet échange. »[863] Afin d'approfondir ce sujet, on reviendra sur des exemples concrets en tentant de déterminer les cas où des ONG jugent nécessaire de

[860] Entretien n°7, OI2, DPO, 11/12/2019

[861] FAST, Larissa, "data sharing between humanitarian organisations and donors: toward understanding and articulating responsible practice", NCHS paper, 2022 https://www.humanitarianstudies.no/wp-content/uploads/NCHS-paper-06-April-2022-Data-sharing-between-humanitarian-organisations-and-donors.pdf

[862] RAFTREE, Lynda, KONDAKHCHYAN, Anna, "Responsible data sharing with governments", CaLP, 10/03/2021https://www.im-portal.org/help-library/case-study-responsible-data-sharing-with-governments-0

[863] "The exchange and use of data, as an act, while containing a 'material' exchange, is indistinguishable from the political economy and power relationships that define the appropriateness of that exchange"MCDONALD, Sean Martin, GANSKY, Ben, "Data as representation, Conference on the Valuation of Data", IARIW-CIGI, November 2023 https://iariw.org/wp-content/uploads/2023/10/IARIW-CIGI-2023-McDonald.pdf

conserver une forme de confidentialité. Mais les humanitaires sont inégaux face aux requêtes des États. On pense plus spécifiquement au fait que des organisations internationales comme l'UNHCR ou le CICR sont dotées d'outils dont les ONG ne disposent pas : les privilèges et immunités. Cependant, il ne faut pas oublier qu'appliquer ces derniers à l'espace numérique ne va pas de soi, surtout dans le cas de l'informatique en nuage.

## Section 1 — Souverainetés étatiques, accès au terrain et échanges de données

Il existe divers mécanismes de partage de données entre ONG et acteurs étatiques. Larissa Fast en donne un premier aperçu : « Les mécanismes de partage des données sont formels (contrats et modèles de rapport) et informels (questions lors des visites sur place, par courrier électronique et par téléphone). Ils sont également intentionnels et non intentionnels. Les mécanismes formels et informels impliquent une intentionnalité de partage. Mais les données sont également abandonnées. Les programmes humanitaires prennent fin et les données peuvent ou non être correctement détruites. La violence et l'insécurité peuvent contraindre les humanitaires à partir, laissant potentiellement derrière eux des données sensibles, sans parler des collègues. Le retrait en 2021 de l'armée américaine et de ses alliés en Afghanistan n'est qu'un exemple parmi d'autres[864]. Cette situation soulève des questions éthiques et pratiques quant aux risques que ces données abandonnées font peser sur les personnes laissées sur place. »[865]

Comme cette citation le suggère, la communication d'information avec des acteurs étatiques est de prime abord très formalisée et fait l'objet de divers encadrements juridiques. Ainsi, pour les transferts de données à l'international, le RGPD impose une série de mesures d'encadrement, en fonction du niveau de protection du pays concerné[866]. Cela permet d'établir les responsabilités de chaque acteur et de préciser les finalités des traitements de données. Et dans le cas où le pays ne présente pas un niveau de protection équivalent, les ONG sont tenues de prendre des mesures supplémentaires de réduction de risque, en faisant ratifier par exemple des clauses contractuelles types. Ces dernières sont établies par différentes autorités de protection des données[867]. Et elles peuvent être formalisées lors de la validation d'un accord de siège (traduction de l'expression « Host country agreement »)[868],

---

[864] Les talibans avaient récupéré les bases de données personnelles et biométriques (y compris des empreintes digitales) de nombreux Afghans, cocréées ou cofinancées par les gouvernements étrangers avant leur départ. "Afghanistan : les systèmes de données biométriques mettent en danger de nombreux Afghans", *Human Rights Watch*, 30/03/2022 https://www.hrw.org/fr/news/2022/03/30/afghanistan-les-systemes-de-donnees-biometriques-mettent-en-danger-de-nombreux

[865] "The mechanisms for sharing data are formal (contracts and reporting templates) and informal (queries at site visits, over email and telephone). They are also intentional and unintentional. The formal and informal mechanisms imply an intentionality to sharing. But data are also abandoned. Humanitarian programs close, and data may or may not be properly destroyed. Violence and insecurity may force humanitarians to depart, potentially leaving behind sensitive data-not to mention colleagues. The 2021 withdrawal of the U.S. military and its allies in Afghanistan is just one example. This raises ethical and practical questions about the risks these abandoned data pose to the people left behind." FAST, Larissa,"Governing Data: Relationships, Trust & Ethics in Leveraging Data & Technology in Service of Humanitarian Health Delivery", *Daedalus* 2023, 152 (2), p. 125–140.

[866] European data protection supervisor, "Transfers internationaux",https://www.edps.europa.eu/data-protection/data-protection/reference-library/international-transfers_fr

[867] Cartong, « Les accords de partage de données, boîte à outils gestion responsable de données », https://cartong.pages.gitlab.cartong.org/learning-corner/en/3_legal_contract_RD/3_5_data_transfer_sharing

[868] UNHCR, "Working with the host government", 17/04/2024 https://emergency.unhcr.org/coordination-and-communication/working-others/working-host-government

UNHCR, mémorandum et protocole d'accord avec les partenaires, 12/01/2024 https://emergency.unhcr.org/fr/coordination-and-communication/travailler-avec-les-autres/m%C3%A9morandums-et-protocoles-d%E2%80%99accord-avec-les-partenaires

soit des accords avec les gouvernements en place fixant les conditions d'intervention : « *Souvent, on va faire une sorte d'accord, hein, quand même, de MOU ou de "data sharing agreement". On essaye en tout cas d'encadrer. On essaye dans le meilleur des cas d'avoir une trace écrite quand même de ce qu'on fait, de plus en plus pour tracer les échanges. On essaye de rappeler les grands principes en matière de protection des données, toujours*. »[869]

Des « principes opérationnels conjoints » [870]peuvent également être entérinés. Ces derniers documents ne sont en revanche pas contraignants. Ils ont pour première finalité la garantie de l'espace humanitaire et la reconnaissance par différentes autorités locales et des belligérants du caractère impartial de l'aide[871]. Les "principes opérationnels conjoints" peuvent également comprendre des annexes précisant les modalités de partage de données. Par exemple, les « principes opérationnels conjoints » signés pour une mission au Yémen [872] mentionnent — sans se référer au RGPD — l'ensemble des données pouvant être échangées avec les acteurs locaux, en particulier les autorités : des cartes d'identité des travailleurs humanitaires, les permis des véhicules, les plans des programmes (villages, date et activités), la liste de tout le personnel international et local (titre, rang hiérarchique, passeport, etc.). Le document énumère aussi les types d'informations ne pouvant pas être partagées : la liste des bénéficiaires, les inventaires des équipements, les contrats des employés locaux et la liste des contacts du personnel de l'ONG (numéros de téléphone et adresse mail).

La protection juridique qu'offrent les documents qu'on a mentionnés a cependant plusieurs limites. Il s'agit de documents non contraignants. Et surtout, communiquer certaines données peut constituer une obligation légale selon le droit local, tout en contrevenant au RGPD. C'est ce que nous a confié un enquêté : « *Et parfois on a des pays où on intervient, on a une demande de l'État de transférer l'ensemble des données, mais ça c'est totalement illégal. C'est illégal par rapport à notre loi française et au RGPD, mais c'est totalement légal dans le pays où on intervient. Et du coup ça crée forcément un risque, pour nos staffs nationaux, et expatriés*. »[873]

---

[869] Entretien n° 86, ONG22 DPO, 27/10/2022

[870] "these multilateral agreements are publicly accessible, but many of the bilateral agreements under which digital humanitarian interfaces are being developed and deployed are not. This is for a range of reasons, including the fact of some of these agreements taking informal forms—that of a memorandum of understanding, for instance, commonly seen as a "more flexible, lower-profile alternative" to a formal treaty" JOHNS, Fleur, #Help Digital Humanitarianism and the Remaking of International Order, Oxford University Press, 2023, p.181

[871]« De tels accords peuvent augmenter la probabilité que les organisations travaillant dans une région opèrent conformément à une compréhension commune des JOP, ce qui, à son tour, peut aider à la coordination des réponses humanitaires et, en fin de compte, conduire à de meilleurs résultats pour les populations touchées par les conflits. »« Such arrangements can increase the likelihood that organizations working in a region operate in accordance with a common understanding of the JOPs, which, in turn, can help in the coordination of humanitarian responses and ultimately lead to better outcomes for conflict-affected populations. »
BARBER, Martin, BOWDEN, Mark, « Ensuring better outcomes for civilians in armed conflict, what role for humanitarian principles? » Chathamhouse, December 2023 https://www.chathamhouse.org/sites/default/files/2023-12/2023-12-13-ensuring-better-outcomes-civilians-armed-conflict-barber-bowden.pdf

[872]" Joint Operating Principles of the Humanitarian Country Team in Yemen, Annex 4 : Information sharing guidance Document for INGOs working in Yemen", 2017, https://www.humanitarianlibrary.org/resource/annex-4-information-sharing-guidance-document-ingos-working-yemen
« Les principes opérationnels communs (JOP) fournissent des orientations aux humanitaires sur la manière de naviguer dans leur environnement opérationnel. À bien des égards, il s'agit d'un ensemble de positions communes, d'orientations existantes et de cadres juridiques que la communauté humanitaire s'est engagée à respecter afin d'assurer la cohérence de sa position vis-à-vis des parties prenantes extérieures. L'élaboration des JOP ne doit être considérée que comme le début d'un processus qui comprendra également des efforts structurés pour sensibiliser les partenaires humanitaires à la manière dont ils doivent être mis en pratique.
En fonction des domaines dans lesquels les principes humanitaires risquent le plus d'être compromis, les JOP peuvent être spécifiques et se concentrer sur une partie prenante ou une zone géographique particulière, ou bien couvrir l'ensemble d'une intervention humanitaire. » « Humanitarian access working group toolkit », Norwegian Refugee council, https://www.protecthumanitarianspace.com/toolkits/humanitarian-access-working-group-toolkit/5-implementing

[873] Entretien n° 86, ONG22,DPO, 27/10/2022

Or il existe peu de ressources pour « combler » les incertitudes produites par ce type de contradiction entre deux systèmes juridiques. Ceci résulte entre autres du fait d'un manque de jurisprudence et d'accompagnement des autorités de protections nationales (cf. chapitre 2). Pour régler ces conflits, il est parfois à dessein choisi d'enfreindre la loi locale : « *On fait des cartes, pour identifier les personnes atteintes de maladie. On ne le fait pas foyer par foyer, on veut pas ce genre de carte, ça peut tomber dans de mauvaises mains. Il y a des gens qui ne déclarent pas leur tuberculose, alors que le reporting est obligatoire. Si on fait ce type de carte, le ministère de la Santé va s'en rendre compte, et on va les exposer*. »[874]

Une autre solution consiste à anonymiser les données, bien que cette option comprenne des limites : « *Certains projets sont en partenariats avec des ministères, et là c'est une autre problématique qu'on essaye de mettre en place, c'est l'anonymisation des données et plus on avance sur la problématique, plus on se rend compte que c'est pratiquement inaccessible, souvent c'est entendu comme le retrait des informations identifiantes des bases de données, mais ça va beaucoup plus loin que ça*. »[875] Et surtout, anonymiser les données ne contente pas toujours les acteurs étatiques : « *Ça doit être très clair le type de données qu'on échange, sachant que les "best practice" c'est de se limiter aux données anonymes. Mais ils peuvent accepter qu'on travaille seulement s'ils savent qui l'on aide. Il y a un équilibre délicat entre la protection des bénéficiaires et la possibilité de les aider. »* [876] Et si communiquer des données anonymisées des personnes secourues est admissible, le partage des listes des bénéficiaires[877] constitue une ligne rouge que les ONG refusent généralement de franchir[878]. Cela ne signifie cependant pas que les États ne puissent pas avoir accès à ces données via d'autres moyens, grâce à diverses cyber-opérations intrusives (cf. chapitre 5).

Mais pour certains humanitaires, ces sollicitations peuvent, dans une certaine mesure, sembler « légitimes » : *« Vous devez nous fournir la liste complète de vos employés, la liste des personnes que vous aidez, la liste des bénévoles, et ce n'est pas facile parce que, bien sûr, sous un certain aspect, ils sont absolument habilités à partager ces informations. »*[879] Un autre enquêté nous a également fait part du fait que « *Bien avant le RGPD, je lui dis, bah écoute, il faut que vous m'expliquiez des choses, et notamment l'identité des gens, et ce gars me dit, on est payé par les gouvernements, si un gouvernement nous demande des informations qu'on a sur ses ressortissants, on ne peut pas lui refuser*. »[880] Et donc partager ou non les listes dépend du degré de confiance aux autorités locales : *« Et on doit se poser la question : est-ce qu'on peut faire confiance au gouvernement ou est-ce qu'on doit être plus prudents ? Ça peut être difficile de trancher. Il y a eu des cas où on a décidé de ne pas continuer à cause de manque de*

[874] Entretien 17, ONG6, DPO, 31/01/2020
Encore aujourd'hui dans certains pays la tuberculose est une maladie particulièrement stigmatisée.
https://www.emro.who.int/rc69-marketplace/Study_on_TB_stigma_Sudan_fr.pdf?ua=1&ua=1
[875] Entretien n° 88, ONG24, DPO,15/11/2022
[876] Entretien n° 87, ONG23, DPO, 10/11/2022
[877] ces listes sont établies afin de mieux cibler un programme (distributions alimentaires ou cash transfert), ou sont relatives à des programmes d'enregistrement en vue de formalités administratives (le cas de l'UNHCR). Et ces dernières peuvent donc contenir de nombreuses informations personnelles, voire sensibles : nom, genre, âge, facteurs de vulnérabilités (et donc des données de santé, ethnique, informations relatives à l'orientation sexuelle, etc.).
[878] Entretien n° 38, 0I4, 03/06/2020
[879] « you have to give us your full list of employee, the list of people you are helping, the list of volunteers, and it is not easy because of course under a certain aspect they are absolutely intitled to share this information. »
Entretien n° 38, 0I 4,03/06/2020
[880] Entretien n° 28, ONG8, ingénieur, 09/04/2020

*confiance, on a décidé de ne rien faire*. »[881] Cette confiance peut varier selon le type d'acteur à qui s'adresse une ONG au sein d'un État, et comme un enquêté en fait la remarque : « *c'était un défi non seulement de partager des informations, mais aussi de trouver un moyen structuré de s'adresser aux personnes qui demandent des informations, qui sont souvent des parties différentes du gouvernement*. »[882]

Mais communiquer ce type de liste ne va pas sans risques. Les autorités peuvent s'en servir pour cibler des minorités persécutées. Et les ONG s'inquiètent aussi de tentatives de « favorisation » de tel ou tel groupe social par l'ajout sur ces listes de noms de bénéficiaires en fonction de critères qui ne sont pas les leurs. Dans certains cas, les gouvernements peuvent même s'efforcer d'imposer leurs propres listes de bénéficiaires. Tout ceci traduit des tensions existantes entre des principes humanitaires, comme l'impartialité, et la nature des structures sociales et/ou religieuses locales [883]. Human Right Watch a documenté différents exemples de ce genre au Yémen. D'après l'organisation, ce type de sollicitation provient tout aussi bien de groupes non étatiques, les Houthis, que des autorités centrales, cherchant à reprendre le contrôle de leur territoire et à imposer les groupes sociaux leur étant favorables[884].

Il va sans dire que ces requêtes sont nettement moins formalisées et sortent clairement du cadre des mémorandums d'entente : « *et si certaines demandes illégitimes peuvent être formulées par des voies officielles, d'autres s'apparentent clairement à des demandes forcées ou à de la coercition arrivent que les accords de partage des données entre les organisations humanitaires et les autorités publiques entraînent des failles dans la protection des données*. »[885]

Ainsi, les négociations informelles prennent parfois le pas, limitant la portée contraignante des accords. Et de fait, comme le remarque Sean Mcdonnald les mémorandums d'entente ne sont pas dépourvus de caractère politique : « Parmi les accords avec les pays hôtes auxquels nous avons accès, les dispositions relatives au partage des données — notamment avec les services de sécurité — sont monnaie courante. La politisation des accords avec les pays hôtes n'est pas nouvelle, mais il est important de reconnaître que toute promesse faite par une organisation humanitaire — en particulier en matière de confidentialité des données, de sécurité ou d'éthique — est limitée par les intérêts du gouvernement. »[886]

Et pour tout dire, comme le dénonce une de nos enquêtés, ces derniers peuvent être, dans certains cas, signés strictement « pour la forme » : « *Je dois taper du poing dans des réunions avec l'ONU. Je m'en fous du contrat, ce qui compte c'est la protection des gens, au-delà des*

---

[881] Entretien n° 86, ONG 22, DPO, 27/10/2022

[882] « it was a challenge not just share information, but coming with structured way to address, the people who are demanding information, who are often different part of government. » Entretien n38, OI 4, Deputy Head of Operations Unit,03/06/2020

[883] NIMKAR, Ruta, LABS, Meraki, "Humanitarian cash and social protection in Yemen", Calp Case Study, 2021https://www.calpnetwork.org/wp-content/uploads/2021/01/CaLP-Yemen-Case-Study-WEB-1.pdf

[884] Human rights watch, "Deadly consequences, obstruction of aid in Yemen during Covid19", 14/09/2020 https://www.hrw.org/report/2020/09/14/deadly-consequences/obstruction-aid-yemen-during-covid-19#_ftn83

[885] RAFTREE, Linda, « Etude de cas : partage responsable des données avec les gouvernements », CaLP, 2021 https://www.calpnetwork.org/wp-content/uploads/2021/03/CaLP-Case-Study-Responsible-Data-Sharing-with-Governments_FR.pdf

[886] "Among the Host Country Agreements that we can access, data sharing provisions – especially with security services – are commonplace. The politicization of Host Country Agreements isn't new, but it's important to recognize that any promise made by a humanitarian organization – particularly about data privacy, security, or ethics – is bounded by the interests of the government. "McDonald, Sean," From Space to Supply Chains: A Plan for Humanitarian Data Governance", 12/08/ 2019 https://ssrn.com/abstract=3436179

*clauses des country host agreement. Ils font du chantage pour obtenir des data, il y a des distorsions des obligations légales pour faire du "background check" sur des bénéficiaires au Yémen. Et on manque de compétences pour gérer les demandes des États hôtes. (…) On n'est pas comme une boite, on n'a pas choisi l'entité avec qui on transfère les données, on est dans des pays où rien ne fonctionne avec des administrations corrompues*. »[887]

Mais refuser de communiquer de telles listes peut être parfois difficile, surtout en cas de fortes pressions de la part des acteurs étatiques. Et, comme le note un journaliste du journal *The New Humanitarian* : « La question de la manipulation des listes de bénéficiaires et/ou des pressions exercées pour partager ces listes est particulièrement préoccupante, et les cas impliquant le recours à la violence et à la coercition dans les points de distribution de l'aide ont augmenté en 2019. »[888] Les petites ONG ou les ONG locales seraient les plus soumises à ce type de pression : « Une autre agence d'aide en charge d'un grand nombre de projets a déclaré que les autorités locales exerçaient une pression énorme sur le personnel national le plus vulnérable de leur agence, dont les proches sont des cibles potentielles de représailles, pour qu'il leur remette des listes confidentielles de bénéficiaires de l'aide et qu'il supprime des noms ou en ajoute de nouveaux. » [889] Ajoutons qu'un autre moyen d'obtenir ces listes consiste à imposer des partenaires locaux : « Le ministère des Affaires étrangères, en collaboration avec le ministère des Affaires sociales, fournit une liste de partenaires préapprouvés qui ne comprend que des organisations qui ont été contrôlées et approuvées par les services de renseignement syriens. Les services de sécurité syriens font régulièrement appel à ces partenaires locaux et peuvent, selon les humanitaires, avoir accès à leurs listes de bénéficiaires et à leurs programmes à tout moment. » [890] Ce dernier point peut donc compliquer l'agenda de localisation de l'aide (qui constitue pour rappel à déléguer plus de pouvoir aux ONG locales).

Enfin est-il possible d'établir un lien entre partage de données et accès au terrain ? On ne dispose pas de témoignage direct d'une expulsion d'une ONG par un gouvernement du fait d'un refus de partage d'informations. Un enquêté appartenant à une OI nous assure qu'il n'a pas connaissance d'un tel événement : « *A ma connaissance j'ai pas entendu parler d'un refus d'échange de données qui nous aurait emmenés à être renvoyé du pays, donc ça reste on va être embêtés, certains pays vont essayer de nous montrer que c'est quand même eux qui décident, mais à ma connaissance lorsqu'on a des demandes de données qu'on refuse… effectivement il y a négociation, on explique, et puis au final ça se passe assez bien, de ce que*

---

[887] Entretien n° 83, ONG1, DPO, 14/10/2022

[888] "The issue of the manipulation of beneficiary lists and/or pressure to share these lists is of particular concern, and cases involving the use of violence and coercion at aid distribution points have increased in 2019." SLEMROD, Annie, "UN experts : Uptick in Houthi obstacles to Yemen aid delivery", *The New humanitarian*, 03/03/2020
https://www.thenewhumanitarian.org/news/2020/02/03/Yemen-Houthis-aid-worker-safety

[889] "Another aid agency in charge of a large number of projects said that authorities at the local level put huge pressure on their agency's more vulnerable national staff, whose relatives are potential targets of retaliation, to hand over confidential aid recipient lists and to delete names or add new ones." Human rights watch, Deadly consequences, obstruction of aid in Yemen during Covid19, 14/09/2020
https://www.hrw.org/report/2020/09/14/deadly-consequences/obstruction-aid-yemen-during-covid-19#_ftn83

[890] "The Ministry of Foreign Affairs, in collaboration with the Ministry of Social Affairs, provides a list of preapproved partners that includes only organizations that have been vetted and approved by Syrian intelligence branches. The Syrian security services regularly engage these local partners and can, according to the humanitarians, have access to their beneficiary lists and programming at any point." HALL, Natasha, "The implication of the UN Cross-Border Vote in Syria", *CSIS,* 04/06/2021
https://www.csis.org/analysis/implications-un-cross-border-vote-syria

*j'en sais*. » [891] Il est toutefois important de noter que cet enquêté travaille pour une organisation internationale, bénéficiant de privilèges et d'immunité, facilitant les négociations avec les États. Et, cette possibilité est évoquée dans des enquêtes du Conseil de sécurité de l'ONU sur le blocage de l'aide au Yémen : « Certains acteurs humanitaires ont indiqué au groupe d'experts qu'ils s'étaient vu refuser l'accès à certaines zones ou l'autorisation de voyager parce qu'ils avaient refusé de partager des informations sur les bénéficiaires ou des informations personnelles sur leur personnel national. » [892] En outre, il existe plus généralement un dispositif de l'OCHA servant à centraliser les données sur les « accidents d'accès » [893]. Un rapport de ce type concernant l'Afghanistan recense ainsi, sur un total de 137 accidents, 23 demandes de liste de personnel d'ONG et de données sensibles, 22 « accidents » relatifs à des délais dans la signature d'accords-cadres, 10 sur la sélection des bénéficiaires, etc. [894]

Pour conclure, les différents exemples qu'on a évoqués découlent en partie d'une volonté de maintenir une forme de contrôle sur des ONG dans des contextes où l'espace humanitaire est fortement mis en cause. Cela est par exemple le cas en Syrie ou au Yémen. Autre cas de figure symptomatique : les zones dans lesquelles des groupes armés non étatiques et des acteurs gouvernementaux se discutent le contrôle d'un territoire. Enfin, on a vu que partager des listes de bénéficiaires est donc considéré comme une ligne rouge pour bien des ONG. Il existe certes différentes modalités pouvant encadrer les échanges de données. Cependant, comme nous le rappelle Sean Martin Mcdonald, les mémorandums d'ententes et les autres accords s'inscrivent dans des rapports de pouvoirs dépassant le cadre contractuel initial[895]. Négocier ce type de requête relève de l'ordre de l'informel, et les ONG disposent de ressources inégales.

## Section 2 — Immunités et privilèges des organisations internationales humanitaires, un outil de protection des données ? Le cas de l'UNHCR et du CICR

Pour contrer ce qui leur parait parfois constituer des « ingérences informationnelles », les organisations humanitaires ne disposent en effet pas des mêmes ressources, selon qu'il s'agit de petites ONG locales, d'ONG internationales occidentales. Sur ce point, la résolution d'Amsterdam relative à la protection des données dans l'humanitaire, adoptée en 2015 lors

---

[891] Entretien n° 93, OI2, DPO, 02/06/2022

[892] « Some humanitarian actors reported to the Panel that they had been denied access to certain areas or denied travel authorization because they had refused to share information on beneficiaries or personal information about their national staff. » GUNARATNE, Dakshinie Ruwnathika, HIMMICHE, Ahmed, THOMPSON, Henry, TOUGAS, Marie-Louise, PAES, Wolf-Christian, "Final report of the Panel of experts on Yemen", 27/12/2019 https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2020_70.pdf

[893] « OCHA développe des outils et fournit des conseils aux coordinateurs humanitaires et aux équipes humanitaires nationales sur la manière de traiter les questions liées à l'accès, y compris l'engagement humanitaire avec les groupes armés non étatiques et l'adhésion aux principes humanitaires. Nous avons également mis au point un cadre de suivi de l'accès et d'établissement de rapports, comprenant une base de données et un manuel, basé sur une classification des contraintes d'accès afin d'améliorer la collecte et l'analyse des données, et d'informer les politiques et l'accès dans les réponses sur le terrain. » ; "OCHA develops tools and provides guidance to Humanitarian Coordinators and Humanitarian Country Teams on how to address access-related issues, including humanitarian engagement with non-State armed groups and adherence to humanitarian principles. We have also developed an Access Monitoring and Reporting Framework, including a database and handbook, based on a classification of access constraints for better data collection and analysis, and to inform policy and access in responses on the ground."
https://www.unocha.org/humanitarian-access

[894] "Humanitarian Access snapshot dashboard", OCHA, january 2024 https://response.reliefweb.int/afghanistan/humanitarian-access-snapshot

[895] MCDONALD, Sean, "From Space to Supply Chains: A Plan for Humanitarian Data Governance", 12/08/ 2019 https://ssrn.com/abstract=3436179

de la 37e conférence des autorités de protection des données, est d'ailleurs très claire. On y lit en effet que : « Les organisations humanitaires ne jouissant pas de privilèges et d'immunités peuvent subir des pressions pour fournir des données collectées à des fins humanitaires aux autorités souhaitant utiliser ces données à d'autres fins (par exemple le contrôle des flux migratoires et la lutte contre le terrorisme). »[896] Logiquement, d'après cette citation, les privilèges et immunités pourraient contribuer à la protection des données des bénéficiaires. Le chercheur Ben Hayes va dans le même sens et souligne que : « Les gouvernements peuvent également demander des données directement aux organisations humanitaires, voire affirmer leur compétence ou les saisir contre leur gré. Les organisations qui bénéficient de privilèges et d'immunités ont des règles bien établies pour traiter les demandes des gouvernements et peuvent faire valoir divers intérêts légitimes, y compris les droits fondamentaux de leurs bénéficiaires, pour refuser des demandes injustifiées. » [897]

### §1 — Les privilèges et immunités des Organisations internationales

Afin de mieux comprendre ce point, il nous a paru nécessaire d'effectuer un léger zoom : on ne parlera donc plus dans les lignes qui suivent d'ONG, mais d'organisations internationales (OI). En effet, seules ces dernières peuvent disposer d'immunités et de privilèges, qui sont reconnus par la signature d'accords bilatéraux entre des organisations internationales et les États. Sachant que ces accords s'appuient en grande partie sur la Convention de Vienne sur les relations diplomatiques de 1961 et 1963 et la Convention sur les privilèges et immunités de l'ONU de 1946[898].

Pour être claire, en droit international, les privilèges exemptent leurs sujets d'une partie des lois d'un État, tandis que les immunités de juridiction exonèrent le personnel de poursuites administratives et judiciaires[899]. Les privilèges de l'OI signifient qu'elle est affranchie de certaines mesures, comme des taxes et droits de douane, et ont pour finalité la facilitation de l'exercice du mandat de l'OI en la déchargeant de contraintes administratives. Et surtout, les privilèges et immunités participent à garantir le caractère confidentiel de l'action de l'OI. Ils assurent en effet l'inviolabilité des documents, des manuscrits et des archives ; la non-ingérence dans les communications officielles et le droit d'expédier et de recevoir sa

[896] « Humanitarian organizations not benefiting from Privileges and Immunities may come under pressure to provide data collected for humanitarian purposes to authorities wishing to use such data for other purposes (for example control of migration flows and the fight against terrorism. »
The 37th international conference of data protection and privacy commissioners, Amsterdam, 27/10/2015 http://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-Privacy-and-International-Humanitarian-Action.pdf

[897] "Governments may also request data directly from HOs, or even assert jurisdiction or seize it against their wishes. Organizations that benefit from privileges and immunities have well-established rules for dealing with requests from governments and can assert various legitimate interests, including the fundamental rights of their beneficiaries, as a reason to refuse unwarranted requests.
HAYES, Ben, « Migration and data protection: doing no harm in an age of mass displacement, mass surveillance and "big data", *International Review of the Red Cross*, 2017, 99 (1),p.179–209. https://international-review.icrc.org/sites/default/files/irrc_99_12.pdf

[898]« Immunité, Dictionnaire pratique du droit humanitaire », MSF https://dictionnaire-droit-humanitaire.org/content/article/2/immunite/
https://www.icj-cij.org/fr/autres-textes/convention-sur-les-privileges
https://legal.un.org/ilc/texts/instruments/french/conventions/9_2_1963.pdf

[899] « La distinction entre immunité et privilège n'est pas facile à établir avec précision. Les termes sont souvent utilisés indifféremment, mais, en règle générale, un privilège implique une sorte d'exemption de respecter certaines règles ou lois […], tandis qu'une immunité n'implique pas d'exemption de respecter le droit positif, mais confère une protection d'ordre procédural face à l'engagement de poursuites dans l'État hôte » SIR IVOR, Roberts (dir.), *Satow's Diplomatic Practice*, 6e éd., Oxford University Press, Oxford, 2009, p. 121

correspondance par courrier diplomatique ou sacs scellés[900]. Précisons que l'inviolabilité des communications de l'OI inclut toute sorte de documents, dont les conversations « e-mails » des employés de l'OI. Pour bénéficier de privilèges et immunités, les documents doivent être identifiés comme appartenant à l'OI[901]. Mais surtout, les OI utilisent ce type d'outil juridique de façon différente selon leur mandat. Par exemple, le HCR et le CICR sont deux organisations internationales, elles bénéficient donc toutes les deux de privilèges et d'immunités, mais, comme on va tout de suite le voir, elles n'ont pas la même approche de la confidentialité et n'opèrent pas avec les mêmes contraintes.

## § 2 — L'UNHCR

Pour commencer, l'UNHCR est une organisation internationale, non soumise au droit national local, et en tant que telle, l'UNHCR bénéficie aussi de privilèges et d'immunités, garantissant la confidentialité de ses échanges. Mais l'organisation effectue un travail d'enregistrement des demandeurs d'asile. Et pour ce faire, elle est amenée à échanger régulièrement des données avec les États. L'agence onusienne travaille en effet en responsabilité conjointe avec les gouvernements locaux. Il revient normalement à l'État de déterminer le statut d'un réfugié, mais l'UNHCR peut s'en charger, notamment dans les cas où le gouvernement n'est pas signataire de la convention relative au statut des réfugiés de 1951[902].

La répartition des rôles entre les États et l'UNHCR quant à l'enregistrement des demandeurs d'asile varie selon les pays et peut faire l'objet de négociations et évoluer au fil du temps[903]. Dans certains cas, l'UNHCR n'a qu'une fonction d'assistance. Le gouvernement est responsable en premier lieu de l'enregistrement des réfugiés, et l'UNHCR apporte simplement son soutien. Dans certains cas, le gouvernement et l'UNHCR mènent des démarches d'enregistrement conjointes. Enfin, il peut arriver que l'UNHCR soit mandaté par le gouvernement, qui lui délègue les opérations d'enregistrement des réfugiés. L'organisation humanitaire mène alors ces dernières en cohérence avec son mandat de protection. Mais,

---

[900] DEBUF, Els "Tools to Do the Job: The ICRC's Legal Status, Privileges and Immunities", *International Review of the Red Cross*, Vol. 97, No. 897–898, 2015, pp. 321–329.Les accords garantissant au CICR l'inviolabilité des documents, écrits, archives et données, sont formulées comme tels : « L'État… s'engage à respecter le caractère confidentiel des rapports, lettres et autres communications adressés par le CICR au gouvernement, et notamment à ne pas en divulguer le contenu à quiconque hormis le destinataire et à ne pas en autoriser l'utilisation dans le cadre de procédures juridiques sans le consentement du CICR. »

[901] Convention on the privileges and immunities of the United nation, 1946 https://www.un.org/en/ethics/assets/pdfs/Convention%20of%20Privileges-Immunities%20of%20the%20UN.pdf

[902] https://www.unhcr.org/fr/en-bref/qui-nous-sommes/la-convention-de-1951-relative-au-statut-des-refugies « La Convention de 1951 relative au statut des réfugiés et son Protocole de 1967 constituent le fondement du régime international des réfugiés, c'est-à-dire les normes juridiques et les institutions compétentes en matière de protection des réfugiés. La majeure partie des nations du monde entier ont signé ou ratifié cette Convention et son Protocole, et pourtant, un grand nombre des pays qui accueillent le plus de réfugiés au monde ne l'ont pas fait : 149 États-membres de l'ONU sont actuellement partis à la Convention, à son Protocole de 1967 ou aux deux, tandis que 44 ne le sont pas » La coopération entre le HCR et les États hôtes non-signataires peut revêtir la forme spécifique d'un Protocole d'accord bilatéral. En définissant les conditions de la coopération et en réitérant les principes essentiels de la protection des réfugiés, ces protocoles peuvent créer un lien important entre les États non signataires et la Convention relative aux réfugiés. Toutefois, il n'existe pas d'approche universelle pour sceller de tels accords, dont le contenu varie considérablement. » JANMYR, MAJA, « Les États non-signataires et le régime international des réfugiés, Revue des Migrations forcées », *RMF* 67, Juillet 2021, https://www.fmreview.org/fr/numero67/janmyr

[903] WALKEY, Claire, "Registration and refugee status determination: a missing link, School of advanced study university of London", 16/08/2020 https://rli.sas.ac.uk/blog/registration-and-refugee-status-determination-a-missing-link

TWIGT, Mirjam, "Doing Refugee Right(s) with Technologies? Humanitarian Crises and the Multiplication of "Exceptional" Legal States", *Refugee Survey Quarterly*, 2023;, hdad020, https://doi.org/10.1093/rsq/hdad020

quelle que soit la situation, les opérations d'enregistrement des réfugiés nécessitent de collecter un certain nombre de données personnelles ainsi que biométriques[904]. Qui peut alors y avoir accès ? Lorsque l'UNHCR est le principal responsable de l'enregistrement des réfugiés, les gouvernements ne pourraient-ils pas avoir accès aux données des réfugiés ? Aux yeux des États, il est légitime de savoir qui se trouve sur son territoire et quelles personnes veulent faire l'objet d'une demande d'asile, et même Privacy International reconnait que : « Le HCR ne peut pas dire à un gouvernement d'accueil qu'il ne partagera pas d'information sur des personnes qui relèvent de sa juridiction. L'agence opère normalement sur la base d'un accord avec le pays hôte, donc toujours avec le consentement de ce dernier. » [905] Et donc l'UNHCR indique que des données « biographiques » peuvent être partagées avec les gouvernements locaux. En revanche, l'organisation précise qu'il garde confidentielles des données biométriques (photographies, scan d'iris, empreintes digitales). Mais au regard de la quantité de données biométriques traitées par l'UNHCR, un audit datant de 2016 avertit que : « La mise en œuvre récente de son système de gestion de l'identité biométrique ayant augmenté la probabilité de demandes de partage de données biométriques par les gouvernements hôtes, il existe des risques liés à des accords de partage de données inadéquats, et la sécurité et la protection des personnes concernées pourraient également être compromises. »[906]

Dernier point, les politiques de protection des données spécifient clairement que l'UNHCR ne transmet pas de données avec les États d'origines des demandeurs d'asile. Mais des données personnelles peuvent être partagées avec des pays tiers en cas de réunification familiale ou dans le cadre de programmes de « retour volontaire »[907]. Et en l'absence de reconnaissance du statut de réfugié, il est possible que des données soient partagées avec le pays d'origine : « En ce qui concerne les personnes dont il est établi qu'elles n'ont pas besoin d'une protection internationale (c'est-à-dire les cas rejetés après épuisement des voies de recours disponibles), le partage limité de données à caractère personnel avec les autorités du pays d'origine est légitime afin de faciliter le retour, même si cela se fait sans le consentement des personnes concernées. »[908] L'UNHCR précise tout de même que le partage de données ne doit pas aller au-delà de ce qui est légalement nécessaire pour assurer le retour de la personne, et que ce dernier ne doit pas mettre la personne en danger.

---

[904] KAURIN, Dragana, "Data protection and digital agency for refugees", World Refugee Council research paper n°12, may 2019https://www.cigionline.org/static/documents/documents/WRC%20Research%20Paper%20no.12.pdf

[905] "UNHCR cannot tell a host government that it will not share information on individuals who are under the jurisdiction of the host government. The agency normally operates on the basis of a host country agreement, thus always with the consent of the host country." "Why we work on refugee privacy", *Privacy International*, 08/07/2011 https://privacyinternational.org/news-analysis/1322/why-we-work-refugee-privacy

[906] "Since the recent implementation of BIMS increased the probability of requests of sharing of biometric data by host governments, there were risks related to inadequate data sharing arrangements, and the security and protection of persons of concern could also be compromise." REPORT 2016/181 Audit of the Biometric Identity Management System at the Office of the United Nations High Commissioner for Refugees, 22 December 2016 Assignment No. AR2016/163/03
Ladek, S, Abdelkhaliq, N, Scott Cameron, Z, Green, S;Procter, C., "Evaluation of UNHCR's Data Use and Information Management Approaches », UN doc ES/2019/07, UNHCR, 2019,

[907] "Advisory opinion on the rules of confidentiality regarding asylum information", UNHCR, 2005,https://www.refworld.org/jurisprudence/amicus/unhcr/2005/en/93151

[908]"Regarding persons found not to be in need of international protection (that is, rejected cases after exhaustion of available legal remedies), the limited sharing of personal data with the authorities of the country of origin is legitimate in order to facilitate return, even if this is without the consent of the individuals concerned." Procedural standards for refugee status determination under UNHCR's mandate, Confidentiality and data protection in UNHCR RSD procedures, UNHCR, August 2020

Et pourtant, en dépit des risques, l'UNHCR a partagé avec le gouvernement bangladais des données de réfugiés rohingyas, une minorité musulmane gravement persécutée en Birmanie[909]. Pour rappel, ce pays est accusé de crime de guerre, voire de nettoyage ethnique à l'égard des Rohingyas. Et le Bangladesh a par le passé déjà expulsé des réfugiés rohingyas[910], et il a par la suite transmis ces mêmes données à l'État birman.

Revenons sur le déroulé des événements. Précisons tout d'abord que le Bangladesh n'est pas signataire de la Convention sur les réfugiés de 1951. Les différentes opérations d'enregistrement des réfugiés sont donc en principe menées en majeure partie par l'UNHCR. Le gouvernement du Bangladesh collabore toutefois avec l'UNHCR pour diverses opérations de comptage de foyers de réfugiés. Puis en juin 2018, l'UNHCR et le gouvernement du Bangladesh recueillent conjointement des données personnelles et biométriques (des scans d'iris). Leur collecte avait pour finalité la création d'une carte donnant droit à différents services ainsi que l'examen du droit d'exercice à un retour volontaire en Birmanie. Or, rappelons que le contexte politique y est extrêmement sensible pour les Rohingyas. La Birmanie persécute cette minorité musulmane et le pays est à ce titre accusé d'avoir commis des crimes contre l'humanité à son égard[911]. En outre, le Bangladesh a déjà par le passé effectué plusieurs opérations de retours forcés de réfugiés rohingyas. Et surtout, un accord a été noué entre le Bangladesh et la Birmanie, en novembre 2017, pour examiner leurs conditions de retour. L'UNHCR s'y oppose, arguant que les conditions ne sont pas réunies, mais reste ouvert au fait d'examiner de possibles et futurs plans de retours volontaires. L'UNHCR avait alors considéré en février 2018 « que les garanties nécessaires pour les retours potentiels de réfugiés au Myanmar sont absentes. Le HCR a appelé le Myanmar à autoriser l'accès humanitaire sans entraves nécessaire dans les zones de retour et à créer les conditions d'une solution sûre et durable, en mettant par exemple en œuvre les recommandations de la Commission consultative du Rakhine. » [912] Ainsi, en avril 2018, un accord avait été signé entre le Bangladesh et l'UNHCR assurant le droit au retour des Rohingyas une fois que les conditions seraient réunies[913]. L'UNHCR a également signé un accord avec la Birmanie, conditionnant des solutions de rapatriement à un contexte politique sûr pour les Rohingyas[914]. Les parties prenantes n'auraient pas signé d'accords tripartites bien que l'UNHCR ait travaillé à ce sujet.

---

[909] Les Rohingyas sont persécutés depuis les années 1970, la dernière vague d'exil date de 2016 à la suite d'explosion de violence à leur égard de la part de l'armée birmane.

[910]« Entre 1992 et 2005, le Myanmar et le Bangladesh se sont ainsi mis d'accord sur le rapatriement d'environ 230 000 Rohingyas. En raison de l'absence de droits et du risque de rapatriement forcé, de nombreux Rohingyas tentent de rejoindre d'autres États d'Asie du Sud-Est, la Malaisie en premier lieu. » BAZIN Judith, « Rohingyas, réfugiés et apatrides », *Plein droit*, 2016/3 (n° 110), p. 28-31 https://www.cairn.info/revue-plein-droit-2016-3-page-28.htm

[911] Amnesty International, "My world is finished, Rohingya targeted in crimes against humanity in Myanmar", 2017 https://amnestyfr.cdn.prismic.io/amnestyfr%2F9bfae98e-caaa-4486-915f-11f320583e96_my+world+is+finished+myanmar+asa+1672882017.pdf

[912]"That the necessary safeguards for the potential returns of refugees to Myanmar are absent. UNHCR has called on Myanmar to allow the necessary unhindered humanitarian access in areas of return and to create conditions for a safe and sustainable solution, including by implementing the recommendations of the Rakhine Advisory Commission." UNHCR, "Operational Update, Bangaldesh",23 January-5 February https://reliefweb.int/report/bangladesh/unhcr-bangladesh-operational-update-23-january-5-february-2018

[913]Accord du Bangladesh et du HCR sur le retour volontaire des réfugiés, qui décideront quand les conditions seront propices, UNHCR, 13/04/2018 https://www.unhcr.org/news/news-releases/bangladesh-and-unhcr-agree-voluntary-returns-framework-when-refugees-decide

[914]« Le HCR et le PNUD conviennent du texte d'un mémorandum d'accord avec le Myanmar sur les conditions nécessaires au retour des réfugiés rohingyas », UNHCR, communiqués de presse, 31/05/2018 https://www.unhcr.org/fr/actualites/news-releases/le-hcr-et-le-pnud-conviennent-du-texte-dun-memorandum-daccord-avec-le

C'est dans ce contexte que l'agence mène courant juin 2018 une opération de collecte de données auprès de réfugiés rohingyas, dans le camp de Cox's Bazar. Or l'agence onusienne aurait mal informé les bénéficiaires sur l'objectif de l'opération. Sa première finalité était de permettre d'avoir droit à une carte délivrant différents services. Sa seconde finalité était de permettre un examen d'éligibilité au retour. Les deux opérations n'étaient pas nécessairement liées : il était possible de refuser de communiquer des informations dédiées à l'examen d'un droit au retour sans pour autant ne pas bénéficier des services de l'UNHCR. Or pour éviter ce type de malentendu, les politiques de l'UNHCR déconseillent fortement de mener ce type d'opération de façon conjointe. Certes, un formulaire a été distribué pour expliquer le contexte de l'opération, mais ce dernier était en anglais et avec des cases précochées, nonobstant la non-maitrise de cette langue par les réfugiés. Pour l'organisation Human Right Watch, il tombe sous le sens que le consentement des réfugiés n'a manifestement pas été pris en compte[915].

Les exilés rohingyas n'auraient surement pas consenti à ce qu'à la suite de son accord avec le Myanmar, le Bangladesh soumette au moins 830 000 noms d'exilés rohingyas au Myanmar avec des données biométriques, pour des examens de rapatriement. Cela dit, l'UNHCR a déclaré à l'HRW qu'il n'a joué aucun rôle dans l'établissement de ces listes, mais qu'elles incluaient des noms et des données biométriques collectées lors des exercices conjoints d'enregistrement avec le Bangladesh. L'examen des cas de rapatriement par le Myanmar requérait apriori des informations d'un certain niveau de précision qui n'ont pu être obtenues par le Bangladesh que lors de l'opération d'enregistrement commune avec le HCR : « L'évaluation indépendante de la réponse d'urgence du HCR, publiée en décembre 2018, a noté que pour les listes que le Bangladesh devrait préparer pour le Myanmar, les autorités "exigeraient un niveau de détail sur le lieu d'origine, la composition de la famille et ainsi de suite" que le gouvernement n'avait pas obtenu lors de son enregistrement initial. »[916]

Mais l'UNHCR était-il au courant au préalable de cet échange, et si oui, y a-t-il consenti ? A-t-il rompu l'accord de partage de données entre l'organisation et le Bangladesh ? Pour rappel, l'UNHCR avait en effet signé un « data sharing agreement » avec le Bangladesh, précisant « que toute utilisation des informations à des fins autres que l'assistance et l'identification ou

[915] " UN shared Rohingya data without informed consent", UNHCR, 15/06/2021 https://www.hrw.org/news/2021/06/15/un-shared-rohingya-data-without-informed-consent
BIN SHAFIQUE, Sharid, "Digital ID in Bangladeshi refugee camps : a case study", *The Engine Room*, 2020 https://digitalid.theengineroom.org/assets/pdfs/%5BEnglish%5D%20Bangladesh%20Case%20Study%20-%20DigitalID%20-%20The%20Engine%20Room.pdf
THOMAS, Elise, "Tagged, tracked and in danger : how the Rohingya got caught in the UN's risky biometric database", *Wired*, 12/03/2018 https://www.wired.co.uk/article/united-nations-refugees-biometric-database-rohingya-myanmar-bangladesh

[916] "UNHCR's independent evaluation of its emergency response, published in December 2018, noted that for the lists Bangladesh would need to prepare for Myanmar, authorities would "require a level of detail about place of origin, family composition and so on" that the government had not obtained in its initial registration." HRW, "UN shared Rohingya data without informed consent", 15/06/2021,https://www.hrw.org/news/2021/06/15/un-shared-rohingya-data-without-informed-consent

le transfert à des tiers devra être approuvée par le HCR. »[917] Mais le contenu complet de ce dernier n'a pas été communiqué publiquement[918].

Ce cas a largement été couvert par la presse spécialisée et a vivement ému le milieu de la solidarité internationale[919]. En guise de complément, on peut revenir sur une autre affaire ayant lieu présentement au Liban. L'UNHCR y prend en charge depuis 2012 l'enregistrement des réfugiés syriens, le pays n'étant pas signataire de la Convention de 1951. Mais en 2015, le gouvernement souhaite suspendre l'enregistrement des demandeurs d'asile, et avoir accès aux données des réfugiés que détient l'UNHCR. Cette demande inclut des données biométriques. Cette dernière requête a été refusée par l'organisation humanitaire, qui invoque un manque de cadre en matière de protection des données[920]. Le contexte se tend progressivement. L'UNHCR continue malgré tout de mener des opérations conjointes d'enregistrement partiel d'exilés[921], tandis que le gouvernement devient plus hostile à leur présence sur son sol, et que la situation économique du pays se dégrade fortement. Pire, d'après Amnesty International, le Liban a commencé courant 2023 à mener des opérations

[917] "that any use of information for purposes other than assistance and identification or transfer to third parties would need to be approved by UNHCR" UNHCR, "Operational Update, Bangaldesh",23 January-5 February https://reliefweb.int/report/bangladesh/unhcr-bangladesh-operational-update-23-january-5-february-2018

[918] "UNHCR said it was unable to share a copy of its data-sharing agreement with Bangladesh without the government's permission. Human Rights Watch asked the Bangladesh government for a copy of the agreement but has yet to receive a response." https://www.hrw.org/news/2021/06/15/un-shared-rohingya-data-without-informed-consent

[919] RAHMAN, Zara, "The UN's refugee data shame", *The New Humanitarian*, 21/06/2021 https://www.thenewhumanitarian.org/opinion/2021/6/21/rohingya-data-protection-and-UN-betrayal

[920] « In 2014, there were fears that the iris scans that UNHCR collected during refugee registration were shared with the Ministry of Social Affairs, after comments from then Social Affairs Minister Rashid Derbas saying that they had the iris scans of Syrian refugees on the record. He later clarified that "while the government didn't currently have the biometric data, it was working with UNHCR to 'establish a system that would turn the data over to General Security.'" He continued: "'Why wouldn't they [UNHCR] give it to us, they are working on Lebanese territory.'" At the time, UNHCR staff rejected the idea that data would be shared with the government. »
ROBBIN, ZOE, "Jordan: is the UN's biometric registration for Syrian refugee a threat to their privacy?", *Middle East eye*, 23/10/2022 https://www.middleeasteye.net/news/jordan-syrian-refugees-un-biometrics-threat-data-privacy
ROBEHMED, Sacha, « The future of Biometrics and digital ID in Lebanon, assessing proposed systems for elections and social assistance »,*SMEX*, 2021,https://smex.org/wp-content/uploads/2021/01/210121_SMEX_PI_ElectoralDigitalID_Draft5_EN.pdf

[921]« Bien que le HCR se soit considéré comme "tenu de se conformer 'à l'ordonnance de suspension, il a eu recours, en l'absence de procédures d'enregistrement, à' une inscription" des réfugiés individuels. Pour ce faire, il ne recueille que des informations de base et des données biométriques dans la base de données du système d'information sur l'assistance aux réfugiés (RAIS) du HCR. Un représentant du gouvernement estime que le HCR avait enregistré environ 40 000 Syriens en juin 2016. Alors que l'enregistrement n'est ostensiblement effectué qu'à des fins d'assistance, ce que le HCR considère en pratique comme de l'assistance dans ces cas semble être très large. Comme l'explique un haut fonctionnaire du HCR, "pour nous, il s'agit également de protection, donc si un cas nous est soumis et qu'il a besoin d'une assistance psychosociale, juridique, d'une protection, etc. Les personnes enregistrées seraient également éligibles à la réinstallation à l'étranger. Cela signifie essentiellement que la principale différence entre les personnes enregistrées et celles qui le sont est que ces dernières n'obtiennent pas de certificat du HCR, qui, comme nous l'avons expliqué précédemment, est devenu pour beaucoup un élément essentiel pour résider au Liban." " While UNHCR considered itself 'duty bound to comply' with the suspension order, it has in the absence of registration procedures resorted to 'recording' individual refugees. This is done by collecting only basic information and biometrics in UNHCR's Refugee Assistance Information System (RAIS) database. One government official estimates that UNHCR had recorded an approximate 40,000 Syrians by June 2016. While recording is ostensibly done only for assistance purposes, what UNHCR in practice considers assistance in these cases appears to be very broad. As a senior UNHCR official explains, 'for us it is also protection, so if a case approaches us and needs psychosocial, legal assistance, protection, etc., that's part of our assistance … '. Recorded individuals are reportedly also eligible for resettlement abroad. This essentially means that the main difference between those who are recorded and those who are registered is that those who are recorded do not get a UNHCR certificate, which, as previously explained, has for many become essential for residency in Lebanon »
JANMYR, Maja,"UNHCR and the Syrian refugee response: negotiating status and registration in Lebanon", *The International Journal of Human Rights*, 2018, 22:3, p. 393-419,
"the registration of Syrian refugees by UNHCR in Lebanon was suspended by the Government in 2015. While UNHCR continues to update data on the previously registered population, UNHCR advocates for the resumption of registration activities so as to better manage needs and responses in Lebanon. For asylum-seekers with nationalities other than Syrian, UNHCR continues to conduct refugee status determination (RSD) in order to identify international protection needs and durable solutions. "
« L'enregistrement des réfugiés syriens par le HCR au Liban a été suspendu par le Gouvernement en 2015. Alors que le HCR continue à mettre à jour les données sur la population précédemment enregistrée, le HCR plaide pour la reprise des activités d'enregistrement afin de mieux gérer les besoins et les réponses au Liban. Pour les demandeurs d'asile de nationalité autre que syrienne, le HCR continue de procéder à la détermination du statut de réfugié (DSR) afin d'identifier les besoins en matière de protection internationale et de solution durable. »https://www.unhcr.org/lb/refugees-and-asylum-seekers

d'expulsion forcée en direction de la Syrie[922]. C'est dans ce contexte que le gouvernement exige à nouveau d'avoir accès à des données de l'UNHCR. Et finalement, courant 2023, un accord est noué entre l'organisation humanitaire et le Liban. Ce dernier n'est pas rendu public, mais dans un communiqué de presse, l'UNHCR assure que le Liban s'est engagé à ne pas transmettre ces données au gouvernement syrien ni à mener des opérations de rapatriement forcé. Il tout de même précisé que cet accord implique de communiquer des données au service de renseignement libanais : « Pour mettre en œuvre l'accord du mois d'août, le HCR partagera désormais avec la direction générale de la Sûreté générale les données personnelles de base des réfugiés syriens connus du HCR dans le cadre d'un transfert unique. Les données personnelles partagées ne comprendront pas les antécédents personnels, tels que la région d'origine en Syrie, les informations de contact au Liban ou d'autres informations sensibles. »[923] Elle stipule également qu'elle ne transmet pas de données au gouvernement syrien et indique que ce partage de données se fait dans la continuation de sa collaboration avec l'État libanais : « Le HCR partage déjà certaines données avec le gouvernement libanais afin d'assurer la protection et l'assistance nécessaires. L'accord du mois d'août s'appuie sur la collaboration en cours entre le HCR et le gouvernement libanais. »[924] Nous ne disposons pas de plus de détails sur la nature des négociations, mais ces éléments donnent une première image des risques que représentent les échanges de données entre une organisation internationale et un État.

On peut citer un dernier exemple pour clore cette section : le « data sharing agreement » signé par l'UNHCR en 2019 avec le département de la Sécurité intérieure américain (DHS). Ce dernier requiert la communication des données biométriques d'exilés souhaitant s'établir aux États unis. Précisons qu'aux États-Unis, l'UNHCR joue un rôle dans la toute première étape d'examen de candidatures[925], mais que le processus d'enregistrement et les opérations de criblages des réfugiés sont partagés entre de multiples organes étatiques, dont des

---

[922] Amnesty International, « Lebanon : halt summary deportations of Syrian refugees », 11/05/2023https://www.amnesty.org/en/latest/news/2023/05/lebanon-halt-summary-deportations-of-syrian-refugees/

[923]« To implement the August agreement, UNHCR will now share with the General Directorate of General Security basic personal data of Syrian refugees known to UNHCR as part of a one-time transfer. Shared personal data will not include personal histories, such as the area of origin in Syria, contact information in Lebanon or other sensitive information. "

**«** UNHCR already shares some data with the Government of Lebanon for the purposes of ensuring needed protection and assistance. The August agreement builds on the ongoing collaboration between UNHCR and the Government of Lebanon". Update on data sharing, UNHCR Lebanon, 24/11/2023

https://help.unhcr.org/lebanon/en/2023/11/24/update-on-data-sharing/

« Réfugiés syriens : menace à peine voilée du directeur de la Sûreté contre le HCR », L'Orient-le Jour, 06/10/2023

https://www.lorientlejour.com/article/1351598/refugies-syriens-menace-a-peine-voilee-du-directeur-de-la-surete-contre-le-hcr.html

WALID TAKKOUCHE, Karin, "A new layer of refugee politics at UNHCR biometric technology: Syrian refugee biometric registration by UNHCR in Lebanon", Master Thesis, Political Studies, American University of Beirut, May 2023

https://scholarworks.aub.edu.lb/bitstream/handle/10938/24075/TakkoucheKarin.pdf?sequence=3

EL-HAGE, Anne-Marie, "Ivo Freijsen : no hidden agenda to keep Syrian refugees in Lebanon", L'Orient Today, 23/05/2024

https://today.lorientlejour.com/article/1414892/ivo-freijsen-no-hidden-agenda-to-keep-syrian-refugees-in-lebanon.html

[924]**«** UNHCR already shares some data with the Government of Lebanon for the purposes of ensuring needed protection and assistance. The August agreement builds on the ongoing collaboration between UNHCR and the Government of Lebanon". Update on data sharing, UNHCR Lebanon, 24/11/2023

https://help.unhcr.org/lebanon/en/2023/11/24/update-on-data-sharing/

« Réfugiés syriens : menace à peine voilée du directeur de la Sûreté contre le HCR », L'Orient-le Jour, 06/10/2023

https://www.lorientlejour.com/article/1351598/refugies-syriens-menace-a-peine-voilee-du-directeur-de-la-surete-contre-le-hcr.html

WALID TAKKOUCHE, Karin, "A new layer of refugee politics at UNHCR biometric technology: Syrian refugee biometric registration by UNHCR in Lebanon", Master Thesis, Political Studies, American University of Beirut, May 2023

https://scholarworks.aub.edu.lb/bitstream/handle/10938/24075/TakkoucheKarin.pdf?sequence=3

EL-HAGE, Anne-Marie, "Ivo Freijsen : no hidden agenda to keep Syrian refugees in Lebanon", L'Orient Today, 23/05/2024

https://today.lorientlejour.com/article/1414892/ivo-freijsen-no-hidden-agenda-to-keep-syrian-refugees-in-lebanon.html

[925] JACOBSEN, LINDSKOV, Katja, "Biometric data flows and unintended consequences of counterterrorism", *International review of the Red Cross*, 2021, 103 (916-917),p.619-652 https://international-review.icrc.org/sites/default/files/reviews-pdf/2022-02/biometric-data-flows-and-unintended-consequences-of-counterterrorism-916.pdf

organismes de sécurité comme le Federal Bureau of Investigation (FBI). Cependant, l'accord de 2019 a été conclu entre le DHS et l'UNHCR afin d'élargir la diversité des informations accessibles au département d'État pour soutenir le programme américain d'admission des réfugiés (USRAP). Et l'UNHCR partage désormais directement les informations biométriques et biographiques avec le système d'identification biométrique automatisé (IDENT) de l'Office of Biometric Identity Management (OBIM) du DHS. Selon les communiqués officiels, IDENT « fournit des informations biométriques aux utilisateurs autorisés afin de vérifier l'identité des personnes qu'ils rencontrent dans le cadre de leurs missions et de déterminer si ces personnes peuvent bénéficier d'une prestation ou si elles doivent faire l'objet d'une action des services de police ou de renseignement. Le DHS utilise les données du HCR pour vérifier que l'individu traité par le personnel du SCIS est le même que celui qui a été enregistré et référé par l'UNHCR. »[926] La base de données, dont la finalité est le criblage des demandeurs de visa, existe depuis 1994 et n'a cessé de croitre exponentiellement. Elle contiendrait des informations sur plus de 250 millions de personnes ayant postulé au statut de réfugié aux USA. Et d'après des activistes de défense des droits de l'homme en ligne, elle pourrait contenir des données d'individus n'ayant jamais mis les pieds sur le sol américain : « Les individus peuvent abandonner le processus de réinstallation des réfugiés pour diverses raisons, mais le département "peut dans ces cas continuer à détenir des données biométriques sur des individus qu'il ne rencontrera peut-être pas", ont déclaré les responsables dans l'AIP. Selon les données de l'UNHCR, moins d'un quart des quelque 85 000 dossiers examinés par l'U.S. Citizenship and Immigration Services (USCIS) en 2018 ont abouti à l'approbation de l'admission du réfugié aux États-Unis. L'agence a rejeté 33 485 références de réfugiés et a fermé 30 438 autres dossiers pour des raisons non spécifiées, mais dans le cadre du nouveau programme, elle serait toujours en mesure de conserver les profils biométriques de ces personnes. »[927]

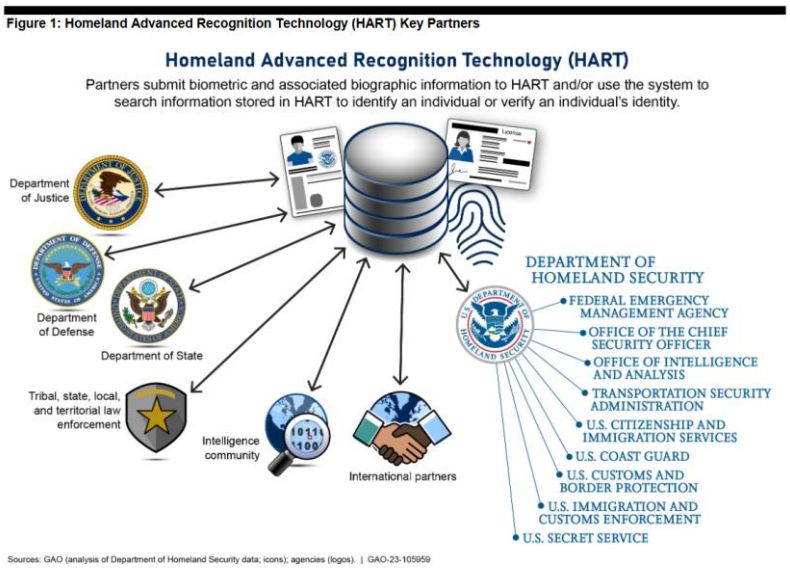
En tout cas, depuis 2015, il est projeté de refondre la base de données en un nouveau système de gestion de l'information : l'« Homeland Advanced Recognition Technology ( HART). La base de données pourra contenir au moins sept types d'identifiants biométriques, dont des données faciales et vocales, de l'ADN, des cicatrices et des tatouages. Il inclura également des informations biographiques, telles que le nom, la date de naissance, les descripteurs physiques, le pays d'origine, et des informations sur les « schémas relationnels » des personnes[928]. L'objectif de ce projet est aussi d'améliorer l'interopérabilité de base de données entre des agences fédérales comme l'ICE (Immigration and Customs Enforcement),

[926] « Provides biometric encounter information to authorized users to verify the identity of individuals they encounter pursuant to their missions and determine whether those individuals are eligible to receive a benefit or should be subject to a law enforcement or intelligence action. DHS uses UNHCR data to verify that the individual being processed by SCIS personnel is the same individual who was registered and referred by UNHCR." https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis081-unhcr-august2019.pdf

[927] "Individuals might drop out of the refugee resettlement process for a variety of reasons, but the department "may in those cases continue to hold biometrics on individuals it may not encounter," officials said in the PIA. According to UNHCR data, less than a quarter of the nearly 85,000 cases reviewed by USCIS in 2018 resulted in the refugee being approved for admission to the U.S. The agency rejected 33,485 refugee referrals and closed another 30,438 cases for unspecified reasons, but under the new program, it would still be able to maintain biometric profiles on those individuals." CORRIGAN, Jack, "Most refugees who apply for asylum in the U.S. never set foot in the country, but under an agreement with the United Nations, DHS and its partners can still build biometric profiles on them", *NextGOUV*, 20/08/2019, https://www.nextgov.com/emerging-tech/2019/08/dhs-collecting-biometrics-thousands-refugees-who-will-never-enter-us/159310/

[928] LYNCH, Jennifer, « HART : Homeland Security's Massive New Database Will Include Face Recognition, DNA, and Peoples' "Non-Obvious Relationships", EFF, 07/06/2018 https://www.eff.org/fr/deeplinks/2018/06/hart-homeland-securitys-massive-new-database-will-include-face-recognition-dna-and

le Customs and Border Protection, le Federal Bureau of Investigation (FBI), et le département de la défense, pour ne citer qu'eux[929].




**PARTENAIRES DE LA BASE DE DONNEES HART [930]**

Ajoutons que la base de données pourrait communiquer avec des services de sécurité et de renseignement d'autres États, comme les Five Eyes (Etats-Unis, Canada, Grande-Bretagne, Australie, Nouvelle-Zélande) pays d'Amérique latine (le Mexique, le Guatemala, le Honduras et le Salvador), et des pays européens comme la Grèce ou l'Italie. D'après Statewatch, le département de la sécurité intérieure est en négociation pour élargir les partenariats avec des institutions européennes[931]. Il va sans dire que le risque est grand que des données de migrants soient partagées avec leurs pays d'origine que les exilés cherchent à fuir. Dénoncé par des organisations américaines de défense de droits de l'homme[932], le projet est au point mort depuis plusieurs années[933], mais l'accord de partage de données entre le HCR et le département de la sécurité intérieure via IDENT est toujours valide.

En substance, ces différents exemples sont une bonne illustration du fait que malgré les privilèges et immunités du HCR, l'organisation humanitaire a pu partager des données, parfois personnelles et sensibles, de réfugiés avec des États cherchant à assurer la surveillance de leurs frontières et de flux de migrations.

---

[929]AIZEKI, Mizue, SHAH, Paromita, "HART attack, How DHS's massive biometrics database will supercharge surveillance and threaten rights", may 2022 https://surveillanceresistancelab.org/wp-content/uploads/2023/01/HART-Attack-2022.pdf

[930] United States Government Accountability Office,"
BIOMETRIC IDENTITY SYSTEM DHS Needs to Address SignificantShortcomings in Program Management and Privacy", September 2023 https://www.gao.gov/assets/gao-23-105959.pdf

[931] "EU and USA plough ahead with secret discussions on biometric data exchange scheme", Statewatch, 24/08/2023https://www.statewatch.org/news/2023/august/eu-and-usa-plough-ahead-with-secret-discussions-on-biometric-data-exchange-scheme/
Statewatch, EU : council presidency seeks "common vision" on US database access demands, 25/01/2024
https://www.statewatch.org/news/2024/january/eu-council-presidency-seeks-common-vision-on-us-database-access-demands/

[932]Electronic Frontier Foundation, "Comments of the electronic frontier foundation regarding notice of proposed rulemaking on the collection and use of biometrics by u.s. citizenship and immigration services", 2020,https://www.eff.org/files/2020/10/22/2020-10-13_-_dhs_nprm_on_biometric_collection_-_eff_website.pdf

[933]"US Government accountability office, Biometric identity system, DHS needs to address significant shortcomings in program management and privacy",september 2023 https://www.gao.gov/assets/gao-23-105959.pdf

## §3 — Le CICR

Prenons maintenant le cas très différent du CICR. Il se distingue d'une ONG « classique » sans être pour autant une organisation internationale à proprement parler. En clair, le CICR a été fondé par des individus privés. Il est doté d'un statut d'association selon le Code civil suisse. Mais afin de pouvoir remplir son mandat, le CICR bénéficie d'un statut équivalent à celui d'une organisation internationale [934]. Par voie de conséquence, le CICR peut théoriquement accomplir son mandat en conservant une certaine confidentialité, et donc « dans le respect du droit applicable, le CICR se réserve à tout moment la possibilité de décider quel type d'information il souhaite partager avec ses interlocuteurs (autorités étatiques ou non étatiques, ou tiers). Les décisions portant sur la transmission d'informations confidentielles se prennent par le CICR seul, sur la base de procédures internes agréées. »[935]

Le partage de données, et plus spécifiquement de données biométriques, n'est donc pas totalement proscrit selon la politique de protection de données du CICR qui stipule que « le CICR ne partagera pas de données biométriques à des gouvernements ou à des autorités, à moins que les conditions suivantes soient remplies : le transfert de données est nécessaire à l'intérêt vital de la personne. Le transfert de données est nécessaire à la réalisation d'une mission humanitaire. La personne concernée est informée qu'un transfert de données est envisagé et n'y objecte pas. »[936]

Autre particularité, outre les différents privilèges et immunités qu'il partage avec les agences onusiennes, le CICR jouit d'un droit de « non-divulgation » à l'encontre de la justice internationale. Ce droit a été reconnu à la date du 27 juillet 1999, par le Tribunal international de l'ex-Yougoslavie, à la suite du refus du CICR qu'un de ses anciens employés témoigne dans

---

[934] Statuts du Comité international de la Croix-Rouge, 01/01/2018
https://www.icrc.org/fr/document/statuts-du-comite-international-de-la-croix-rouge
RONA, Gabor, « Le statut du CICR : dans une catégorie à part », 17/02/2004 https://www.icrc.org/fr/doc/resources/documents/misc/5wwhdp.htm
« Nous bénéficions actuellement de privilèges et d'immunités dans 106 États. Dans la grande majorité des cas, ces privilèges nous ont été accordés en vertu d'accords de siège. Le CICR jouit par exemple de privilèges et d'immunités en Belgique, en France, en Suisse et bientôt en Irlande. C'est également le cas en Afrique du Sud, en Australie, en Corée du Sud, aux États-Unis et en Russie. » Le point sur le statut juridique du CICR, 20/03/2019 https://www.icrc.org/fr/document/le-point-sur-le-statut-juridique-du-cicr

[935] « Doctrine sur l'approche confidentielle du Comité international de la Croix- Rouge (CICR)
Moyen spécifique du CICR pour obtenir des autorités étatiques et non étatiques le respect du droit », *Revue internationale de la croix rouge*, vol 94, 2012/3 https://international-review.icrc.org/sites/default/files/ricr-887-confidentiel.pdf
ICRC's Directorate, Access to Information Policy, April 2019 https://www.icrc.org/sites/default/files/document_new/file_list/access-information-policy.pdf

[936]"In order to safeguard the neutrality, impartiality and independence of the ICRC and the exclusively humanitarian nature of its work, the ICRC will not share or otherwise transfer biometric data to any government or authority, unless all of the following conditions are met: (i) the transfer is in the vital interest of the data subject or of another person; (ii) the transfer is necessary in order to enable an authority to fulfil an obligation of a humanitarian nature; (iii) the Data Subject is informed that the data transfer is envisaged and does not object (unless the data subjects are unaccounted for and the purpose of sharing is indeed to identify the whereabouts of the data subject or identify human remains); (iv) a Data Protection Impact Assessment (DPIA) is carried out prior to the data sharing, and the DPIA does not highlight risks for the data subjects or other persons which take primacy over the perceived benefits of the sharing; and (v) The recipient commits in writing to only use the transferred data for the specified humanitarian purpose", ICRC, "Policy on the processing of Biometric Data by the ICRC", 28/08/2019

l'affaire Simic[937]. Cette exemption de témoignage a été justifiée par la mission humanitaire du CICR[938], mais aussi par son approche spécifique reposant sur le principe de confidentialité[939].

Ce dernier parait rentrer en tension avec d'autres impératifs comme celui de témoigner et de publiciser des violations des droits de l'homme, mais également de sortir de l'anonymat et rendre visibles des populations marginalisées et persécutées. Cela dit, le CICR est aussi garant de l'application du droit international humanitaire (DIH). En cas de violation de ce dernier, sa démarche n'est pas de porter directement les affaires sur le plan judiciaire, mais de communiquer de façon non publique avec les parties prenantes, et ce afin de les confronter aux preuves des violations en question et de les placer devant leur responsabilité[940]. Et pour citer la juriste Anne Marie La Rosa, la Cour pénale internationale et le CICR ont tous deux pour mission la prévention des violations du droit international humanitaire, et malgré la différence d'approche, leurs actions sont, pour la juriste, complémentaires. Anne Marie La Rosa déclare ainsi que « tandis que la CPI poursuit et sanctionne, le CICR s'attache à promouvoir le respect du droit international humanitaire au moyen du dialogue confidentiel et de la persuasion. »[941]

Comment le CICR justifie-t-il ce privilège de « non-divulgation » ? De manière générale, les privilèges et immunités sont motivés par la nécessité de garantir l'accomplissement efficace du mandat de l'agence en toute indépendance, sans être contraints par l'application des lois du pays hôte. Il s'agit « d'outil pour faire le travail » selon l'expression de la juriste Els Debuf[942], et plus spécifiquement pour le CICR : « la confidentialité est également primordiale (…) lorsqu'il doit convaincre les parties à un conflit armé d'avoir accès aux zones de conflit, à la population civile, aux personnes privées de liberté et aux forces combattantes elles-mêmes. Si les parties à un conflit avaient l'impression que les informations recueillies par le CICR sur les zones de conflit ou dans les lieux de détention pourraient être utilisées ultérieurement dans le cadre de procédures judiciaires, d'enquêtes publiques ou d'autres procédures

---

[937] https://www.icty.org/fr/content/milan-simi%C4%87

[938] « Les tribunaux internationaux ne reconnaissent en principe aucune des immunités traditionnellement reconnues devant les tribunaux nationaux. L'obligation de coopération avec les tribunaux est absolue. Toutefois ces tribunaux ont reconnu la nécessité de protéger la mission d'intérêt public que remplissent des organisations humanitaires et celle des correspondants de guerre dans les situations de conflits armés. » Immunité, Dictionnaire pratique du droit humanitaire, MSF
https://dictionnaire-droit-humanitaire.org/content/article/2/immunite/

[939] LA ROSA, Anne-Marie, *Chapitre IV. Organisations humanitaires et instances pénales internationales : situation singulière du CICR* In : *Juridictions pénales internationales : La procédure et la preuve*, Genève : Graduate Institute Publications, 2003 https://books.openedition.org/iheid/584?lang=fr
« Cette immunité n'a été expressément reconnue par le TPIY qu'au CICR. Elle a été confirmée par la Cour pénale internationale, qui reconnaît expressément dans son Règlement de procédure et de preuve que les informations en la possession du CICR n'ont pas à être communiquées, et cela y compris dans le cadre du témoignage (règle 73). La partie de cette règle qui traite du CICR est le résultat d'un compromis. Le CICR avait préconisé une règle conférant une protection absolue alors que plusieurs États avaient insisté pour que la Cour ait un rôle à jouer dans la détermination au cas par cas de l'information du CICR, s'il y en a, qui devait être transmise. Ainsi, aux termes de la règle 73, le CICR doit mener des consultations avec la Cour si celle-ci juge l'information comme "d'une grande importance dans un cas d'espèce". Le CICR a toutefois le dernier mot sur la divulgation de son information. Cette règle interdit également le recours aux informations détenues dans le cadre d'activités couvertes par le secret professionnel. » Immunité, Dictionnaire pratique du droit humanitaire, MSF
https://dictionnaire-droit-humanitaire.org/content/article/2/immunite/
Tribunal pénal international pour l'ex-Yougoslavie (TPIY), Le Procureur c. Blagoje Simić et autres, affaire n° IT-95-9-PT, Décision relative à la requête de l'Accusation en application de l'article 73 du Règlement concernant la déposition d'un témoin (Chambre de première instance II), 27 juillet 1999, par. 73

[940] "Action by the International Committee of the Red Cross in the event of violations of international humanitarian law or of other fundamental rules protecting persons in situations of violence", *International Review of the Red Cross*, Vol.87, No.858, 2005, p.393-400

[941] LA ROSA, Anne-Marie, « Le CICR et la Cour pénale internationale : deux approches distinctes mais complémentaires pour veiller au respect du droit international humanitaire », CICR, 03/03/2009 https://www.icrc.org/fr/doc/resources/documents/interview/international-criminal-court-interview-101008.htm

[942] DEBUF, Els "Tools to Do the Job: The ICRC's Legal Status, Privileges and Immunities", *International Review of the Red Cross*, Vol. 97, No. 897–898, 2015, pp. 321–329

analogues, ceci serait susceptible non seulement de compromettre la capacité de l'organisation à recueillir des informations importantes et à discuter avec les parties d'accusations de violations ou à les entretenir de toute autre préoccupation humanitaire, mais, très probablement, de lui interdire totalement d'y procéder. »[943]

On peut quant à nous remarquer qu'on a fait jusqu'à présent l'hypothèse qu'assurer la confidentialité de ses données peut compliquer l'allocation de l'aide. Ou du moins, on a supposé qu'un État peut s'opposer à l'action d'une ONG sur son territoire si elle ne lui communiquait pas certaines informations qu'elle détenait. Le CICR raisonne de façon tout à fait opposée : la confidentialité devient une condition d'accès au terrain. Cette approche lui permettrait, selon le CICR, d'assurer la confiance des acteurs présents sur place. Lier accès et confidentialité est une posture qui est propre au CICR. L'UNHCR, en tant qu'organisation internationale, bénéficie aussi de privilège et immunité, garantissant la confidentialité de ses échanges. Mais comme le remarque Privacy International, et comme on a pu le voir, l'organisation effectue un travail commun d'enregistrement des demandeurs d'asile. Et il est bien plus amené à échanger des données avec les gouvernements. Cela dit, l'approche du CICR lui a également valu des reproches. Il a par exemple été très lourdement critiqué pour son silence et son absence de dénonciations publiques au sujet des déportations de personnes juives lors de la Seconde Guerre mondiale[944]. Toutefois, cette posture n'est pas absolue : le CICR peut choisir dans de rares cas — à la suite de négociations internes — de sortir de sa réserve et opter pour des « modes d'action subsidiaires », voire des formes de dénonciations publiques de violation du droit international humanitaire[945]. Par exemple en 2013, le CICR a fini par communiquer publiquement lors du jugement de terroristes du 11/09 le contenu de rapports de ses visites à des détenus de Guantanamo[946].

Enfin, dernier point crucial, en dépit de l'importance que revêt la confidentialité pour l'organisation, le CICR insiste vivement sur le fait qu'il n'a pas à appliquer le RGPD du fait de ses privilèges et immunités. La position du CICR est partagée par l'ONU, qui a plaidé auprès du Comité européen à la protection des données (CEPD) pour la reconnaissance de l'interprétation d'une « non-application » du RGPD[947]. En guise de réponse, le CEPD a confirmé que « l'application du RGPD est sans préjudice des dispositions du droit international, telles

---

[943] « Le privilège du CICR de ne pas divulguer des informations confidentielles », *Revue Internationale de la Croix Rouge*, Volume 97, 2015/1 & 2 https://international-review.icrc.org/sites/default/files/12-cicr-97-2015_1-2-memorandum.pdf

[944] CARDIA VONECHE, Isabelle, « Revisiter le silence du Comité international de la CroixRouge (CICR) face aux déportations », *Témoigner. Entre histoire et mémoire*, 134, 2022, http://journals.openedition.org/temoigner/10926

[945] "Action by the International Committee of the Red Cross in the event of violations of international humanitarian law or of other fundamental rules protecting persons in situations of violence", International Review of the Red Cross, Vol.87, No.858, 2005, p.393-400

[946] BUSSARD, Stéphane, « Brèche dans la confidentialité des rapports du CICR sur les détenus de Guantanamo », Le Temps, 10/11/2015 https://www.letemps.ch/monde/breche-confidentialite-rapports-cicr-detenus-guantanamo
EARNEST, Thomas, "ICRC's Public Reply Regarding Order to Turn Over Confidential Reports to Military Commission", *Just Security*, 19/11/2013 https://www.justsecurity.org/3444/icrcs-public-reply-order-turn-confidential-reports-military-commission/
US ordered to hand over Red Cross files on conditions a Guantanamo Bay, The Guardian, 06/11/2013, https://www.theguardian.com/world/2013/nov/06/us-red-cross-files-conditions-guantanamo

[947] "United Nations, Impact of the European Union's data protection regulations on the Activities of UN system Organizations", EDPB, 14/05/2020https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/2020.05.14_letter_to_edpb_chair_with_un_comments_on_guidelines_2-2020.pdf

que celles régissant les privilèges et immunités des missions diplomatiques et des postes consulaires hors UE, ainsi que des organisations internationales. »[948]

Pour clarifier cette position, on se référera à l'argumentation d'un des DPO du CICR, Massimo Marelli [949] . Tout d'abord, il rappelle que les privilèges et immunités permettent l'accomplissement efficace du mandat de l'organisation internationale. Il fait ainsi remarquer que les OI agissent à l'échelle internationale, et appliquer le droit régional ou national en matière de protection des données signifierait une surcharge administrative résultant de la mise en conformité aux différents cadres législatifs, parfois contradictoires. En outre, pour lui, différentes mesures du RGPD portent potentiellement atteinte au principe de confidentialité cher au CICR.

Lors du processus de vote du RGPD, le CICR avait fait part aux institutions européennes de ses inquiétudes relatives à ce sujet : « Le CICR a indiqué que le projet de règlement pouvait susciter trois préoccupations différentes. La première concerne l'incidence que certaines dispositions du projet de règlement pourraient avoir sur la confidentialité des données à caractère personnel traitées par le CICR. Le mandat du CICR, en particulier, exige que le CICR, dans certaines circonstances, traite certaines catégories de données à caractère personnel comme confidentielles, alors que le projet de règlement imposerait certaines obligations de divulgation. Selon le CICR, ces dispositions pourraient constituer une entrave à l'accomplissement du mandat du CICR tel qu'il lui a été conféré par les traités de droit international humanitaire. » [950]

En clair, plusieurs points semblent poser problème au CICR. Tout d'abord, les pouvoirs d'investigation accordés aux autorités de protection des données peuvent contredire l'approche du CICR, notamment en matière de contrôle a posteriori du respect du RGPD. La notification de fuite de données fait également partie des points de tension, puisqu'il s'agit éventuellement de communiquer des données de l'organisation aux autorités. Notons tout de même que l'organisation a fait preuve d'une relative transparence en communiquant de façon plutôt directe sur sa cyberattaque en 2022. Enfin, le droit d'accès des personnes concernées à leurs données est également problématique pour le CICR, comme l'organisation en avait fait part au Conseil de l'Europe[951]. Et de fait, la politique de protection des données du CICR

[948] "The application of the GDPR is without prejudice to the provisions of international law, such as the ones governing the privileges and immunities of non-EU diplomatic missions and consular posts, as well as international organisations." Guidelines 05/2021 on the interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, 14/02/2023https://edpb.europa.eu/system/files/2023-02/edpb_guidelines_05-2021_interplay_between_the_application_of_art3-chapter_v_of_the_gdpr_v2_en_0.pdf

[949] MARELLI, Massimo, "The law and practice of international organizations' interactions with personal data protection domestic regulation: At the crossroads between the international and domestic legal orders", *Computer Law & Security Review*, Volume 50, 2023.

[950] « The ICRC has indicated that the draft Regulation may give rise to three different concerns. A first concerns relates to the certain provisions of the draft Regulation may have on the confidentiality of personal data processed by the ICRC. The ICRC's mandate, in particular, requires the ICRC, in some circumstances, to treat certain categories of personal data as confidential, while the draft Regulation would impose certain obligations of disclosure. According to the ICRC, these provisions could constitute an impediment to the performance of ICRC's mandate as conferred on it in international humanitarian law treaties. » Council of the European Union," Applicability of the General Data Protection Regulation to the activities of the International Committee of the Red Cross", Brussels, 25/03/2015 https://data.consilium.europa.eu/doc/document/ST-7355-2015-INIT/en/pdf

[951] "Restrictions on specific principles and on the rights of information, access, rectification and erasure or on the right to data portability, the right to object, measures based on profiling, as well as on the communication of a personal data breach to a data subject and on certain

mentionne des restrictions à ce droit qu'on ne retrouve pas dans le RGPD. On peut ainsi y lire que le droit d'accès aux données doit être refusé « lorsque des motifs d'intérêt public prépondérants l'imposent », dont le respect du principe de confidentialité. Notons que le RGPD ménage tout de même des marges permettant au responsable de traitement de s'opposer aux demandes d'accès (surtout si l'organisme estime que la demande est infondée ou excessive, et à condition de justifier cette appréciation)[952].

Enfin, plus généralement, on peut noter d'autres points de friction entre le RGPD et le mandat du CICR, comme a pu nous l'indique un enquêté : « *au CICR, on est aussi garant du DIH, si on a des preuves de violation du DIH, nos règles nous permettent si une personne vient nous voir pour supprimer les données et qu'on en a besoin pour prouver une violation, on peut émettre une objection, et on va garder ces données-là parce qu'elles vont pouvoir aider à prouver qu'un crime de guerre a été commis. (…) cela est permis parce qu'on a des privilège et immunité et un décalage par rapport au droit national* ». [953]

Cela étant, la non-application du texte ne découle pas simplement de l'argumentation du CICR. En tout cas, pour Massimo Marelli, le règlement lui-même contient des indications relatives à ce sujet. Certes, l'article 2 (2) du règlement, qui liste l'ensemble des cas où ce dernier ne s'applique pas, ne mentionne pas les OI[954]. Cela semble indiquer qu'elles sont concernées par le règlement. Néanmoins, Massimo Marelli interprète différemment cet article. Selon lui, il désigne l'ensemble des acteurs pour lesquels l'application du règlement est tout bonnement impossible et non pas l'ensemble des acteurs non concernés par le RGPD : « Il convient de souligner que l'article 2 fournit une liste d'activités de traitement auxquelles le RGPD est inapplicable, et non une liste d'acteurs auxquels il ne s'applique pas. »[955]

---

related obligations of the controllers may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of human life especially in response to natural or man-made disasters, the prevention, investigation and prosecution of criminal offences or of breaches of ethics for regulated professions, other public interests of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, the keeping of public registers kept for reasons of general public interest, further processing of archived personal data to provide specific information related to the political behaviour under former totalitarian state regimes or the protection of the data subject or the rights and freedoms of others, including social protection, public health and humanitarian purposes, such as the performance of a task incumbent upon the International Red Cross and Red Crescent Movement under the Geneva Conventions. " https://data.consilium.europa.eu/doc/document/ST-8837-2015-INIT/en/pdf Council of the European Union, Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Applicability of the General Data Protection Regulation to the activities of the International Committee of the Red Cross (ICRC), 12/05/2015

[952]« Le droit d'accès aux données doit être refusé lorsque des motifs d'intérêt public prépondérant l'imposent. Parmi ces motifs figurent notamment : a) le respect de la confidentialité, une méthode de travail essentielle pour le CICR. » Règles du CICR en matière de protection des données personnelles, 2020https://www.icrc.org/fr/publication/4261-icrc-rules-on-personal-data-protection

[953] Entretien n° 93, OI2, 02/06/2022

[954] Article 2 (2) , Champ d'application matériel : Le présent règlement ne s'applique pas au traitement de données à caractère personnel effectué : a) dans le cadre d'une activité qui ne relève pas du champ d'application du droit de l'Union; b) par les États membres dans le cadre d'activités qui relèvent du champ d'application du chapitre 2 du titre V du traité sur l'Union européenne; c) par une personne physique dans le cadre d'une activité strictement personnelle ou domestique; d) par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre des menaces pour la sécurité publique et la prévention de telles menaces. https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre1

[955] « It should be highlighted that Article 2 provides a list of processing activities to which GDPR is inapplicable, not a list of actors to whom it shall not apply. » MARELLI, Massimo, "The law and practice of international organizations' interactions with personal data protection domestic regulation: At the crossroads between the international and domestic legal orders", *Computer Law & Security Review*, Volume 50, 2023.

Autre argument, les OI sont toujours associées non pas à des entités privées, mais à des « pays tiers »[956], qui n'ont pas à appliquer le RGPD, ces derniers restant ainsi souverains sur leurs données. Et comme l'avance Massimo Marelli : « Une lecture attentive du texte et de l'architecture du RGPD permet de conclure qu'il n'a pas été rédigé pour s'appliquer aux OI. Aucun article du RGPD n'impose explicitement d'obligations légales aux OI. Chaque fois que les OI sont mentionnées, elles le sont dans les mêmes termes que les pays tiers, auxquels le RGPD ne s'applique pas. »[957]

Massimo Marelli alerte cependant sur deux articles qui lui paraissent contenir des points de flou. L'article 3 (2)[958] relatif au champ d'application du RGPD ne précise pas s'il applique aux OI et aux pays tiers, et pour le DPO : « cela crée des chevauchements possibles et des questions quant à l'interprétation du RGPD dans les cas où une entité qui n'est pas établie dans l'UE est tenue d'appliquer le RGPD en vertu de l'article 3, paragraphe 2, et a également besoin de recevoir des données. En particulier, on peut légitimement se demander si, dans de tels cas, le chapitre V s'applique aux transferts vers ces entités, bien qu'elles soient déjà tenues d'appliquer le RGPD en vertu de l'article 3, paragraphe 2. » [959]

Enfin, l'article 44 du RGPD peut donner lieu à des interprétations en faveur d'une applicabilité aux OI. Il concerne les mesures à appliquer pour les transferts de données à des OI et à des pays tiers. La dernière partie de l'article spécifie que : « les conditions définies dans le présent chapitre sont respectées par le responsable du traitement et le sous-traitant, y compris pour les transferts ultérieurs de données à caractère personnel au départ du pays tiers ou de l'organisation internationale vers un autre pays tiers ou à une autre organisation internationale. » Cela signifierait que le pays tiers ou l'OI doivent appliquer le RGPD à des transferts ultérieurs de données ?

Mais pour Massimo Marelli cette interprétation n'est pas juste : « Il est clair que cette disposition exigeant de l'entité transférante qu'elle veille à ce que tout transfert, y compris les transferts ultérieurs, soit "protégé" en vertu du chapitre V, s'applique à la partie transférante initiale, c'est-à-dire aux responsables du traitement et aux sous-traitants au sens du RGPD qui

[956] Un pays tiers est un pays qui n'est pas lié par le règlement général sur la protection des données (RGPD), contrairement aux 28 États membres de l'UE et aux trois pays de l'Espace économique européen (EEE), la Norvège, le Liechtenstein et l'Islande

[957] « A careful reading of the text and the architecture of GDPR leads to the conclusion that it was not drafted to apply to IOs. No article in GDPR explicitly imposes legal obligations on IOs. On each occasion where IOs are mentioned, they are referred to in the same terms as third countries,to whom GDPR does not apply. »
MARELLI, Massimo, *ibid*.

[958] Article 3 (2) : Le présent règlement s'applique au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées : a) à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes; ou b) au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union. https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre1#Article3

[959]« this does create possible overlaps and questions as to the interpretation of the GPDR for cases in which an entity that is not established in the EU is required to apply the GDPR by virtue of Art 3(2), and also needs to receive data. In particular, it may legitimately be asked whether in such cases, Chapter V applies for transfers to such entities, despite them already being required to apply the GDPR by virtue of 3(2). »Feedback to Guidelines 05/2021 on the interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/ICRC%20DPO%20Feedback%20to%20Guidelines%205-2021_30.01.2022.pdf

cherchent à transférer des données à caractère personnel vers des OI et/ou des pays tiers en premier lieu, et non au destinataire dans un pays tiers de l'OI réceptrice. » [960]

Il n'empêche que transférer des données à une OI requiere d'appliquer le même test d'équivalence qu'aux pays tiers et implique la nécessité d'adopter un cadre normatif de type « droit souple » en interne : « Une fois cet objectif établit, et compte tenu du fait que l'immunité de juridiction signifie que les lois nationales ne peuvent pas être appliquées aux OI, les lois nationales indiquent alors que tout transfert vers un pays tiers ou une OI est interdit, à moins que les conditions de protection spécifiques et supplémentaires énoncées dans les dispositions pertinentes régissant les transferts internationaux (par exemple, le chapitre V du RGPD) ne soient respectées. Ces mécanismes visent à garantir que, même si les données à caractère personnel sortent du cadre protecteur de l'ordre juridique national, le niveau de protection qu'il offre est maintenu et n'est pas remis en cause. » [961]

La non-application du RGPD exige donc que l'organisation « respecte » dans les formes le droit national et régional, comme le rappelle Massimo Marelli. D'où la nécessité de mettre en place un cadre de droit souple et un mécanisme de redevabilité interne. Ce point est rappelé en entretien : « les gens qui ont travaillé là-dessus ont été inspirés, sauf erreur, par l'histoire qui a eu lieu en France quand Interpol avait été questionné par la CNIL vis-à-vis la position d'une organisation internationale qui a ses privilèges et immunités, vis-à-vis de lois, en particulier la loi sur la protection des données européenne, dans laquelle le pays a aussi des responsabilités vis-à-vis des citoyens, même si le "territorial scope" est plus large, ça c'était intéressant et on s'est dit, attention on a beau être une organisation internationale, on a certainement des obligations légales et ça a permis de créer le bureau de la protection des données et la commission qui permet d'avoir une cour. »[962]

Ainsi, le CICR s'est doté en 2016 d'une politique de protection des données. Elle permettrait de réconcilier deux impératifs : l'impératif de protection et le respect des privilèges et immunités[963]. Le RGPD lui sert largement de référence[964]. Il s'agit cependant d'une version adaptée du règlement : certains points diffèrent, notamment concernant les droits des

---

[960]"The law and practice of international organizations' interactions with personal data protection domestic regulation: At the crossroads between the international and domestic legal orders", I, Volume 50,2023, 105849 It is clear that this provision requiring the transferring entity to ensure that any transfer, including onward transfers, are 'protected' under Chapter V applies to the initial transferring party, i.e. the controllers and processors under GDPR who seek to transfer personal data to IOs and/or third countries first, and not on the recipient in a third country of the receiving IO." MARELLI, Massimo,*ibid*.

[961] having established this objective, and taking into account that immunity from jurisdiction means that the domestic laws cannot be enforced against IOs— domestic laws then indicate that any transfer to a third country or an IO is prohibited unless the specific, additional protective conditions set out in relevant provisions regulating international transfers (e.g. Chapter V of the GDPR) are complied with. These mechanisms seek to ensure that even as personal data exits the protective umbrella of the domestic legal order, the level of protection afforded therein is maintained and not undermined"MARELLI, Massimo, *ibid.*
WIEWIOROWSKI, Wojciech, 'International Organisations Demonstrate Dedication to Data Protection'17 July 2018 https://www.edps.europa.eu/press-publications/press-news/blog/international-organisations-demonstrate-dedication-data_en

[962] Entretien n° 93, OI2, DPO, 02/06/2022

[963]FRED H, Cate; CHRISTOPHER, Kuner; DAN JERKER, Svantesson; LYNSKEY, Orla; MILLARD, Christopher, "Data Protection and Humanitarian Emergencies"2017, Maurer Faculty. 2644. https://www.repository.law.indiana.edu/facpub/2644

[964]MARELLI, Massimo, *ibid*, « In certain areas EU law has become the leading model that other countries and international organizations seek to emulate ; data protection is a good example of this. Dozen of data protection laws in all regions of the world have been inspired by the EU model, and international organizations such as the Office of the United Nations High Commissioner for Refugees (UNHCR) and the International Committee of the Red Cross (ICRC) have also turned to EU law as an important source of inspiration when adopting data protection policies and guidelines. In 2017 the ICRC and the Brussels Privacy Hub also published a handbook on data protection and humanitarian action based on a number of internationally recognized data protection standards, including those of EU law. As such policies become more widely adopted, they may lead to the gradual crystallization of international law based on EU standards. »

bénéficiaires, comme on le verra dans le dernier chapitre de la thèse. Une commission interne a été mise en place, pour servir d'équivalent à une autorité de protection des données. Cela dit, la transparence de cette institution pose question et le juriste Asaf Lubin s'inquiète du manque de redevabilité du CICR[965]. Et le paragraphe traitant de la « redevabilité » au sein du « data protection Handbook » du CICR est réduit à sa portion congrue, à peine une dizaine de lignes dans un manuel de près de 300 pages. L'application et le respect de ce droit ne dépendaient alors que de l'organisation elle-même [966]. En somme, si les privilèges et immunités garantissent la réalisation du mandat de l'OI et s'ils offrent une forme de protection, ceci se ferait au prix d'un manque de redevabilité.

À ce stade, on peut en venir aux limites relatives aux privilèges et immunités en tant qu'outils de protection des données. Tout d'abord, malgré leur importance pour les OI, ces derniers ne sont pas acquis. Le CICR doit ainsi négocier ce qu'il nomme des « accords de siège » avec les États afin de s'assurer de leur reconnaissance. D'où un travail diplomatique : « La non-reconnaissance des privilèges et immunités conférés au CICR est l'un des défis les plus difficiles à relever. Bien que 196 États aient ratifié l'importance de la mission humanitaire du CICR exprimée dans les Conventions de Genève, en 2016, le CICR n'a obtenu le statut juridique, les privilèges et les immunités que dans 103 pays, y compris des États où le CICR n'opère pas. »[967] Quels sont les arguments des États refusant de signer ce type d'accord ? En entretien, il nous a été précisé que le CICR a du mal à faire reconnaitre ses privilèges et immunités surtout dans le cas d'« États faillis », pour reprendre l'expression utilisée par nos enquêtés, comme le Yémen ou la Syrie[968]. Et cela n'est pas sans conséquence en matière de confidentialité, comme s'en inquiète l'OIM : « L'OIM jouit de l'inviolabilité de ses locaux dans 129 (…) États sur 175. Ses biens et avoirs sont protégés dans 122 (…) États seulement, et ses archives et documents dans 127 (…) États. Cette situation met en danger la capacité de l'Organisation à exécuter ses fonctions ainsi que les avoirs payés par les États Membres. (…) Par ailleurs, l'absence d'inviolabilité des locaux, des archives et des documents est lourde de conséquences pour l'Organisation sous l'angle de la confidentialité et de la protection des données relatives aux bénéficiaires. »[969]

---

[965] LUBIN, Asaf, "Data Protection as an International Legal Obligation for International Organizations: The ICRC as a Case Study, in BUCHAN, Russell, LUBIN, Asaf (eds.), *The Rights to Privacy and Data Protection in Times of Armed Conflict*, NATO CCDCOE, 2022 https://ssrn.com/abstract=4115810

[966] DOMINICE, Christian, « La nature et l'étendue de l'immunité de juridiction des organisations internationales, In : L'ordre juridique international entre tradition et innovation », Genève : Graduate Institute Publications, 1997 https://books.openedition.org/iheid/1343?lang=fr

BOON, K. E., MEGRET, F., "New Approaches to the Accountability of International Organizations", *International Organizations Law Review*, *16*(1), 1-10. 2019, https://brill.com/view/journals/iolr/16/1/article-p1_1.xml?language=en

EISEMANN, Pierre Michel, SAROOSHI, Dan, (dir.), *Mesures de réparation et responsabilité à raison des actes des organisations internationales / Remedies and responsibility for actions of international organizations*, 2014, Académie de droit international de La Haye http://www.diva-portal.se/smash/get/diva2:1246433/FULLTEXT01.pdf

BERGOTA SANDVIK ,Kristin, Lindskov Jacobsen, Katja, *UNHCR and the Struggle for Accountability, Technology, law and results-based managemen*t, London: Routledge, 2016, 194 p.

diplo, Geneva internet platform, Data talks november 2017 : GDPR and data immunities, november 2017 https://www.diplomacy.edu/sites/default/files/DataTalks_November17.pdf

TWIGT, Mirjam, Doing Refugee Right(s) with Technologies? Humanitarian Crises and the Multiplication of "Exceptional" Legal States, *Refugee Survey Quarterly*, 2023;, hdad020, https://doi.org/10.1093/rsq/hdad020

[967] LE BLOND, Stevens, CUEVAS, Alejandro, TRONCOSO-PASTORIZA, Juan Ramon, JOVANOVIC, Philipp, FORD, Bryan, HUBAUX, Jean-Pierre, "On Enforcing the Digital Immunity of a Large Humanitarian Organization",2018 IEEE Symposium on Security and Privacyhttps://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8418617

[968] Entretien n° 7, OI2, DPO, 11/12/2019

[969] OIM, Privilèges et immunités, comité permanent des programmes et des finances, douzième session, 13-14 mai 2013 https://www.iom.int/sites/g/files/tmzbdl486/files/2019-01/SCPF_96_7.pdf

En outre, une fois les accords signés, le respect de ces derniers n'est jamais tout à fait acquis. Cela est flagrant concernant les activités de renseignements touchant les organisations internationales. Les États-suniens ainsi que les Britanniques, pour ne citer qu'eux, ont, par exemple, à de multiples reprises, placé sous écoute les personnels et les communications de l'ONU[970]. L'ampleur de ces opérations et de ces interceptions peut être discutée. Toujours est-il que Philippe Bolopion, l'actuel directeur de cabinet d'Human Rights Watch, s'exprime sans concession sur ce sujet dans une courte dépêche pour le monde, publiée en 2008. L'écoute de personnel onusien serait une pratique courante : « Ce n'est qu'en 1946 qu'a été adoptée la Convention sur les privilèges et immunités de l'ONU, qui déclare que les locaux de l'organisation sont *"inviolables"* et doivent rester exempts de toute forme d'*'interférence »*. Cette convention est depuis violée, sans grandes conséquences : chaque fois qu'un faux diplomate ou journaliste est pris en flagrant délit d'espionnage, il est discrètement renvoyé dans son pays. »[971] Et surtout, le respect des privilèges et immunités est d'autant plus fragile que son application dans le cyberespace n'est pas assurée, ce qui laisse les OI potentiellement vulnérables dans des cas de cyber-opérations — comme le notent Robin Denys-Sacha, Gérard Cahin et Evelyne Lagrange[972].

À ce sujet, dès 2012, le CICR s'inquiétait des difficultés accrues pour respecter le principe de confidentialité cher à l'organisation dans un contexte de transformation numérique : « L'essor et la diversification rapides de technologies de l'information toujours plus performantes et complexes à contrôler : il devient de plus en plus difficile de garantir qu'une information confidentielle, traitée par le CICR dans le cadre d'un dialogue bilatéral avec des autorités, ne fasse pas l'objet de fuites volontaires ou involontaires, internes ou par une tierce partie, malgré les mesures de protection techniques et humaines mises en place pour les éviter. »[973] Et il est vrai que les privilèges et immunités ont été pensés pour un monde pré-internet comme le remarque Massimo Marelli : « ces privilèges et immunités, élaborés en tant que concept juridique à l'ère pré-internet, devront peut-être être adaptés et des clarifications seront peut-être nécessaires quant à leur interprétation et leur application dans un environnement numérique. En particulier, il est important de clarifier l'application de ces privilèges et immunités pour inclure les données (en transit ou au repos) stockées et traitées non seulement par l'organisation humanitaire directement, mais aussi par un prestataire de

---

[970] STARKS, Tim, DEYOUNG, Karen, "U.S eavesdropped on U.N secretary general, leaks reveal",*The WashingtonPost*,17/04/2023, https://www.washingtonpost.com/national-security/2023/04/15/united-nations-leaked-documents/
BOOTH, Robert, BORGER, Julian, "US diplomats spied on UN leadership", *The Guardian,* 28/11/2010 https://www.theguardian.com/world/2010/nov/28/us-embassy-cables-spying-un
Daily Press Briefing by the Office of the Spokesperson for the Secretary-General, 29/11/2010
https://press.un.org/en/2010/db101129.doc.htm
UPI archive, U.N to Britain: if spying on us, stop it, 26/02/2004 https://www.upi.com/Archives/2004/02/26/UN-to-Britain-If-spying-on-us-stop-it/8241077771600/

[971] BOLOPION, Philippe, « L'ONU, « un nid d'espions », *Le Monde*, 10/03/2008https://www.lemonde.fr/international/article/2008/03/10/l-onu-un-nid-d-espions_1021042_3210.html#

[972] DENYS-SACHA, Robin, CAHIN, Gérard, LAGRANGE, Évelyne, « « Les cyberattaques contre les organisations internationales. In: *Annuaire français de droit international*, volume 64, 2018. pp. 383-392.
Les institutions européennes sont également très ciblées, une tendance en augmentation d'après les dires du CERT-EU
BODNAR, Bogdan, Cyberattaques ciblant l'Union européenne : » C'est essentiellement de l'espionnage », *Numérama,* 24/05/2022
https://www.numerama.com/cyberguerre/969411-cyberattaques-ciblant-lunion-europeenne-cest-essentiellement-de-lespionnage.html
Dernier exemple en date, une campagne de phishing ciblant des diplomates européens avec un mail d'invitation de dégustation de vin.
SINGH, Sudeep, TAY, Roy, European diplomats targeted by spikedwine with wineloader, Zscaler, 27/02/2024 https://www.zscaler.com/blogs/security-research/european-diplomats-targeted-spikedwine-wineloader

[973] Doctrine sur l'approche confidentielle du Comité international de la Croix- Rouge (CICR)
Moyen spécifique du CICR pour obtenir des autorités étatiques et non étatiques le respect du droit, Revue internationale de la croix rouge, vol 94, 2012/3 https://www.icrc.org/fr/doc/assets/files/review/2012/icrc-88-confidentiality-fre.pdf

services tiers ou une organisation distincte. Cela devrait inclure les données hébergées ou traitées d'une autre manière par des fournisseurs de technologie tiers pour le compte de l'organisation, ainsi que les serveurs et les réseaux utilisés par l'organisation, qu'ils appartiennent à l'organisation ou à un fournisseur de services tiers. » [974]

Cependant, une partie de la littérature considère que le principe d'inviolabilité des archives et de la correspondance diplomatique (art. 22 et 24) assuré par la Convention de Vienne est suffisant pour protéger les mails et les données stockées sur les ordinateurs (qui sont des biens des ambassades)[975]. Autre argument, toujours d'après ces textes juridiques les biens et locaux d'une OI sont inviolables, où qu'ils se trouvent et quel qu'en soient les détenteurs[976], ce qui pour les juristes Russell Buchan et Nicholas Tsagourias va dans le sens d'une applicabilité de la Convention de Vienne à l'espace numérique : « Il est important de noter que les biens et les actifs sont protégés "où qu'ils se trouvent et quel qu'en soit le détenteur". Cela signifie que les données stockées par les OI dans le nuage sont protégées contre les ingérences même si elles résident sur des réseaux et des systèmes informatiques soutenus par une infrastructure numérique située sur le territoire d'un autre État et indépendamment du fait que cette infrastructure soit détenue ou exploitée par le secteur public ou privé. On peut supposer que les "biens" et les "actifs" d'une OI doivent être identifiables en tant que tels pour qu'elle bénéficie d'une protection contre les ingérences. »[977]

Mais le chercheur Nick Robinson, qui a travaillé sur l'ambassade numérique estonienne au Luxembourg, est moins assuré de ce point : « Eileen Denza (2016) a soutenu que les archives et les documents d'une mission diplomatique sont inviolables sous quelque forme que ce soit et où qu'ils se trouvent (et cela est donc interprété comme incluant les formes modernes de stockage de l'information — telles que les dispositifs de stockage externes). Mais à une époque où les réseaux de communication et les flux de données sont de plus en plus complexes, les mêmes principes et la même interprétation du droit diplomatique s'appliquent-ils ? »[978]

---

[974]"these privileges and immunities, developed as a legal concept in a pre-internet era, may need to be adapted, and clarifications may be required as to their interpretation and application in a digital environment. In particular, it is important to clarify the application of these privileges and immunities to include data (in transit or at rest) stored and processed not only by the humanitarian organization directly, but by a third-party service provider or separate organization. This should include data that is hosted or otherwise processed by third-party technology providers on behalf of the organization, as well as the servers and networks used by the organization, regardless of whether they belong to the organization or to a third-party service provider. " MARELLI, Massimo, "Hacking humanitarian: moving towards a humanitarian cybersecurity strategy", *Humanitarian Law&Policy*, ICRC blog, 16/01/2020 https://blogs.icrc.org/law-and-policy/2020/01/16/hacking-humanitarians-cybersecurity-strategy/

[975]PATRICIO GRANÉ, Labat, BURKE, Naomi, "The Protection of Diplomatic Correspondence in the Digital Age: Time to Revise the Vienna Convention?', in BEHRENS, Paul (ed.), *Diplomatic Law in a New Millennium*, Oxford, 2017,p.204-230https://doi.org/10.1093/oso/9780198795940.003.0013

[976] « Les locaux de l'Organisation sont inviolables. Ses biens et avoirs, où qu'ils se trouvent et quel soit leur détenteur sont exempts de perquisition, réquisition, confiscation, expropriation ou de toute autre forme de contrainte exécutive, administrative, judiciaire ou législative. https://treaties.un.org/doc/source/docs/III-1-in-French.pdf

[977]« Importantly, property and assets are protected "wherever located and by whomsoever held." This means that data stored by IOs in the Cloud is protected from interference even though it resides on computer networks and systems supported by cyber infrastructure located within the territory of another State and regardless of whether that infrastructure is publicly or privately owned or operated. Presumably, an IO's "property" and "assets" must be identifiable as such for it to enjoy protection from interference. »BUCHAN, Russell, TSAGOURIAS, Nicholas, "hacking international organizations : the role of privileges and immunities", Articles of war, 14/12/2021 https://lieber.westpoint.edu/hacking-international-organizations-privileges-immunities/

[978] « Eileen Denza (2016) has argued that the archives and documents of a diplomatic mission are inviolable in whatever form they are and wherever they may be (and it is thus interpreted to include modern forms of information storage – such as external storage devices). But in

Et effectivement, comment s'assurer de l'application des privilèges et immunités à l'informatique en nuage ? Un cloud consiste à externaliser la gestion des données d'une organisation, qui ne sont plus directement stockées sur les serveurs de cette dernière. Elles sont alors gérées par un prestataire technique. Un fournisseur de service met à disposition d'un utilisateur ses propres capacités de calcul et de stockage[979]. Cette option technique est considérée comme plus efficace, agile, économique, etc. Les coût de maintenance du système d'information d'une organisation ne pesant pas directement sur cette dernière. Mais l'informatique en nuage inquiète les défenseurs de la vie privée : les clouds impliquent une externalisation des systèmes d'information d'une organisation à un acteur tiers, d'où le fait qu'il soit difficile de conserver la main sur les modalités de conservation des données. Le cloud repose sur une délocalisation des ressources numériques dont la gestion ne se fait plus en interne. De surcroit, un fournisseur de cloud peut choisir de stocker les données d'un Cloud dans plusieurs datacenter dépendant différentes juridictions. Le choix du lieu de stockage se faisant en fonction de facteurs économiques et techniques[980], dont l'utilisateur n'a pas toujours connaissance. Il reste ainsi difficile pour ce dernier de déterminer où sont conservées ses données. Le Cloud repose sur un fonctionnement mondialisé, échappe aux souverainetés étatiques, et l'ensemble de ses composantes peuvent se retrouver dans des territoires différents (et donc avec des systèmes de juridiction différents et des gouvernements n'ayant pas le même positionnement vis-à-vis des Conventions de Genève). D'où un mouvement de territorialisation du Cloud[981], au niveau régional ou national, n'ayant pour le moment pas entamé l'hégémonie américaine.

Or, l'usage du cloud en entreprise et dans les organisations a connu une forte augmentation, en lien avec la production accrue de données. Selon des chiffres de l'agence européenne de statistique, fin 2023, 45 % des entreprises auraient recours à de l'informatique nuagique à l'échelle de l'Union, avec de fortes disparités entre pays.

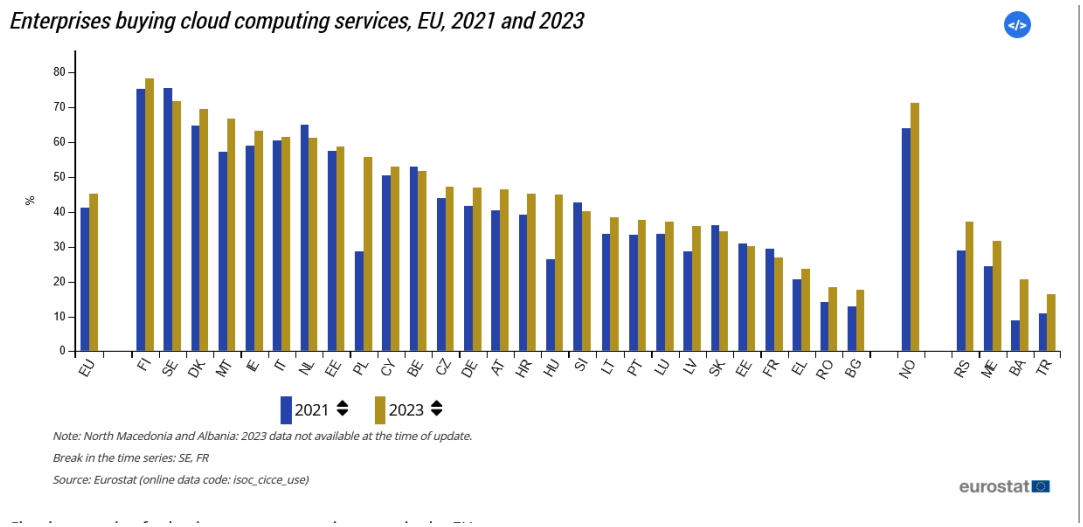
---

an age of increasingly complex communication networks and data flows, do the same principles and interpretation of diplomatic law apply."ROBINSON, Nicholas, David," Distributed denial of government, the data embassy and the legal and legal implications of extraterritorial data storage", Doctoral Thesis, philosophy, University of London, 2020 https://pure.royalholloway.ac.uk/ws/portalfiles/portal/44682853/2020_Robinson_N_PhD.pdf

[979] Il existe plusieurs type de service de Cloud, selon des degrés d'externalisation. On en distingue généralement trois :• Le IaaS (Infrastructure as a Service) : dans ce service le prestataire met à la disposition de son client l'espace de stockage et la puissance de traitement de son infrastructure informatique. Il se charge seulement de la gestion de l'infrastructure (serveurs, connexions réseau, résilience, bande passante…) ;Le PaaS (Platform as a Service) : dans ce service, le prestataire fournit aussi à l'utilisateur les systèmes d'exploitation et les logiciels de traitement de bases de données lui permettant de développer et/ou de gérer les applications et les outils de son choix. Le client ne s'occupe plus de la mise en place et de la maintenance des plateformes nécessaires au déploiement de ce type d'opération ; Le SaaS (Software as a Service) : ce service correspond au fait que le prestataire gère l'ensemble du dispositif informatique, jusqu'aux applications qu'il héberge lui-même et qu'il met à la disposition de son client.

[980] https://www.ibm.com/fr-fr/topics/cloud-storage

[981] « Les volontés d'émancipation du joug américain se renforcent à mesure que les autres gouvernements réalisent les impacts de l'ascendant structurel des États-Unis sur l'informatique en nuage. Ils tentent donc de les contourner en proposant des solutions nationales ou régionales qui garantiraient un meilleur contrôle de l'accessibilité aux données et protégeraient leur souveraineté. Il s'agit d'une forme de territorialisation du cloud qui peut s'opérer, en fonction de l'échelle, par le recours à des entreprises nationales et régionales, par l'utilisation, la construction ou la relocalisation de data centers sur leur sol ou par la mise en place de mesures juridiquement contraignantes et à portée extraterritoriale. De récents progrès dans les techniques de chiffrement (le chiffrement homomorphe, par exemple) autorisent le traitement des données sans que celles-ci soient déchiffrées, ce qui limite leur exposition. Il est alors possible d'envisager une autre forme de territorialisation qui garantirait la souveraineté sur les données par la possession de la clé de déchiffrement. » BOMONT, Clotilde, "Géopolitique du cloud défense français, analyse des nouvelles formes d'organisation spatiale du pouvoir de l'Etat à travers la construction d'un objet socio-technique", thèse de doctorat, Géographie, Université Paris 1 Panthéon Sorbonne, 2023




**ENTREPRISES EUROPEENNES UTILISANT DES SERVICES DE CLOUD COMPUTING[982]**

Et comme le rappelle un DPO du CICR, Massimo Marelli : « Les entreprises technologiques poussent de plus en plus et rapidement leur offre de logiciels et de stockage vers le nuage public et ne soutiennent plus les alternatives non basées sur le nuage, les rendant souvent obsolètes. (…) Même les logiciels acquis aujourd'hui en tant que solution sur site sont susceptibles d'être liés à des applications de cloud public et/ou de partager des données de diagnostic ou de télémétrie entre les différentes juridictions. » [983] On assisterait à une augmentation du nombre de client de cloud, tandis que le nombre de fournisseurs resterait stable, d'où un marché très concentré, et sans surprises encore dominé par les acteurs américains.

L'écosystème onusien reflète cette domination américaine, avec Microsoft comme principal fournisseur de service, selon une enquête de 2019[984].

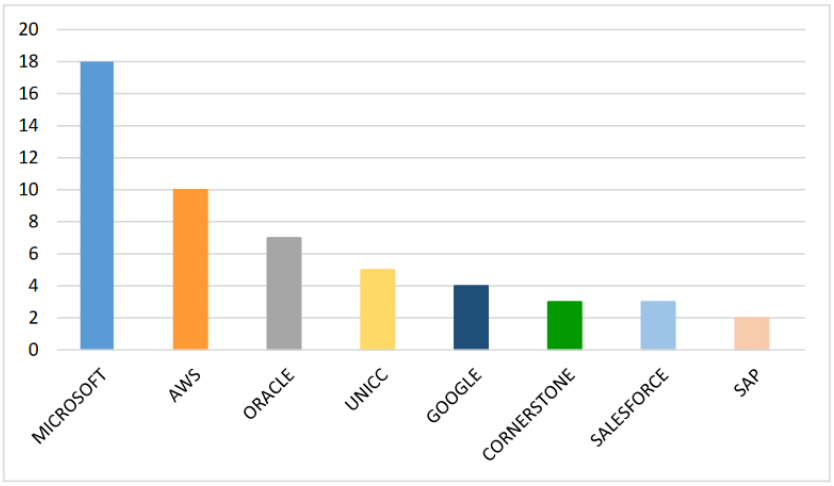
[982] "Cloud computing - statistics on the use by enterprises ", Eurosat, December 2023, https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises

[983] "technology companies are increasingly and rapidly pushing their offering of software and storage to the public cloud and are no longer supporting non-cloud-based alternatives, often rendering them obsolete. (…) Even software that is procured as an on-premise solution today is likely to be linked to public cloud applications and/or sharing diagnostic or telemetry data across jurisdictions" MARELLI, Massimo, "Hacking humanitarians: Defining the cyber perimeter and developing a cyber security strategy for international humanitarian organizations in digital transformation" *International Review of the Red Cross*. 2020;102(913):367-387

[984] CALLEJAS, Jorge, DUMITRIU, Petru, "Managing cloud computing services in the United Nations system", JIU/REP/2019/5 https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2019_5_final.pdf

Figure IV
**Cloud services providers for United Nations organizations**

(Number of organizations)




**FOURNISSEURS DE CLOUD DE L'ONU**[985]

Or recourir au Cloud place une OI dans une situation juridique délicate, surtout si des données d'une OI sont stockées dans un pays ne reconnaissant pas les privilèges et immunités de cette dernière, ou si des données sont échangées dans le cadre d'un programme avec un partenaire : « *lorsque d'autres régulations nous obligent à le faire… on va être soumis malgré nos immunités, lorsqu'on travaille avec un third party, un financial provider ou un opérateur mobile, etc., eux-mêmes sont soumis à leur propre législation, et on va pas leur demander d'être hors la loi chez eux, c'est évident, donc là il faut trouver de bons moyens, donc on va faire des DPIA, et trouver de bonnes mesures, et pouvoir faire un transfert et que la balance entre les bénéfices pour les populations affectées et les risques*. »[986]

Il faut garder à l'esprit que le sujet du Cloud est très discuté. D'un côté, l'informatique en nuage peut être considérée, dans une certaine mesure, comme plus sécurisée, puisqu'il repose sur un principe d'externalisation de la cybersécurité. Il permettrait de se reposer sur des acteurs ayant plus de compétences, sans avoir à gérer le travail de sécurisation des réseaux en interne. D'un autre côté, le cloud et l'externalisation des services informatiques de façon plus générale représentent un risque de perte de contrôle de l'information.

Notons bien que pour jouir de privilèges et immunités, les données doivent être labélisées comme appartenant à une OI. Autre point, ces dernières ne bénéficient plus du statut propre à l'OI, comme le notent Russell Buchan et Nicholas Tsagourias : « lorsqu'un OI transmet des données à un autre acteur ou partage des données avec lui et, ce faisant, en abandonne le contrôle, ces données ne peuvent plus être décrites comme "appartenant" ou "détenues par" l'OI. »[987] Et dans le cas d'une sous-traitance, à partir de quand considère-t-on que l'OI abandonne en partie le contrôle des données ? Les risques liés à l'informatique en nuage relatifs au respect des privilèges et immunités n'ont pas échappé aux juristes d'organisations

[985] CALLEJAS, Jorge, DUMITRIU, Petru, ibid.
[986] Entretien n° 93, OI 2, DPO, 02/06/2023
[987] "The caveat, however, is that where an IO passes data to or shares data with another actor and, in doing so, relinquishes control over it, those data can no longer be described as "belonging to" or "held by" the IO", BUCHAN, Russell, TSAGOURIAS, Nicholas, ibid.

internationales. Lors d'une conférence sur le cloud organisé par l'ONU, une participante met en exergue cette problématique : « Globalement, le grand défi pour les organisations internationales est qu'elles ont l'impression de n'avoir aucun contrôle sur les données. Dans le cadre traditionnel où les données sont conservées dans les locaux de l'organisation, le contrôle est plus clairement défini et le sentiment de contrôle est plus grand, alors que dans le cadre de l'informatique dématérialisée, en particulier dans le cadre de l'informatique dématérialisée publique, ce sentiment est plus fort. »[988] Pour ajouter au sentiment de manque de maitrise, l'informatique en nuage est particulièrement vulnérable aux effets de l'extraterritorialité du droit, et plus spécifiquement à une série de lois américaines, comme le Patriot Act, le FISAA[989] et le Cloud Act. Ce dernier découle d'une affaire remontant à 2013 : un procureur américain avait lancé un mandat sur la base du SCA (stored communication act, un texte datant de 1986) requérant que Microsoft communique des données d'un de leurs clients, un Irlandais poursuivi dans une affaire de trafic de drogue. Microsoft avait refusé d'obtempérer, au motif que les données du client étaient hébergées dans une antenne située hors du territoire états-unien. En réaction, l'administration américaine a publié le « C*larifying Lawful Overseas Use of Data Act »* — (Cloud Act), qui renforce les compétences des forces de l'ordre. La procédure d'enquêtes pénales est simplifiée : il n'est plus besoin de s'appuyer sur des accords de coopérations judiciaires, mécanismes décrits comme lourds. Il suffit en effet de contraindre les fournisseurs de service américains, par mandat ou assignation, à leur fournir les données, stockées sur des serveurs, situés aux États-Unis ou dans des pays étrangers, sans passer par les tribunaux (américains ou étrangers). Et du fait de « GAG order », les personnes concernées ne sont pas nécessairement informées de ces demandes[990], pratique contestée par les entreprises du Web elles-mêmes.

[988]« It is more difficult to argue as well unavailability of archives because the data are being stored by the Cloud service provider and not by the international organization themselves. In overall, the big challenge for international organizations is the fact that they feel that they have no control over the data. In the traditional setting of having the data on premises, control is more clearly defined and it's more -- the feeling of control, at least, is bigger; whereas, in the Cloud setting, especially in the public Cloud setting. »Internet Governance Forum, Managing Cloud computing in the United Nations System, 2017 https://www.intgovforum.org/en/content/igf-2017-day-1-room-xxv-of29-managing-cloud-computing-in-the-united-nations-system

[989] BOMONT, Clotilde, « Extension de la loi FISA, La « souveraineté numérique » européenne loin des préoccupations américaines », IRSEM, Brève stratégique -70, 03/06/2024 https://www.irsem.fr/media/bs-70-b-mont.pdf

[990] SMITH, Brad,"The secret gag orders must stop", *The Whashington Post*, 13/06/2021 https://www.washingtonpost.com/opinions/2021/06/13/microsoft-brad-smith-trump-justice-department-gag-orders/

Le Cloud Act permet ainsi de s'affranchir des règles classiques de la coopération judiciaire internationale, parfois jugées lourdes et chronophages. Il rend caduc l'accord entre l'Union européenne et les États-Unis d'Amérique en matière d'entraide judiciaire, conclu à Washington le 25 juin 2003 [991].

En substance, le Cloud Act rend possible, dans le cadre d'enquêtes de droit pénal, la réquisition de données de personnes non américaines à partir du moment où elles transitent par une firme états-unienne. Au regard de l'ampleur de la domination des acteurs américains dans le paysage contemporain numérique, et également concernant l'informatique en nuage, le Cloud Act a des répercussions conséquentes en matière d'atteinte à la vie privée. Et il a fait couler beaucoup d'encre. Son interaction avec le RGPD a été très discutée, surtout en ce qui concerne son article 48[992]. En réaction, certaines firmes américaines, notamment Microsoft, ont repris l'argument de la souveraineté numérique à leur compte. Microsoft a ainsi amorcé un mouvement de relocalisation de leur offre de Cloud sur le terrain européen, sans que ce type de service ne permette toutefois pas à leur client d'échapper au Cloud Act (puisque le fournisseur reste américain)[993]. Or, le Cloud Act contiendrait des garanties assurant le respect par les juges américains des privilèges et immunités des OI ? Rien n'est moins sûr. Le texte du Cloud Act ne fait pas référence à ce sujet. Et le Comité européen de la protection des données (CEPD) dans une note sur le Cloud remarque qu'il ne dispose pas de réponses claires sur ce point : « le US Cloud Act pourrait également contourner les protections accordées par le protocole sur les privilèges et immunités des institutions européennes, qui empêche les fournisseurs de services d'informatique en nuage de divulguer aux autorités répressives les données à caractère personnel qui leur sont confiées par les institutions européennes. »[994] Des archivistes s'en inquiètent également, la profession étant fortement concernée par les enjeux de stockage de données. Ainsi Elaine Goh et Eng Sengasang notent : « Le Cloud Act a été perçu comme un "empiètement massif de la part du gouvernement américain qui va à l'encontre des normes du droit international", ce qui est potentiellement un sujet de préoccupation pour les organisations internationales. » [995]

Or, les autres textes relatifs à la réquisition de preuves électroniques dans le cadre d'enquêtes pénales sont beaucoup plus explicites. Le règlement relatif aux *injonctions européennes* de

---

[991] CHRISTAKIS, *Théodore, «* Données, extraterritorialité et solutions internationales aux problèmes transatlantiques d'accès aux preuves numériques *» dans* USA v. Microsoft : Quel Impact ? Statut des données, souveraineté numérique et preuves dans les nuages, *CEIS & The Chertoff Group White Paper*,2017
MIGNON, Emmanuelle, "The Cloud Act : Unveilling European powerlessness", Revue européenne du droit,septembre 2020 https://geopolitique.eu/articles/the-cloud-act-unveiling-european-powerlessness/

[992]Art 48 du RGPD : « toute décision d'une juridiction ou d'une autorité administrative d'un pays tiers exigeant d'un responsable de traitement ou d'un sous-traitant qu'il transfère ou divulgue des données à caractère personnel ne peut être reconnue ou rendue exécutoire de quelque manière que ce soit à la condition qu'elle soit fondée sur un accord international tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers demandeur et l'Union ou un Etat membre, sans préjudice d'autres motifs de transfert en vertu du présent chapitre. »

[993] LAUSSON, Julien, "Microsoft prend l'engagement de laisser les données des clients européens en Europe", Numerama, 10/05/2021 https://www.numerama.com/tech/710425-microsoft-prend-lengagement-de-laisser-les-donnees-des-clients-europeens-en-europe.html

[994]"the US CLOUD Act might also circumvent the protections granted under the Protocol on Privileges and Immunities of the European institutions31, which prevents cloud service providers from disclosing personal data entrusted to them by European institutions to law enforcement authorities.", EDPB, "Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence", July 2019https://edpb.europa.eu/sites/default/files/files/file2/edpb_edps_joint_response_us_cloudact_annex.pdf

[995] "The CLOUD Act has been perceived as a "massive overreach on the part of the U.S. government that contravenes the norms of international law," which is potentially a matter of concern for international organizations."GOH, Elaine, SENGSAVANG, Eng (eds), *Recordkeeping in international organization, archives in transition in digital, networked environments*, London : Routledge, 2020, 262 p.

*production* et de *conservation* de *preuves électroniques* en *matière pénale (ou règlement sur les preuves électroniques)* mentionne de façon claire l'obligation du respect des privilèges et immunités[996]. Cependant, le règlement sur les preuves électroniques rappelle qu'il n'existe pas de définition commune à l'échelle européenne des immunités et privilèges. Pour clarifier ce point, il incite à se référer aux droits des États (émetteurs et destinataires des requêtes en données). Le texte mentionne toutefois non pas des organisations, mais des personnes couvertes par des privilèges et immunités (des diplomates) ou des personnes couvertes par le secret professionnel (des avocats) ou par le secret des sources (des journalistes).

Le même constat peut être fait au sujet de la convention de Budapest sur la Cybercriminalité[997]. La première version du texte autorise dans une certaine mesure la réquisition de preuves numériques dans le cadre d'enquêtes pénales, ce qui pourrait contrevenir aux immunités et privilèges d'OI. Et donc lors de l'ajout d'un protocole additionnel au texte, la Commission européenne à la protection des données « recommande d'inclure dans le mandat qu'en plus de prévoir des garanties appropriées pour la protection des données à caractère personnel, le protocole devrait assurer le respect d'autres garanties attachées aux données, telles que les privilèges et immunités. »[998] La seconde version du texte comprend donc une mention sur ce point dans sa section 5 sur les procédures relatives à la coopération internationale en l'absence d'accords internationaux applicables[999].

Alors comment le CICR prend-il en compte ce contexte ? Est-il possible malgré tout de conserver une certaine maitrise de ses données dans le cyberespace ? En réaction à ce qui apparait comme des cas d'ingérence américaine se sont multipliés des appels à regagner une forme de souveraineté numérique. Ce désir de souveraineté différentes formes selon qu'on a affaire à l'Europe, la France ou la Chine ou la Russie. Toujours est-il que les projets de cloud souverain se multiplient, mais n'ont pas — pour le moment — entamé la domination des acteurs américains. Quant au CICR, pour Massimo Marelli, il ne faut pas pour autant renoncer à l'instrument juridique des privilèges et immunités pour assurer la souveraineté de l'OI dans le cyberespace. Ce terme signifie pour lui une maitrise de l'ensemble du périmètre numérique d'une organisation. Cela implique de s'intéresser à la fois au cadre juridique, à la couche informationnelle et à l'infrastructure (et donc les câbles, les centres de données, etc.) Et pour

---

[996] Art 5 : « Si l'autorité d'émission constate que les données requises relatives à l'accès, aux transactions ou au contenu sont protégées par ces immunités et privilèges ou que leur divulgation porterait atteinte aux intérêts fondamentaux de l'autre État membre, elle n'émet pas l'injonction européenne de production. » règlement (ue) 2023/1543 du parlement européen et du conseil du 12 juillet 2023 https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32023R1543

[997] Il s'agit d'un des premiers traités internationaux portant sur la criminalité opérant sur les réseaux informatique, le texte est entré en vigueur en 2004. A ce titre il comprend des mesures d'interception de preuve numérique dans le cadre d'enquêtes relatives à ce type d'infraction (haine en ligne, pédopornographie, piratage et atteinte au droit d'auteur).

[998]« The EDPS recommends including in the mandate that in addition to providing for appropriate safeguards for personal data protection, the protocol should ensure the respect of other safeguards attached to the data such as privileges and immunities. »EDPS Opinion regarding the participation in the negotiations in view of a Second Additional Protocol to the Budapest Cybercrime Convention, 2019 https://www.edps.europa.eu/sites/default/files/publication/19-04-02_edps_opinion_budapest_convention_en.pdf

[999] Article 11 – Vidéoconférence, 1) Une Partie requérante peut demander, et la Partie requise peut autoriser, le recueil de la déposition d'un témoin ou d'un expert par vidéoconférence. La Partie requérante et la Partie requise se concertent pour faciliter le règlement de toutes les questions pouvant se poser concernant l'exécution de la demande, y compris le cas échéant le choix de la Partie qui préside la séance ; les autorités et personnes qui doivent être présentes ; si l'une des Parties ou les deux doivent demander au témoin ou à l'expert de prêter un serment particulier, lui dispenser des avertissements ou des instructions ; la manière d'interroger le témoin ou l'expert ; la manière permettant de garantir dûment les droits du témoin ou de l'expert ; le traitement des revendications de privilèges ou d'immunité ; le traitement des objections aux questions ou réponses ; et la question de savoir si l'une des Parties ou les deux assurent des services de traduction, d'interprétation et de transcription. » Deuxième Protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques https://rm.coe.int/1680ad0df7

Massimo Marelli, être souverain « signifie qu'un État ou une organisation internationale (OI) peut exercer un contrôle total sur les données qu'il traite (qui ne sont pas dans le domaine public), à l'exclusion de toute (autre) entité. En d'autres termes, aucun (autre) État ne peut, par application de la loi, rechercher et obtenir des données du "souverain des données". La notion de souveraineté est utilisée par analogie, car les organisations internationales ne jouissent évidemment pas de la souveraineté territoriale. Une organisation internationale peut plutôt chercher à tirer parti des privilèges et immunités dont elle jouit, y compris l'inviolabilité de sa correspondance et de ses archives et son immunité de juridiction, en combinaison avec d'autres mesures organisationnelles et techniques pour parvenir à un "contrôle exclusif" sur les données. »[1000]

Mais comment dans le contexte que l'on a évoqué assurer l'application des privilèges et immunités ? De manière générale, la reconnaissance de ces derniers découle d'accords de sièges bilatéraux, noués entre une organisation internationale et un État. Le numérique, en complexifiant le nombre d'acteurs impliqués, met à mal cette relation bilatérale. Rentrent en jeu des entreprises, des prestataires et sous-traitants[1001]. Malgré tout, pour tenter de maitriser l'externalisation de la gestion des données, Massimo Marelli recommande de contractualiser la reconnaissance des privilèges et immunités avec les prestataires : « Les sous-traitants et sous-traitants secondaires devraient être liés par une obligation contractuelle de notifier à toute autorité requérante qui cherche à accéder aux données que les données en question sont couvertes par les privilèges et immunités d'une organisation humanitaire ; de refuser toute demande d'accès par les autorités, qu'elle soit informelle, administrative ou judiciaire, et de réorienter la demande des autorités vers l'organisation humanitaire. » [1002] Il écrit également que « dans les cas où l'organisation humanitaire traite des données par l'intermédiaire de fournisseurs de technologie tiers, tels qu'un fournisseur de solutions en nuage, l'organisation devrait alors veiller à ce que toute clarification entre cette dernière et l'État hôte, comme souligné ci-dessus, soit également reflété dans les arrangements contractuels avec la société de technologie, afin de s'assurer que la société s'engage à les défendre et que le personnel de la société est prêt à les mettre en œuvre. »[1003]

---

[1000]« understand data sovereignty as indicating that a state or an International Organisation (IO) can exercise full control over the data it processes (which are not in the public domain), to the exclusion of any (other) entity. In other words, no (other) state may by application of law seek and obtain data of the 'data sovereign'.The notion of sovereignty is used analogously, since international organizations obviously do not enjoy territorial sovereignty. Rather, an international organization may seek to leverage the privileges and immunities it enjoys, including the inviolability of its correspondence and archives and its immunity from jurisdiction, in combination with other organizational and technical measures to achieve "exclusive control" over data. »
MARTIN, Aaron, SHARMA, Gargi, DE SOUZA, Siddharth Peter, TAYLOR, Linnet, VAN EERD, Boudewijn, MCDONALD, Sean Martin, MARELLI, Massimo, CHEESMAN, Margie, SCHEEL, Stephan, DIJSTELBLOEM, Huub, "Digitisation and Sovereignty in Humanitarian Space: Technologies, Territories and Tensions", Geopolitics, 28:3, 2023, p. 1362-1397

[1001] MARELLI, Massimo, *ibid.*

[1002]"Data Processors and Sub-Processors should be bound by contractual obligation to notify any requesting authorities who seek to access data, that the data in question is covered by a Humanitarian Organization's privileges and immunities; to decline any requests for access by authorities, whether informal, administrative or through judicial process, and to re-direct the authorities' request to the Humanitarian Organization." *Ibid.*

[1003] « due consideration may need to be given to the application of agreements for the sharing of data between the host country and third countries, as well as to the possibility that third countries may seek to access data held by technology companies through US CLOUD Act-type legislation and other relevant domestic laws having extraterritorial implications »; « in cases where the humanitarian organization processes data through third-party technology providers, such as a cloud solution provider, the organization would then need to ensure that any clarifications between itself and the host State, as highlighted above, are also reflected in the contractual arrangements with the technology company, to ensure that the company commits to defending them and the company's staff is prepared to give effect to them. »

Les recommandations du Comité européen de la protection des données concernant l'usage du cloud au sein des institutions européennes vont dans le même sens : « Il est essentiel d'ajouter aux modalités du contrat qu'il est interdit pour les fournisseurs de services en nuage de divulguer aux autorités répressives des États membres de l'UE ou des pays tiers les données à caractère personnel qui leur sont confiées par l'institution de l'UE, sauf autorisation expresse prévue par la législation de l'UE, ou par la législation d'un État membre dans la mesure où les conditions établies dans la législation de l'UE concernant la divulgation sont remplies. » [1004]

Massimo Marelli établit une liste indicative des points à prendre en compte pour la partie d'un contrat relative à la reconnaissance des privilèges et immunités : il est conseillé que les données soient stockées par des parties tierces uniquement sous des juridictions où les privilèges et immunités d'une organisation sont reconnus par les États, les privilèges et immunités doivent inclure l'ensemble des données traitées par une OI, (en transit, en stockage, en traitement) ; l'accord doit comprendre les données détenues par l'OI mais aussi par les fournisseurs de services, comme les serveurs et les réseaux utilisés par l'organisation ; et les données doivent être stockées dans des serveurs distincts d'autres clients ; et le fait qu'elles bénéficient de privilèges et immunités doit être rendu visible lors de leur conservation.

Ces recommandations concernent les accords entre une OI et un prestataire technique. Massimo Marelli ajoute qu'il est aussi nécessaire de les négocier avec les États hôtes. En effet, le CICR a déjà signé un accord de ce type avec la Suisse en 2020[1005]. Ce dernier comprenait les éléments suivants : l'assurance de la liberté d'utilisation de tout moyen de communication (et donc également des techniques de chiffrement comme le précise l'auteur) ; l'assurance d'une absence d'interférence des réseaux utilisés, ainsi que de la possibilité de disposer d'un réseau de connexion à tout moment et de ne pas être touché par des coupures de réseaux. Enfin, l'accord-cadre doit également prendre en considération les législations encadrant la réquisition de données. Et sans rentrer dans le détail des démarches à suivre : « il peut être nécessaire de prendre dûment en considération l'application d'accords de partage de données entre le pays hôte et des pays tiers, ainsi que la possibilité que des pays tiers cherchent à accéder à des données détenues par des entreprises technologiques par le biais d'une

Marelli, Massimo, "Hacking Humanitarians: Defining the Cyber Perimeter and Developing a Cyber Security Strategy for International Humanitarian Organizations in Digital Transformation", *International Review of the Red Cross* (2020), 102 (913), 367–387 p.
KUNER, Christopher, MARELLI, Massimo (co-ed.), Handbook on data protection in humanitarian action, second edition, Brussels Privacy Hub, ICRC, 2020
https://www.icrc.org/en/data-protection-humanitarian-action-handbook

[1004]EDPS, Lignes directrices sur l'utilisation des services d'informatique en nuage par les institutions et les organes de l'Union européenne, 16/03/2018 https://www.edps.europa.eu/sites/default/files/publication/18-03-16_cloud_computing_guidelines_fr.pdf

[1005] « As part of its international mandate, the ICRC processes highly sensitive data on the situation in regions of armed conflict and concerning the victims of such conflicts. In the interests of victims and their families, under the new provisions the ICRC's documents, archives and communications are better protected in an increasingly digital world. Given the changes over time in the composition and management of the ICRC's personnel, it has also become necessary to adapt the social security situation for its staff" Switzerland and ICRC sign protocol amending headquarters agreement, The Federal council, the Portal of the Swiss government, 27/11/2020 https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-81392.html

législation de type US Cloud Act et d'autres lois nationales pertinentes ayant des implications extraterritoriales. » [1006]

Néanmoins, Massimo Marelli reconnait que la protection offerte par les privilèges et immunités ne suffit pas, et qu'il ne faut pas oublier la dimension technique de la souveraineté numérique. Cela peut signifier adopter une démarche de type « privacy by design » qu'on a déjà décrit dans les sections précédentes. Or, comme le surligne Vincent Narbel Graff, un autre DPO du CICR, le Cloud n'a pas été construit avec en tête la protection des données, il n'est pas « privacy by design » [1007]. Et pour tout dire, il est évident qu'atteindre une pleine souveraineté n'est pas actuellement atteignable pour le CICR. Et Massimo Marelli reconnait qu' : « il faut se résigner à "simplement" minimiser les risques associés aux dépendances numériques, et tenter de les réduire autant que faire se peut. » [1008]

Ainsi, en entretien, un enquêté nous a certes avancé que *«l'objectif final est d'avoir la majorité des données en interne, on développe beaucoup nos capacités IT, donc avoir plus de serveurs, plus de personnes pour s'en occuper, ça représente un cout, que toutes les organisations ne peuvent pas s'offrir.* »[1009] Mais l'organisation peut-elle arriver à stocker l'intégralité de ses données en interne alors que le volume d'information produit ne cesse de croitre, du fait de sa numérisation accrue ? Et ce alors que l'offre — selon nos enquêtés du CICR — reste insuffisante : « *il n'existe pas à l'heure actuelle de compagnies pouvant fournir ce type de service, il n'existe pas de fournisseur de la qualité pour de grosses ONG de la taille de CICR. De petites ONG peuvent se baser sur de petites compagnies, elles n'ont pas les mêmes besoins. Mais vers qui on se tourne quand on a du cloud sans recourir aux Américains ?* »[1010]

D'où des solutions de compromis : « *On a l'objectif d'être souverain, mais on se confronte toujours à la potentialité technique. Est-ce que le CICR a les capacités de faire tourner un serveur de type Microsoft ? Non, ni même de la taille d'un serveur suisse, même si on n'utilise pas beaucoup de cloud suisse, on essaye de trouver un entre deux, on a le service et le soutien de Microsoft pour des données hébergées en suisse, voire par nous.* »[1011] Par exemple, le CICR a noué un partenariat avec ECLA, un prestataire suisse, pour héberger les données de son service de réunification familiale. Or ECLA est un partenaire soutenu par Microsoft Azure [1012].

---

[1006] "due consideration may need to be given to the application of agreements for the sharing of data between the host country and third countries, as well as to the possibility that third countries may seek to access data held by technology companies through US CLOUD Act-type legislation and other relevant domestic laws having extraterritorial implications"; "in cases where the humanitarian organization processes data through third-party technology providers, such as a cloud solution provider, the organization would then need to ensure that any clarifications between itself and the host State, as highlighted above, are also reflected in the contractual arrangements with the technology company, to ensure that the company commits to defending them and the company's staff is prepared to give effect to them." Marelli, Massimo, "Hacking Humanitarians: Defining the Cyber Perimeter and Developing a Cyber Security Strategy for International Humanitarian Organizations in Digital Transformation", *International Review of the Red* Cross (2020), 102 (913), 367–387 p.

[1007] C4DT Conference on Trustworthy and Sovereign Cloud Computing, September 13th, 2023https://c4dt.epfl.ch/c4dt-conference-on-trustworthy-and-sovereign-cloud-computing/

[1008] "fundamental objective of asserting control and exercising discretion in the choice and use of digital tools and infrastructures, pointing in other words to the importance of managing and mitigating "digital dependencies", and overdependencies in particular." MARELLI, Massimo, ibid.

[1009] Entretien n°44, OI2, DPO, 07/03/2021

[1010] Ibid.

[1011] Ibid.

[1012] "The ICRC reunifies families separated by conflicts and disasters, keeping data secure in the Microsoft cloud, Microsoft", 04/10/2022 https://customers.microsoft.com/en-us/story/1550914630508022658-icrc-nonprofit-microsoft-cloud

Mais sur le long terme, le CICR cherche à se tourner vers des solutions de cloud européennes, « *Au niveau des solutions, on se tourne vers des États du type Suisse ou Luxembourg, non engagés dans des conflits, ou pris dans les relations géopolitiques.* »[1013] Et l'organisation continue à « en plaider pour la nécessité de développer un cloud souverain destiné aux acteurs humanitaires, « un espace numérique qui offrirait des protections spécifiques aux données des personnes desservies par les organisations humanitaires et prendrait en compte les privilèges et immunités uniques accordés par la loi à ces organisations. »[1014]

Cela dit, pour le moment, il n'existerait que peu de solutions locales dans le pays accueillant le siège du CICR, la Suisse : « *Le CICR a envisagé un moment de se doter d'un cloud suisse. Mais les efforts de la nation helvétique en matière d'informatique en nuage souveraine ne sont pas pour le moment couronnés de succès*. » Et plus franchement, notre enquêté ajoute que « *La Suisse est à la ramasse. Ils ont raté le coche du cloud*. » [1015] Il faut toutefois reconnaitre que le sujet du cloud souverain a été mis à l'agenda politique helvétique. Et les acteurs militant sur ces enjeux utilisent l'argument de la nécessaire sécurité des ONG humanitaires et des OI ayant leur siège à Genève[1016]. L'objectif serait pour la ville de conserver son statut de capitale de la solidarité internationale et de la diplomatie humanitaire. Mais les différentes initiatives existantes n'ont pas pour le moment abouti[1017]. Or, si le CICR s'est rapproché d'institutions suisses pour discuter sur ce sujet (l'EPFL[1018], le CERN), l'organisation humanitaire reste aussi ouverte à des solutions venant d'autres pays, comme le Luxembourg. En effet, le CICR y a ouvert une « délégation au cyberespace ». À vrai dire, il s'agit « simplement » d'un centre de R&D destiné à trouver des solutions techniques, afin de, entre autres objectifs, réduire ses dépendances aux clouds américains. Mais ce dernier est de nature très spécifique : il est couvert par des « privilèges et immunités ».

Le choix du Luxembourg n'est pas anodin. Pour diversifier son économie, largement fondée sur la finance, et soutenir cette dernière, le pays a misé sur le numérique. Et le gouvernement luxembourgeois cherche à renforcer et à mettre en avant ce qui lui semble être les « points forts » du Grand-Duché. En effet, comme le surligne un rapport de la Commission européenne, le pays bénéficie d'une connectivité et d'un réseau d'infrastructure informatique et télécom, qui ont été développés par un réseau satellitaire et une connectivité des centres de données[1019]. Et le Luxembourg peut aussi compter sur un taux d'imposition avantageux pour attirer un bon nombre de sièges de BigTech, connus pour leur appétence pour l'évasion

---

[1013] Entretien n°44, OI2, DPO, 07/03/2022

[1014] « It continued to advocate the creation of a "sovereign cloud", a digital space that would provide specific protections for the data of people served by humanitarian organizations and take into account the unique privileges and immunities afforded by law to these organizations. » ICRC, Annual report, Volume I 2021, https://library.icrc.org/library/docs/DOC/icrc-annual-report-2021-1.pdf

[1015] Entretien n°44, OI2, DPO, 07/03/2022

[1016] Un jour, j'ai été interpellé par le CICR, qui insistait sur la nécessité d'un cloud souverain suisse. « Notre siège physique est à Genève, il faut que notre siège virtuel soit à Genève », m'avait-on dit. Les milieux humanitaires ont besoin d'un terrain numérique neutre et fiable. » SCHNARRENBERGER, Adrien, « Fatih Derder sur le "Swiss Cloud" : "Isabelle Moret peut nous faire gagner cinq ans" », *Blick*, 01/10/2021 https://www.blick.ch/fr/news/suisse/fathi-derder-sur-le-swiss-cloud-isabelle-moret-peut-nous-faire-gagner-cinq-ans-id16875867.html

[1017] SEYDTAGHIA, Anouch, « Autour du cloud en Suisse, deux visions diamétralement opposées se font face », *Le Temps*,13/07/2023 https://www.letemps.ch/economie/autour-du-cloud-en-suisse-deux-visions-diametralement-opposees-se-font-face

[1018] C4DT, Conference on trustworthy and sovereign cloud computing, EPFL, 13/09/2023 https://c4dt.epfl.ch/c4dt-conference-on-trustworthy-and-sovereign-cloud-computing/

[1019] European Commission, Digital decade Country Report, 2023, Luxembourg https://digital-strategy.ec.europa.eu/en/library/country-reports-digital-decade-report-2023

fiscale[1020]. Ainsi, Google projette depuis des années d'y ouvrir un data center[1021]. Ajoutons que le Grand-Duché cherche à développer son offre de cloud souverain, en partenariat avec la Belgique. Les deux pays ont annoncé le lancement du Cloud Clarence, un service d'informatique en nuage grand public présenté comme étant « le premier cloud vraiment souverain »[1022]. Cela dit, il repose sur une collaboration avec Google, mais les promoteurs du projet assurent qu'il reste indépendant. Selon leurs dires, ce dernier reposerait sur une modalité de fonctionnement « déconnectée » de l'entreprise américaine[1023]. Et surtout, dernier point important pour nos recherches, le Grand-Duché se positionne comme « pays d'accueil » pour des « d'ambassades numériques ». Pour ce faire, il dispose d'un réseau de centres de données sécurisé, destiné initialement à des banques. Selon différents communiqués à la date de 2017, le Luxembourg détiendrait environ 40 % des centres de données dits TIER IV à l'échelle européenne[1024]. Il faut cependant actualiser ce chiffre, le marché du cloud et des datacenter étant dynamique et évolutif, et le mettre en perspective avec les autres pays européens et les USA. En 2024, le Luxembourg n'a plus cette position dominante, la France ayant selon l'Uptime Institute mis à niveau ses offres d'hébergement en datacenters. Toujours est-il qu'en 2016, les organisations de l'OTAN et de la Commission européenne ont choisi d'y localiser leur espace de stockage[1025]. On ne dispose pas des précisions sur la nature des discussions sur le statut juridique des données et leurs protections

---

[1020] « Paypal et Amazon faisaient transiter leur bénéfices par le Grand-Duché pour échapper à l'impôt, « PAYPAL échappe à l'impôt en France », *Le Figaro*, 09/10/2013 https://www.lefigaro.fr/flash-eco/2013/10/09/97002-20131009FILWWW00279-paypal-echappe-a-l-impot-en-france.php
MARIN, Jérôme, « Au Luxembourg, Amazon n'aura pas à rembourser 350 millions d'euros d'aides fiscales », *L'Usine digitale*, 15/12/2023 https://www.usine-digitale.fr/editorial/au-luxembourg-amazon-n-aura-pas-a-rembourser-250-millions-d-euros-d-aides-fiscales.N2205090

[1021] Google veut investir 1 milliard pour un nouveau data center au Luxembourg, L'ECHO, 12/07/2017 https://www.lecho.be/entreprises/technologie/google-veut-investir-1-milliard-pour-un-nouveau-data-center-au-luxembourg/9913152.html LAUSSON, Julien, Google échappe à un redressement fiscal record en France, Numérama, 12/07/2017 https://www.numerama.com/business/275793-google-echappe-a-un-redressement-fiscal-record-en-france.html
COELHO, Ophélie, *Géopolitique du Numérique, l'impérialisme à pas de géants*, Paris : les éditions de l'Atelier, 2023, 256 p.

[1022] LABRO, Thierry, Clarence, « le premier cloud vraiment souverain », *Paperjam*, 25/10/2023 https://paperjam.lu/article/clarence-premier-cloud-vraimen

[1023] « Ce projet se fera en lien avec Google Cloud, qui a signé un accord avec Proximus pour la distribution de ses services de cloud souverain sur le territoire belge et luxembourgeois. « Dans le cadre de cet accord, les services de cloud souverain supporteront les activités déconnectées par le biais de Google Distributed Cloud Hosted, qui n'a pas besoin d'être connecté au Google Cloud pour la gestion de l'infrastructure, des services, des API ou des outils » MOUZON, Mélodie, « Un partenariat pour des services de Cloud déconnectés », Virgule, 15/03/2023 https://www.virgule.lu/luxembourg/un-partenariat-pour-des-services-de-cloud-deconnectes/1285751.html

[1024]La Classification Tier des data centers correspond à leur degré de sécurité, en fonction de différents critères, dont leur capacité à supporter des pannes, comme des coupures en alimentation électrique. Cette classification est établie par l'Uptime Institute, un consortium d'entreprises. Source: Uptime Institute, Wikipedia, 17/05/2023 https://fr.wikipedia.org/wiki/Uptime_Institute
« Les secrets des « data centers » luxembourgeois », *Le Quotidien*, 20/05/2015 https://lequotidien.lu/politique-societe/les-secrets-des-data-centers-luxembourgeois/
MESSCHENDORP, Laura, "Luxembourg bets on supercomputer"s, *Financial Times*, 16/02/2021 https://www.ft.com/content/227ad414-e35e-47c5-aae8-332106eace1c
HALL, Ben, « Luxembourg finance minister : "Diversification is crucial",*Financial Time*, 16/02/2021, https://www.ft.com/content/2b40ecee-b174-4173-b3a4-bb0205606b0b
https://cloudscene.com/market/data-centers-in-luxembourg/luxembourg
Le Luxembourg hébergerait 23 datacenter à la date de 2024, dont 8 seraient homologués Tiers IV, à comparer avec les USA (5387 data centers… mais l'organisation d'homologation en recense que 10 à peine…). https://cloudscene.com/market/data-centers-in-united-states/all l'Allemagne ( Pays européen disposant de plus de datacenter, 517 centre de données, mais seulement 1 est homologué Tiers IV), le Royaume Unis (513 datacenter, mais seulement 1 homologué Tiers 4), les Pays bas (297 datacenter, dont 2 tiers IV), la France ( 315 datacenter, dont 13 datacenter seraient homologués Tiers IV ) la Suisse (119 datacenter, dont 6 seraient homologués TIERS IV https://www.hebergeurs-suisse.ch/comparatifs/comparatif-datacenter-et-centre-de-calcul-en-suisse.php )
https://cloudscene.com/region/datacenters-in-europe
https://uptimeinstitute.com/uptime-institute-awards/list/achievements

[1025] « La Commission européenne a inauguré un nouveau data centre au Luxembourg », *Europaforum.lu*, 12/12/2016 https://europaforum.public.lu/fr/actualites/2016/12/comm-datacentre-lu/index.html
« Un accord pour installer un data center au profit de la NSPA », *Paperjam business zu Letzebuerg*, 09/05/2016 https://paperjam.lu/article/communique-un-accord-pour-installer-un-data-center-au-profit-de-la-nspa

grâce aux privilèges et immunités ; au contraire de l'ambassade numérique de l'Estonie, dont l'ouverture a donné lieu à moult débats juridiques. En somme, le Luxembourg se retrouve dans une posture paradoxale : terre d'accueil de nombreux sièges de GAFAM cherchant à échapper à une fiscalité trop forte, il entretient aussi une image favorable à des initiatives de type « ambassades numériques », intéressant des organisations et des États en quête de souveraineté informationnelle, comme c'est le cas de l'Estonie et Monaco ainsi que d'organisations comme le CICR.

Se pencher sur l'ambassade numérique estonienne est donc nécessaire pour mieux comprendre les enjeux liés à la délégation du cyberespace du CICR. Pour cet État balte, la création de l'ambassade numérique fait suite à la cyberattaque russe de 2007. L'Estonie avait alors pris une série de dispositions pour assurer la continuité de l'activité de son gouvernement en cas d'agression par son puissant voisin. Ouvrir une ambassade numérique a paru constituer une solution pour ce pays ayant adopté une stratégie numérique fondée sur la dématérialisation intensive de son administration[1026]. L'ambassade serait une forme de « back up ». Stocker des données dans une de ses ambassades déjà existantes n'était pas possible, par manque de capacité technique, et le pays ne disposerait pas sur place des centres de données suffisamment sécurisés d'après le chercheur Nick Robinson. L'idée est alors de conserver des données relatives à des services essentiels du gouvernement dans des serveurs situés en dehors de ses frontières, tout en dépendant de sa juridiction (comme une ambassade physique)[1027]. Mentionnons au passage le fait que le gouvernement ukrainien — en plein conflit contre la Russie — a aussi envisagé de relocaliser les données de son administration sur des serveurs à l'étranger, et a pu collaborer avec les GAFAM sur ce sujet (par exemple avec Microsoft et AWS)[1028].

En somme, d'ordinaire, un des arguments d'usage du cloud consiste en la volonté d'améliorer et de rendre plus efficient le fonctionnement des services administratifs, pour l'Estonie et l'Ukraine l'enjeu est de l'ordre sécuritaire : il s'agit d'assurer continuité de l'État. En outre, alors que pour des raisons de souveraineté d'autres nations se lancent dans un mouvement de localisation des données au sein de leurs frontières, l'Estonie cherche à assurer le maintien de son gouvernement en stockant ses données dans un autre territoire. Et cela relève comme la note le chercheur Lucas Kello un « splendide paradoxe » : les ambassades de données peuvent contribuer à la disparition progressive de l'Etat territorial, comme l'on alerté depuis

[1026] https://e-estonia.com/solutions/interoperability-services/x-road/

[1027] KOTKA, Taavi, KASK, Laura, RAUDSEPP, Karoliina, STORCH, Tyson, RADLOFF, Rebecca, LIIV, Innar, "Policy and Legal Environment Analysis for e-Government Services Migration to the Public Cloud", In *Proceedings of the 9th International Conference on Theory and Practice of Electronic Governance* (ICEGOV '15-16). Association for Computing Machinery, New York, NY, USA, 103–108. https://doi.org/10.1145/2910019.2910056

[1028] SATTER, PEARSON, J, « Exclusive : Ukraine prepares potential move of sensitive data to another country - official, » *Reuters*, 2022, https://www.reuters.com/world/europe/exclusive-ukraine-prepares-potential- movesensitive-data-another-country-2022-03-09/
STUPP, C. "Ukraine Has Begun Moving Sensitive Data Outside Its Borders," *Wall Street Journal*, 2022, https://www.wsj.com/articles/ukraine-has-begun-moving-sensitive-data-outside-its-borders-11655199002
AMAZON, "AWS employees help secure vital data so the Ukrainian government, education, and banking institutions can continue to serve Ukrainian people", 14/04/2023 https://www.aboutamazon.eu/news/aws/safeguarding-ukraines-data-to-preserve-its-present-and-build-its-future

longtemps les penseurs politiques, mais d'une manière qui renforce l'Etat plutôt qu'elle ne l'affaiblit. » [1029]

Mais le data center n'a tout de même pas le même statut qu'une ambassade, et comme on peut le lire sur le site du gouvernement estonien : « L'Estonie est le premier pays au monde à créer une ambassade de données. Cela peut sembler futuriste, mais il s'agit en fait d'un centre de données sécurisé, ou plutôt « une ambassade sans ambassadeur », située dans une installation sécurisée à l'extérieur de l'Estonie. Bien qu'il bénéficie du niveau de sécurité le plus élevé pour les centres de données, il ne s'agit pas d'une ambassade au sens diplomatique traditionnel du terme, mais de quelque chose de tout à fait nouveau au regard du droit international. »[1030]

D'un point de vue juridique, le traité signé avec le Luxembourg mentionne la Convention de Vienne comme texte de référence, il en reprend certains éléments : l'inviolabilité des locaux, le data center ne pouvant être perquisitionné, des personnes non habilitées ne peuvent y pénétrer ; il bénéficie selon l'accord du même statut que les archives estoniennes, et bénéficie également du statut d'inviolabilité[1031]. Mais l'accord ne comprend pas, à dessein, le terme d'« ambassade », et il indique que la convention risque de ne pas suffire en tant que cadre légal pour les datas. Il y a donc une double incertitude juridique : est-il possible d'appliquer la Convention de Vienne à un institut qui n'est pas une ambassade ? Est-il possible de l'appliquer à l'espace numérique ? Ce type d'accord étant encore tout à fait inédit, sa reconnaissance doit être mise à l'épreuve de la pratique[1032]. Le chercheur Nick Robinson, qui a écrit sa thèse sur le sujet, pense que bien qu'une complète réécriture de la Convention de Vienne soit peu probable, la multiplication d'ambassade numérique pourrait rendre nécessaire l'ajout d'une extension au texte existant. Il propose ainsi de le baptiser « Convention de Tallinn ».

D'un point de vue technique, de nombreuses discussions ont été menées pour déterminer la nature de l'architecture informatique de l'ambassade. Ces dernières portaient sur le choix du type de cloud (public ou privé), sur le type de données pouvant y être stockées selon leur degré de sensibilité[1033]. Et au-delà du cas de l'ambassade, l'Estonie défend un modèle théorique hybride d'architecture informationnelle, composé de 3 couches : des solutions de

---

[1029] ROBINSON, Nicholas, David, "Distributed denial of government, the data embassy and the legal and legal implications of extraterritorial data storage", Doctoral thesis, philosophy, University of London, 2020 https://pure.royalholloway.ac.uk/ws/portalfiles/portal/44682853/2020_Robinson_N_PhD.pdf

[1030] "Estonia is the first country in the world to establish a data embassy. It may sound futuristic, but it actually just means a secure data centre. In essence it's an embassy without an ambassador and it's located at a secure facility outside Estonia. While it has the highest security level for data centres, it's not an embassy in the traditional diplomatic sense – it is something completely new under international law." https://e-estonia.com/solutions/e-governance/data-embassy/

[1031] Agreement between the Republic of Estonia and the Grand Duchy of Luxembourg on the hosting of data and information systems, 20/06/2017 https://www.riigiteataja.ee/aktilisa/2280/3201/8002/Lux_Info_Agreement.pdf

[1032] « The legal issues are less clear than the security issue," says Ian Walden, Professor of Information and Communications Law at Queen Mary University of London. The Vienna Convention was written over half a century ago and could clearly be interpreted in a way that "really underpins the virtual data embassies and the concept of being able to place data remotely but securely," explains Professor Walden. However, "the point with the Vienna Convention is there are a set of rules, but their enforceability is somewhat doubtful."
Diplomatic immunity for data : Estonia creates a virtual embassy, Microsoft, 14/12/2017https://blogs.microsoft.com/eupolicy/2017/12/14/diplomatic-immunity-data-estonia-creates-virtual-embassy/

[1033] L'ambassade stocke les données suivantes : fichier du système judiciaire, système d'information du trésor, registre foncier électronique, registre des taxes, registre des entreprises, registre de la population, journal officiel, registre des documents d'identité, registre cadastral, registre national de l'assurance et des pensions. Data Embassy- the digital continuity of a State, E-Estonia, 09/12/2019 https://e-estonia.com/data-embassy-the-digital-continuity-of-a-state/

cloud basées sur le territoire estonien, qui doit nécessiter la construction de data centers, dont le pays ne dispose pour le moment pas[1034] ; d'une couche reposant sur du cloud public, géré par des entreprises privées, potentiellement des GAFAM ; et enfin une ambassade numérique à proprement parler située hors du territoire estonien[1035]. On remarquera que les GAFAM occupent une place non négligeable dans la stratégie de numérisation de l'Estonie. Le Cloud gouvernemental en lui-même dépend d'Amazon et de Microsoft[1036]. Concernant son projet d'ambassade, l'Etat balte a commencé à mener des recherches de concert de concert avec Microsoft[1037]. Mais, fait notable, le pays a cependant choisi de ne pas dépendre de la firme américaine pour son d'ambassade virtuelle, comme on peut le lire sur le site du gouvernement estonien : « L'une des deux options pour parvenir à la continuité numérique — la technologie du nuage — a été testée fin 2014, lorsque l'Estonie s'est lancée dans un projet de recherche avec Microsoft pour voir si un modèle de partenariat public/privé en matière d'informatique en nuage pouvait fonctionner. (…) La technologie du nuage offre une bonne opportunité, mais l'État souhaite également conserver le contrôle total et la juridiction de ses données et de ses systèmes. C'est pourquoi les services de cloud privé ne nous conviennent pas vraiment. »[1038] L'État estonien loue alors un espace de serveur du data center, géré par une entreprise luxembourgeois, Luxconnect [1039] . Le projet n'assure pas une totale indépendance infrastructurelle ( le propriétaire du data center reste Luxconnect), mais le projet ne recoure, a priori pas, à des GAFAM, et le statut juridique accordé par l'accord entre l'Estonie et le Luxembourg procure une immunité aux données du pays balte.

Pour conclure, le gouvernement estonien met en avant la continuité de l'État grâce au numérique, mais en restant en partie dépendant des GAFAM, notamment pour son cloud gouvernemental, dépendance peut être renforcée en raison de la proximité de l'Estonie sur le plan stratégique avec les États-Unis[1040]. Mais malgré tout, le gouvernement estonien tente

---

[1034] Le chercheur Lucas Kello precise que le gouvernement Estonie ne dispose pas encore d'infrastructures suffisantes pour stocker ses données sur ses propres serveurs : « Malgré son appellation, qui suggère un rôle principal, voire exclusif, du gouvernement, le nuage gouvernemental est un partenariat entre les secteurs public et privé. Le gouvernement estonien n'a pas la capacité de construire lui-même des serveurs en nuage ; il compte sur le matériel et l'assistance technique du secteur privé pour les mettre en place et les faire fonctionner » ; « Despite its label, which suggests a primary or even exclusive government role, the Government Cloud is a partnership among the public and private sectors. The Estonian government does not have the capacity to build cloud servers itself; it relies on the private sector's hardware and technical assistance in establishing and running them. » KELLO, Lucas, *Striking back, the end of peace in cyberspace- and how to restore it,* Yale University press, 2022, 183 p.

[1035] KOTKA, T., LIIV, I., « Concept of Estonian Government Cloud and Data Embassies ». In: KŐ, A., FRANCESCONI, E. (eds) *Electronic Government and the Information Systems Perspective*, Lecture Notes in Computer Science, vol 9265, Springer, 2015

[1036] The Government of Estonia signs a Memorandum of Understanding with Microsoft, Microsoft, 28/04/2021, https://news.microsoft.com/en-cee/2021/04/28/the-government-of-estonia-signs-a-memorandum-of-understanding-with-microsoft/

[1037] "Small countries around the world are turning to the concept of "data embassies" because they are in need of sovereign and resilient infrastructure. Nevertheless, they realize that keeping data localized within a single facility or a set geographical boundary could pose a security risk in the event of a crisis, such as a natural disaster or an armed conflict. Data embassies offer one solution to this problem, and sovereign cloud solutions, such as those offered by Google Cloud, offer another." MEYER, Thiébaut, "How data embassies can strengthen resiliency with sovereignty", 12/11/2022 https://cloud.google.com/blog/products/identity-security/data-embassies-strengthening-resiliency-with-sovereignty?hl=en

[1038] "Estonia to Open the world's first data embassy in Luxembourg", 14/06/2017 https://e-estonia.com/estonia-to-open-the-worlds-first-data-embassy-in-luxembourg/

[1039] Il s'agit d'une société anonyme datant de 2006, disposant initialement de financements publics, « l'entreprise n'a pas reçu d'argent frais de l'État depuis 2010. Depuis 2006, date de sa création, elle a essentiellement financé par des prêts ses investissements à hauteur de 334 millions d'euros dans les autoroutes de l'information et ses centres de données ultra-performants. » POUJOL, « Véronique, L'État renfloue les caisses de Luxconnect », *Reporter*, 29/11/2019 https://www.reporter.lu/luxembourg-secteur-ict-etat-renfloue-les-caisses-de-luxconnect/

[1040] Pour comprendre le positionnement de l'Estonie vis à vis des GAFAM, et il s'agit aussi de voir comment le gouvernent américain perçois l'Estonie, comme le remarquent Melissa Aronczyk et Stanislav Budnitsky : « Pour leur part, les États-Unis considèrent l'Estonie comme un

de maintenir un plus grand contrôle pour ses données les plus sensibles, ces dernières devant être conservées dans son ambassade numérique, qui se distancie d'un modèle du « tout GAFAM».

Ce détour par l'Estonie nous a paru nécessaire pour mieux comprendre la spécificité du projet du CICR. La délégation pour le cyberespace est pour le moment un centre de recherche sécurisé, dont les données bénéficient de la protection accordée par les privilèges et immunités de l'organisation. Un de nos enquêtés décrit le projet comme suit : « *Il s'agit de construire un espace digital neutre, le CICR est un des premiers à faire ça, un espace où les données sont stockées et protégées par les immunités et privilèges du CICR une délégation qui n'existerait que dans le cyberespace. C'est comme une délégation physique du CICR, les autorités ne peuvent pas les saisir, ne peuvent pas rentrer dedans. C'est comme une ambassade, ils sont intouchables.* »[1041] Le centre de R&D est dédié à des projets en lien avec la stratégie numérique du CICR, dont le fait de préserver ses privilèges et immunités dans le cyberespace.

Le CICR a mené courant 2022 des négociations actives avec le gouvernement luxembourgeois pour garantir leur reconnaissance dans l'espace numérique. L'accord a été signé et entériné en septembre 2023. Il a pour objectif « d'assurer le bon fonctionnement du CICR au Grand-Duché de Luxembourg, en reconnaissant la personnalité juridique internationale du CICR et en octroyant au CICR et à son personnel les privilèges et immunités nécessaires. »[1042] Les articles 5 et 6 assurent l'inviolabilité des données gérées par le CICR au sein de sa délégation au cyberespace[1043]. Ajoutons que l'article 10 reconnait l'inviolabilité des données du CICR en cas de requête d'information par un État tiers dans le cas d'enquêtes pénales[1044]. Notons au passage que cet article n'était pas présent de façon explicite dans l'accord estonien. La délégation au Cyberespace se matérialise physiquement au Luxembourg par un bureau, et par la location de surfaces de stockages dans un centre de données sécurisé de type Tier IV (qui

---

allié nécessaire dans les débats sur la gouvernance de l'internet. Le département d'État américain qualifie l'Estonie de "berceau du commerce électronique et de l'innovation en matière de gouvernance électronique" et affirme que "l'Estonie montre au monde comment l'ouverture de l'internet et la gouvernance démocratique peuvent conduire à la stabilité, à l'innovation et à la croissance économique". » For its part, the United States sees Estonia as a necessary ally in internet governance debates. The U.S. State Department calls Estonia 'a cradle for e-business and e-governance innovation,' and argues, 'Estonia demonstrates to the world how internet openness and democratic governance can lead to stability, innovation, and economic growth'. ARONCZYK, M,BUDNITSKY, S. "Nation Branding and Internet Governance: Framing Debates over Freedom and Sovereignty". In: KOHL U, ed. *The Net and the Nation State: Multidisciplinary Perspectives on Internet Governance*. Cambridge University Press; 2017:48-66.

[1041] Entretien n°91, OI2, 26/05/2023

[1042] Projet de loi portant approbation de l'« Agreement on the status and privileges and immunities of the International Committee of the Red Cross between the Grand Duchy of Luxembourg and the International Committee of the Red Cross », 01/06/2022 https://wdocs-pub.chd.lu/docs/compilation/docpa/pdf/8093_Dossier_Complet.pdf

[1043] « Article 5 quarter : Immunity of the equipment and licences. The Equipment and Licenses required to operate the Data Centre used by the ICRC and put in place on the premises of the Data Centre shall be regarded as assets of the ICRC and shall enjoy immunity from every form of legal process. Article 6 : Inviolability of archives : 1. The ICRC's archives, including all documents and data (including electronic documents), as well as all Data and Information Systems, and all Equipment and Licenses, which belong to, are used or held by the ICRC, shall be inviolable wherever located. This includes data held in or otherwise processed through servers, server rooms, and any other device containing data hosted by the ICRC. 2. The archives shall be exempt from search, requisition, attachment or execution. Luxembourg shall refrain from interfering with the ICRC's archives by executive, administrative, judicial or legislative or any other action, including by cyber means.

[1044] "Should Luxembourg negotiate and enter into agreements with other States for the exchange or provision of data in the framework of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, Luxembourg will commit to clearly indicating that ICRC data covered by this Agreement as being outside the scope of such agreements." Projet de loi portant approbation de l'« Agreement on the status and privileges and immunities of the International Committee of the Red Cross between the Grand Duchy of Luxembourg and the International Committee of the Red Cross », 01/06/2022 https://wdocs-pub.chd.lu/docs/compilation/docpa/pdf/8093_Dossier_Complet.pdf

est présenté comme étant le niveau de sécurité maximal pour ce type d'infrastructure). Ni le propriétaire du centre de données ni le détail de l'architecture du système d'information n'est précisé dans l'accord. Il semblerait d'après la journaliste Adrienne Fichter que l'environnement d'expérimentation soit géré par Luxconnect [1045], une des principales compagnies supervisant des centres de données au Luxembourg. L'entreprise accueille également l'ambassade numérique estonienne. Cet espace n'est pour le moment qu'un centre de R&D. Mais le président général de Luxconnect déclare lors d'une visite de l'ancien président du CICR, Peter Mauer, que son entreprise « a une expérience de plus de 15 ans en tant que fournisseur de centres de données à plusieurs niveaux, s'appuyant à 100 % sur l'énergie verte, étant entièrement redondant et certifié pour le temps de fonctionnement. Si des organisations similaires au CICR recherchent un lieu pour héberger leurs données, nous serions certainement en mesure de répondre à leurs besoins. » [1046] Et le journaliste et politicien suisse Fatih Derder — qui a fait de la souveraineté numérique son cheval de bataille — agite le spectre d'une délocalisation des données d'organisations humanitaires — dont le CICR — dans d'autres nations, ce qui serait « désastreux » selon lui en termes d'image pour la Suisse[1047]. Le projet n'est pas ouvertement d'actualité. Mais toujours est-il que Massimo Marelli envisage dans un article ce type de structure comme étant une solution afin d'assurer la souveraineté de l'organisation et garantir l'application des privilèges et immunités dans le cyberespace : « En plus d'une cyberstratégie développée sur ces bases, les organisations humanitaires internationales doivent envisager des solutions techniques uniques et propres à leurs spécificités, telles que la création d'un « espace humanitaire numérique » sur le modèle d'un « cloud souverain » ou d'une « ambassade numérique. »[1048]

---

[1045] L'équipe luxembourgeoise du CICR est encore petite, avec onze collaborateurs. Lesquels doivent développer des solutions qui, dans le meilleur des cas, seront ensuite transférées dans le « fonctionnement normal » de l'institution et pourront être utilisées par des délégations « classiques ». Entretemps, l'environnement de test chez Luxconnect a été mis en place. » FICHTER, Adrienne, « Le CICR réinvente son avenir cyber, mais pas en Suisse », *Heidi.news*, 01/08/2023 https://www.heidi.news/cyber/le-cicr-reinvente-son-avenir-cyber-mais-pas-en-suisse Il s'agit d'une société anonyme datant de 2006, disposant initialement de financements publics, « l'entreprise n'a pas reçu d'argent frais de l'État depuis 2010. Depuis 2006, date de sa création, elle a essentiellement financé par des prêts ses investissements à hauteur de 334 millions d'euros dans les autoroutes de l'information et ses centres de données ultra-performants. » POUJOL, Véronique, « L'État renfloue les caisses de Luxconnect », *Reporter*, 29/11/2019 https://www.reporter.lu/luxembourg-secteur-ict-etat-renfloue-les-caisses-de-luxconnect/

[1046] "*has an experience for over 15 years as multi-tier Data center provider relying 100% on green energy, being fully redundant and uptime certified. If organisations similar to the ICRC are looking for a place to host their data, we would certainly be able and prepared to fulfil the requirements* Visit of M. Peter Maurer, Chairman of the International Committee of the Red Cross, LuxConnect, 09/06/2022https://www.luxconnect.lu/visit-of-m-peter-maurer-chairman-of-the/

[1047] « Il n'y a aucune garantie suivant où elles sont stockées. Résultat, il est probable que le CICR aille chercher des solutions ailleurs… C'est une occasion manquée pour la Suisse. » SCHNARRENBERGER, Adrien, « Fatih Derder sur le "Swiss Cloud" : "Isabelle Moret peut nous faire gagner cinq ans" », *Blick*, 01/10/2021
https://www.blick.ch/fr/news/suisse/fathi-derder-sur-le-swiss-cloud-isabelle-moret-peut-nous-faire-gagner-cinq-ans-id16875867.html
« Fathi Derder dit tout haut ce que beaucoup pensent : « Ce serait catastrophique pour la Suisse, en termes d'image, que le CICR, l'institution suisse par excellence, choisisse d'héberger ses données à l'étranger. »
SEYDTAGHIA, Anouch, « Et si la Suisse aidait le CICR et les ONG contre les cyberattaques ? », Le Temps, 23/01/2022 https://www.letemps.ch/economie/cyber/suisse-aidait-cicr-ong-contre-cyberattaques
Des journalistes évoquent aussi la nécessité de développer l'écosystème suisse pour retenir les ONG dans la capitale helvétique : « Ces progrès sont urgents et nécessaires. Car les bases de données contenant toutes les données personnelles du CICR se trouvent toujours en Suisse. Pour l'instant. » FICHTER, Adrienne, « Le CICR réinvente son avenir cyber, mais pas en Suisse », *Heidi.news*, 01/08/2023 https://www.heidi.news/cyber/le-cicr-reinvente-son-avenir-cyber-mais-pas-en-suisse

[1048] "In addition to a cyber strategy developed on these bases, international humanitarian organizations need to consider unique and specific technical solutions to their specificities, such as the creation of a "digital humanitarian space" along the model of a "sovereign cloud" or a "digital embassy"' MARELLI, Massimo, "Hacking Humanitarians: Defining the Cyber Perimeter and Developing a Cyber Security Strategy for International Humanitarian Organizations in Digital Transformation",*International Review of the Red Cross*, 2020, 102 (913), 367–387 p.

Dans ce chapitre, on s'est intéressée à la façon dont les ONG protègent la vie privée des bénéficiaires face à des requêtes de données de la part de gouvernements locaux, des requêtes qui peuvent être tout à fait jugées légitimes par les ONG. Mais on a vu que ces dernières ont lieu dans des contextes de recomposition des souverainetés étatiques. Dans le cadre de crises, des États dits « faillis » cherchent malgré tout à conserver une forme d'autorité sur leur territoire, ce qui passe par un contrôle accru des données d'ONG. En réaction, les humanitaires tentent dans une certaine mesure de se soustraire aux requêtes des États, surtout s'il s'agit pour eux de tenter d'obtenir des listes de bénéficiaires. Mais les ONG se trouvent dans des situations inégales. Par exemple, les organisations internationales disposent de privilèges et immunités, leur permettant en théorie de conserver une certaine indépendance par rapport aux exigences étatiques. Mais tout dépend aussi du mandat de l'organisation internationale. Par exemple, l'UNHCR travaille de concert avec les États à l'enregistrement des exilés. L'organisation se substitue dans certains cas aux gouvernements, mais peut aussi opérer aussi conjointement, surtout lorsque les États souhaitent garder la maitrise de leur territoire et des populations y transitant. Cela signifie le fait de pouvoir mener des opérations conjointes d'enregistrement d'exilés. Et cela implique de pouvoir accéder aux données de l'UNHCR, en ayant parfois pour finalité le fait de mener leur propre agenda sécuritaire, et leurs propres opérations de contrôle des frontières et des flux migratoires. Le CICR conserve, a priori, une plus grande autonomie vis-à-vis des États, et considère la confidentialité comme une valeur cardinale. Mais l'organisation est mise au défi par la transformation numérique des sociétés, qui rend plus difficile l'application des privilèges et immunités dans le cyberspace. Ce dernier cas nous a permis d'explorer la façon de protéger les données dans un contexte de triple recomposition de la définition classique de la souveraineté. En effet, nous pensons tout d'abord au caractère extraterritorial du droit (le Cloud Act). Et cette recomposition découle aussi de la fluidité du numérique et de sa faculté à se jouer des frontières traditionnelles des États, notamment pour l'informatique en nuage. Et enfin, n'oublions pas que les privilèges et immunités permettent à une OI de ne pas appliquer les lois locales d'un État.

## Chapitre 04 — Les ONG et le contrôle du financement du terrorisme : impartialité de l'aide et protection des données

Les études de sécurité et les « borders studies » ont longuement décrit les différentes formes de contrôle des flux migratoires et les processus aboutissant à la construction de la figure de l'exilé comme menace et comme terroriste[1049]. Cette criminalisation des migrants est portée par un assemblage d'acteurs et d'institutions (agences publiques, gouvernements, organisations internationales, acteurs) ; et se traduit par des pratiques et des discours hétérogènes, inscrits à l'échelle transnationale[1050]. Et les ONG venant en aide aux exilés se sont retrouvées — malgré elles — embarquées dans cette gouvernance sécuritaire, entre autres du fait de leur dépendance à l'égard de bailleurs étatiques. La balance entre « care » et « contrôle » a largement été analysée, et elle se manifeste par diverses pratiques, notamment par l'adoption par les ONG d'assemblages technologiques de surveillance et de dispositifs invasifs comme la biométrie[1051]. L'impact sur les ONG de la solidarité internationale des mesures de sanction contre le financement du terrorisme est cependant moins connu. Et pourtant, les humanitaires sont concernés également par ce sujet. Les bailleurs de fonds imposent des opérations de criblage aux personnels d'ONG, voire dans certains cas aux bénéficiaires, afin de vérifier qu'ils ne se trouvent pas sur des listes de terroristes constituées par les États et des organismes onusiens. Les banques conditionnent la gestion de fonds à l'identification de leurs clients, afin de s'assurer qu'ils ne sont pas associés à des organisations criminelles. Et ces institutions traitent dans le cadre de leur obligation de « vigilance raisonnable » une quantité toujours accrue d'informations, ainsi que le décrivent des chercheurs comme Anthony Amicelle, ou Gilles Favarel Garigues, spécialistes des sentinelles de l'argent sale[1052]. Ainsi, des sanctions visant initialement des acteurs illégitimes, comme des narcotrafiquants, des terroristes, des délinquants en col blanc, etc., touchent donc des acteurs nettement plus valorisés sur le plan normatif. Par conséquent, s'intéresser au monde du renseignement financier c'est aussi voir comment se construit le soupçon, voir comment est construite l'illégitimité de certains acteurs, apriori biens sous tous rapports, comme les ONG humanitaires[1053]. Certes, le secteur n'échappe pas aux affaires de fraudes et de détournement

---

[1049] Sachant qu'il est généralement en sciences sociales admis qu'il n'y a pas de définition arrêtée de ce terme, notamment de son caractère hautement politique. Il s'agit plutôt d'un label, appliqué à une forme spécifique d'action violente. D'ailleurs le politiste Xavier Crettier préfère parler de terrorisation que de terrorisme. Terme qu'il définit comme tel : ***«*** *les pratiques de terrorisation c'est l'usage d'une violence intentionnellement indiscriminée à des fins politiques opérant une disjonction entre la cible (l'Etat) et la victime (la population civile), relayée et amplifiée par le soutien le plus souvent recherché des médias ».*

[1050]BIGO, Didier, « Le "*nexus*" sécurité, frontière, immigration : programme et diagramme », *Cultures & Conflits*, 84 , 2011, p.7-12

BIGO, Didier, "La Mondialisation de l'(in)Sécurité? Réflexions Sur Le Champ Des Professionnels de La Gestion Des Inquiétudes et Analytique de La Transnationalisation Des Processus d'(in)Sécurisation", *Cultures et Conflits*, no. 58, 2005, p. 53–100

[1051]JACOBSEN, Katja, "Biometric data flows and unintended consequences of counterterrorism", *International Review of the Red Cross*, 2021, 103, p.619-652

[1052] FAVAREL-GARRIGUES, Gilles, GODEFROY, Thierry, LASCOUMES, Pierre, *Les sentinelles de l'argent sale. Les banques aux prises avec l'antiblanchiment,* Paris : La Découverte, « Cahiers libres », 2009, 312 p.

[1053] FAVAREL-GARRIGUES Gilles, GODEFROY Thierry, LASCOUMES Pierre, « 7. La formation, les réseaux et les autres facteurs d'homogénéisation », dans : FAVAREL-GARRIGUES, Gilles, GODEFROY, Thierry, LASCOUMES, Pierre (dir.), *Les sentinelles de l'argent sale. Les banques aux prises avec l'antiblanchiment*, Paris, La Découverte, « Cahiers libres », 2009, p. 158-170. https://www.cairn.info/les-sentinelles-de-l-argent-sale--9782707154217-page-158.htm

AMICELLE Anthony, « *Policing* & *big data*. La mise en algorithmes d'une politique internationale », *Critique internationale*, 2021/3 (N° 92), p. 23-48. https://www-cairn-info.ezproxy.utc.fr/revue-critique-internationale-2021-3-page-23.htm

de l'aide comme a pu le décrire finement Marc Antoine Pérouse de Montclos en 2001[1054]. Toutefois, le fait de soupçonner les humanitaires de financer potentiellement des groupes terroristes traduit aussi plus largement une criminalisation de l'aide. Et les ONG dénoncent les conséquences des sanctions en matière de violation du droit international humanitaire. N'oublions pas cependant que ces dernières posent aussi des enjeux de protection des données. On verra en effet pourquoi La CNIL, le Comité européen à la protection des données et Privacy international ont alerté sur les atteintes relatives à la vie privée entrainées par des mesures de contrôle des flux financiers.

Comprendre les risques associés à la surveillance des flux financiers des ONG implique de se plonger dans l'univers des sanctions onusiennes, de fréquenter des organismes intergouvernementaux, comme le GAFI, et des acteurs comme les agents de conformité bancaire. Et brosser ce contexte général est nécessaire avant d'aborder des mesures qui concernent plus directement les humanitaires. Ces dernières consistent en des opérations de criblage menées par les bailleurs de fonds souhaitant maintenir un contrôle des financements accordés. Elles comportent aussi en des dispositifs de vigilance raisonnable menés par les banques auprès des ONG dans le cadre de programmes de transferts monétaires.

## Section 1 — Lutte contre le financement du terrorisme : sanctions et impartialité de l'aide

Cette première section adopte donc un point de vue surplombant. Sa vocation est de décrire les enjeux globaux de la lutte contre le financement du terrorisme et ses répercussions générales sur les acteurs humanitaires. Nous allons pour ce faire présenter les différents acteurs impliqués dans la lutte contre le financement du terrorisme. Commençons avec le Groupe d'action financière (GAFI). Cette organisation mondiale, lors de sa création en 1989, était d'abord destinée à la lutte contre le financement du trafic de drogue. Après le 11 septembre 2001 — en octobre 2001, plus précisément —, cette agence a été mandaté pour la lutte contre le financement du terrorisme. Les outils juridiques utilisés pour la lutte contre la délinquance financière ont été transposés à la lutte contre le terrorisme. Anthony Amicelle ou encore Gilles Favarel-Garrigues ont pu décrire cette transition au sein d'un organisme qui se dédie au contrôle de l'adoption du cadre en vigueur et des réglementations adéquates dans la surveillance du blanchiment des capitaux et de la lutte contre le financement du terrorisme (LBC/FT). Le mandat de cette organisation concerne également la conception de standards et l'évaluation des législations nationales. Elle contribue à la diffusion de normes et de recommandations de pratiques professionnelles. Le GAFI a ainsi publié une série de recommandations relatives à de « bonnes pratiques » en la matière, et publie sa propre liste des pays et territoires non coopératifs (du « name and shame »). L'organisation a ainsi contribué à l'élaboration du corpus de droit souple relatif aux opérations de lutte contre le financement du terrorisme.

[1054] PEROUSE DE MONTCLOS, Marc-Antoine, *L'aide humanitaire, l'aide à la guerre ?,* Paris : Editions complexes, 2001,208 p.

Le GAFI a édicté 8 recommandations enjoignant aux États le fait de prendre des mesures de lutte contre le terrorisme[1055]. Ce faisant, l'organisation contribue à établir ce qui relève ou non d'un soutien à un groupe terroriste. Une de ses premières définitions est relativement large. Le GAFI commence en effet par proscrire le financement d'un groupe terroriste, même si ces fonds ne sont pas directement destinés à une action terroriste[1056]. Précisons d'ailleurs au passage que de manière générale, trois éléments sont importants à garder à l'esprit pour estimer ce qui relève d'un soutien à un groupe terroriste : l'intentionnalité ; le fait d'avoir conscience de financer une organisation terroriste ; le fait que le financement soit utilisé directement par une entité pour financer un acte terroriste ; le fait que le financement soit destiné directement ou non à des groupes terroristes.

Un autre organe joue un rôle central dans la lutte contre le financement du terrorisme : le conseil de sécurité de l'ONU. Ce dernier a édicté une série de résolutions qui constituent le cœur de l'architecture normative de la lutte contre le terrorisme. Ainsi, sa première Résolution 1267, adoptée en 1999, prescrit un gel des avoirs et un embargo aérien contre les talibans. À la suite du 11 septembre est adopté sous le gouvernement Bush l'Executive order 13224, qui est formalisé ensuite sous la forme du bien connu Patriot ACT. Et la résolution 1373, adoptée le 28 septembre 2001 par le Conseil de sécurité, calque l'Executive Order du Président Bush [1057]. La résolution 1373 ne cible pas un groupe en particulier et laisse à la discrétion des États la création de listes nationales, d'où un manque de cohésion entre les différents régimes nationaux [1058].

Ce régime de sanction a été critiqué à maintes reprises par des ONG de défense des droits de l'homme. Son manque de transparence a été dénoncé par Amnesty International ou des chercheurs comme Ben Hayes et Gavin Sullivan[1059]. L'élaboration des listes repose en effet sur des négociations à huis clos. Ben Hayes et Gavin Sullivan pointent également le manque de recours laissé aux individus y figurant, et leur caractère extensif. D'après les chercheurs, une

---

[1055] Les 8 mesures originelles édictées par le GAFI sont les suivantes :
1)ratifier et mettre en œuvre toutes les mesures pertinentes des Nations unies ; 2)criminaliser le financement du terrorisme et le blanchiment d'argent qui y est associé ;3) adopter des mesures pour geler et confisquer les actifs terroristes ; 4) établir des mécanismes de signalement des transactions financières suspectes liées au terrorisme ; 5) renforcer la coopération internationale ; 6) établir des régimes de divulgation autour des systèmes alternatifs de remise de fonds et de "virement électronique" ; 7) et examiner l'adéquation des lois et réglementations relatives aux entités qui peuvent être utilisées abusivement pour le financement du terrorisme, 8)en particulier les organisations à but non lucratif.

[1056] FATF's approach is also driven by its view that 'all funds or other assets are fungible'. An organization may spend available assets on activities other than those for which they were originally intended. Even if specific funds or assets are used for non-attack expenses, they may substitute for other resources which can then be used to pay for attacks.
GILLARD, Emanuela-Chiara, "IHL and the humanitarian impact of counterterrorism measures and sanctions, unintended ill effects of well-intended measures", *Chatham House*, September 2021.

[1057] Nations Unies, Conseil de sécurité, Résolution 1373 (2001)
https://www.unodc.org/pdf/crime/terrorism/res_1373_french.pdf

[1058] HAYES, Ben, ibid.
LENFANT, François, VAN BROEKHOVEN, Lia, VAN LIERDE, Frank, « Les conséquences de la guerre contre le terrorisme sur le monde des ONG », *Cultures & Conflit*s, n° 76, 2009,
http://journals.openedition.org/conflits/17779

[1059] SULLIVAN, Gavin, HAYES, Ben, "Blacklisted : targeted sanctions, preemptive security and fundamental rights", ECCHR, 2010
https://www.ecchr.eu/fileadmin/Publikationen/Blacklisted.pdf
KASSEM, Ramzi, MIGNOT-MAHDAVI, Rebecca, SULLIVAN, Gavin," watchlisting the world : digital security infrastructures : informal law, and the "global war on terror", *JustSecurity,* 28/10/2021
https://www.justsecurity.org/78779/watchlisting-the-world-digital-security-infrastructures-informal-law-and-the-global-war-on-terror/
SULLIVAN, Gavin, HAYES, Ben, "Statewatch analysis, time to rethink terrorist blacklisting", *Statewatch Journal*, vol 20 no 3/4, 2010
https://www.statewatch.org/media/documents/analyses/no-120-terrorist-blacklisting.pdf

condamnation pénale pour fait de terrorisme n'est pas toujours nécessaire pour y être inscrite. Ces derniers leur reprochent aussi leur caractère politique. En effet, les listes américaines comprendraient majoritairement des organisations provenant de zones géographiques où les USA sont engagés militairement, comme en Afghanistan, en Irak, ou relevant de sa sphère d'influence, ou celle de ses alliés[1060].

Pour en venir aux humanitaires, la « guerre contre la terreur » a eu des répercussions paradoxales sur les acteurs de la solidarité internationale. Les ONG sont obligées pour accéder aux populations locales d'entrer en contact avec des groupes terroristes. Et elles peuvent acheminer des biens et des matériaux à des populations situées dans des zones contrôlées par des groupes armés. L'interdiction totale de tout contact avec des groupes terroristes est extrêmement rare[1061]. On peut dire qu'il existe parfois une forme d'autocensure de la part des humanitaires et certaines organisations s'interdisent alors de coopérer avec de tels groupes[1062]. Et surtout, certains territoires contrôlés par des terroristes peuvent être interdits d'accès, ce qui fait que les ONG ne peuvent que difficilement venir en aide aux individus ayant besoin d'assistance. L'application de mesures de contre-terrorisme peut ainsi contrevenir aux principes du droit humanitaire en excluant potentiellement des bénéficiaires d'une aide allouée selon des critères d'impartialité. Cela avait été le cas dans la zone frontalière en Syrie. Les bailleurs américains et anglais avaient imposé (avant de revenir sur leur décision) le fait de ne pas acheminer de l'aide via la frontière turco-syrienne, en raison de la présence de groupes djihadistes[1063]. Cela avait été le cas au Congo — en raison de la présence de Boko Haram. Et cela avait été le cas en 2010 en Somalie : une famine frappait une région où les Shebabs[1064] — visés par des sanctions — étaient influents. Pour accéder à ces différentes zones, les humanitaires doivent négocier à la fois auprès d'instances onusiennes et de groupes terroristes[1065], ce qui conduit dans certains cas à les amalgamer avec ces derniers[1066].

Ajoutons que les humanitaires peuvent être accusés de faciliter le transport de membres de groupes terroristes[1067], de dissimuler des informations les concernant, de les soutenir par

---

[1060] J BIERSTEKER, Thomas, ECKERT, Sue, TOURINHI, *Targeted sanctions*, Cambridge university press, 2016,405 p.
BIERSTEKER, Thomas, ECKERT, Sue, *Countering the financing of terrorism*, London : Routledge Taylor & Francis Group, 2008,360 p.

[1061] "Humanitarian action, counterterrorism measures and sanctions in Syria",Diakona International humanitarian law centre, August 2021 https://apidiakoniase.cdn.triggerfish.cloud/uploads/sites/2/2021/08/Diakonia_FactSheets-Sanctions_FullPacket.pdf

[1062] Guide pour l'action humanitaire basée sur les principes, gérer les risques liés à la lutte anti-terroriste, NRC, 2020, https://www.nrc.no/globalassets/pdf/reports/toolkit/nrc_risk_management_toolkit_principled_humanitarian_action_french.pdf

[1063] Some aid agencies halt use of Syrian border gate citing jihadists' taxes on trucks, 04/10/2018
https://www.reuters.com/article/us-mideast-crisis-syria-aid/some-aid-agencies-halt-use-of-syrian-border-gate-citing-jihadists-taxes-on-trucks-idUSKCN1ME1MJ
CUTTS, Mark, "Why the UN Security Council must vote for Syria aid access now", *The New Humanitarian*, O5/07/2022
https://www.thenewhumanitarian.org/opinion/2022/07/05/Why-the-UN-Security-Council-must-vote-for-Syria-aid

[1064] Il s'agit d'un groupe nommé Harakat al-Chabab al-Moudjahidin, soit un groupe islamiste somalien d'idéologie salafiste djihadiste créé en 2006 lors de l'invasion éthiopienne.

[1065] SCHELLHAMMER, Lean, « Breaking the silence, lessons from humanitarian access negotiations under counter-terrorism legislation in north western Syria », Chaberlin, 2021.

[1066] PAULUSSEN, Christophe, GILLARD, Emanuela-Chiara, "Staying in an Area controlled by a terrorist organisation: crime or operational necessity?, *International center for counter-terrorism*, ICCT, 11/01/2021https://www.icct.nl/publication/staying-area-controlled-terrorist-organisation-crime-or-operational-necessity

[1067] « Guerre Israel-Hamas : à Gaza, l'hôpital Al-Shifa toujours visé par des opérations israeliennes, la pression internationale s'accentue sur l'Etat hébreu », Le Monde, AFP, 16/11/202https://www.lemonde.fr/international/article/2023/11/16/guerre-israel-hamas-a-gaza-l-hopital-al-shifa-toujours-vise-par-des-operations-israeliennes-la-pression-internationale-s-accentue-sur-l-etat-hebreu_6200338_3210.html

différents moyens, leur procurer des soins médicaux[1068] et de l'assistance logistique (abris, biens en nature, nourriture, eau, etc.) ; de verser des salaires à du personnel venant de territoires contrôlés par des groupes armés. Cela a été tout récemment le cas de l'United Nations Relief and Works Agency for Palestine Refugees in the Near East (UNRAW) à Gaza[1069]. Ajoutons que MSF a pu être considéré comme une organisation terroriste en Syrie, au Niger, au Congo, au Cameroun par les gouvernements locaux, et des membres de l'organisation ont été arrêtés à ce titre[1070]. Ajoutons que de telles accusations ont été aussi portées contre le CICR au Burkina Fasso, à la suite d'une campagne de désinformation orchestrée par l'entreprise d'influence, Team Jorge[1071]. En substance, dans le cadre de la lutte contre le terrorisme, l'aide humanitaire est criminalisée, comme l'alerte l'ancienne rapporteuse de l'ONU contre le terrorisme, Agnès Callamard. [1072]

Mais dans le même temps, l'humanitaire peut servir les agendas sécuritaires des États. Les chercheurs Duncan McLean et Michiel Hofman nous rappellent ainsi que : « les attentats du 11 septembre 2001 ont complètement changé la donne pour les humanitaires. Une doctrine périphérique de lutte contre le terrorisme a été ressuscitée avec force, non seulement en tant que concept appliqué à l'échelle mondiale par l'Occident et les Nations unies, mais aussi par presque toutes les nations en guerre. (…) Les actions militaires menées par les États-Unis et leurs alliés en Afghanistan et en Irak ont réussi là où l'OTAN avait échoué au Kosovo, en ralliant largement les principales agences humanitaires à leur stratégie militaire et politique. »[1073] Ce contexte fait que les humanitaires n'apparaissent plus comme des acteurs neutres ; un facteur

---

[1068] "The ICRC's medical assistance to the victims of a NIAC on all sides of a NIAC could be rendered difficult based on a strict reading of some of the anti-terrorism instruments. It could imply, for instance, that medical services to persons rendered hors de combat by wounds or sickness, as well as to other persons under the control of an NSAG designated as "terrorist" could be prohibited as they may be considered as support or services to "terrorism"." ICRC engagement with Non State armed groups, why, how, for what purpose, and other salient issues. ICRC position paper, March 2021
PEJIC, Jelena, HERBET, Irénée, RODENHAUSER, Tilman, "ICRC engagement with non-state armed groups : why and how", *humanitarian law Policy ICRC blog*, 04/03/2021
https://blogs.icrc.org/law-and-policy/2021/03/04/icrc-engagement-non-state-armed-groups/

[1069] BERTHEMET, Tanguy, "Guerre Israel-Hamas : un rapport souligne le "rôle vital" de l'UNRWA malgré ses failles", 23/04/2024 https://www.lefigaro.fr/international/guerre-israel-hamas-un-rapport-souligne-le-role-vital-de-l-unrwa-malgre-ses-failles-20240423
Nations unies, Israel n'a toujours pas fourni de preuves liant l'UNRWA au Hamas, selon un rapport indépendant, 23/04/2024 https://www.courrierinternational.com/article/nations-unies-israel-n-a-toujours-pas-fourni-de-preuves-liant-l-unrwa-au-hamas-selon-un-rapport-independant
MATHIEU, Luc, "Gaza : Israel n'a fourni aucune preuve à l'ONU de l'infiltration de l'UNRAW par le Hamas", *Liberation*, 22/04/2024, https://www.liberation.fr/international/moyen-orient/gaza-israel-na-fourni-aucune-preuve-a-lonu-de-linfiltration-de-lunrwa-par-le-hamas-20240422_MUNTC6OY3BDTLJBQVPRJCMFZJY/
PAUPE, Marc, "Attention à ces nouvelles accusations d'Israel lian l'UNRWA et le Hamas", *France24*, 16/05/2024 https://www.france24.com/fr/%C3%A9missions/info-ou-intox/20240516-attention-%C3%A0-ces-accusations-d-isra%C3%ABl-liant-l-unrwa-et-le-hamas

[1070]BOUCHET-SAULNIER, Françoise, « The regrettable new normal : navigating humanitarian action in counter terrorism settings », MSF, 2021, https://www.msf.org/international-activity-report-2021/navigating-humanitarian-action-counter-terrorism-settings
BOUCHET-SAULNIER, Françoise, "How counterterrorism throws back wartime medical assistance and care to pre-Solferino Times", *IRRC* n°916-917, February 2022
https://international-review.icrc.org/articles/how-counterterrorism-throws-back-wartime-medical-assistance-to-pre-solferino-times-916
MSF, "Adding salt to the wound, the experience of MSF frontline workers providing impartial healthcare in counter-terrorism environments", october 2021 https://reliefweb.int/report/afghanistan/adding-salt-wound-experience-msf-frontline-workers-providing-impartial-healthcare

[1071] LELOUP, Damien, REYNAUD, Florian, « Quand la croix rouge était victime d'une campagne sophistiquée de déstabilisation », *Le Monde*, 16/02/2023

[1072] CALLAMARD, Agnes, "Saving lives is not a crime, Report of the Special Rapporteur of the Human Rights Council on extrajudicial, summary or arbitrary executions "(A/73/314), 6/08/2018

[1073] MCLEAN, Duncan, HOFMAN, Michiel, « Droit international humanitaire, souveraineté des États et érosion du consensus humanitaire : la fin de l'humanitarisme? », Droit international humanitaire: le grand retour... en arrière?, *Alternatives humanitaires*, n°23, juillet 2023.
HOFMAN, Hofman, "Humanitarians in the age of counter terrorism: rejected by rebels, co-opted by States", *Alternatives humanitaires*, n°7, 2018, p.12-25

de risque pour les ONG : ces dernières sont — en partie pour cette raison — la cible d'attaques de groupes armés[1074].

En somme, il arrive donc que les humanitaires se retrouvent dans des situations frisant l'illégalité. Et d'une part, les humanitaires sont accusés d'un soutien plus ou moins direct et plus ou moins conscient à des groupes terroristes, dans le même temps, l'aide humanitaire a pu être instrumentalisée à des fins de contre-terrorisme, et dans le même temps, le régime de sanction a pu être détourné, dans certains cas, à des finalités de répression de la société civile comme ont pu le documenter Ben Hayes[1075] ou Amnesty International[1076]. Alors, certes, il a pu exister des cas de détournement de l'aide destinée initialement à des bénéficiaires. Certaines ONG ont pu être accusées de servir de faux-nez et rediriger des financements humanitaires au profit de groupes terroristes[1077]. Cela dit, il est important de préciser que notre objectif n'est pas de documenter le détournement de l'aide humanitaire par des groupes terroristes. Nous n'en avons pas les moyens scientifiques, et notre sujet présent est

---

[1074] MSF, "The regrettable new normal: navigating humanitarian action in counter terrorism settings", 2021, https://www.msf.org/international-activity-report-2021/navigating-humanitarian-action-counter-terrorism-settings
"Humanitarian counterterrorism measures and sanctions in Syria", Diakonia International humanitarian Law Centre, 2021,https://apidiakoniase.cdn.triggerfish.cloud/uploads/sites/2/2021/08/Diakonia_FactSheets-Sanctions_FullPacket.pdf
MACKINTOSH, Kate, MACDONALD, Ingrid, "Counter terrorism and humanitarian action, Humanitarian negotiations", *Humanitarian Exchange*, n°22, 2013
PANTULIA, Sara, MACKINTOSH, Kate, ELHAWARY, Samir, METCALFE, Victoria, "Counter-terrorism and humanitarian action, tension, impact and ways forward", *HPG policy brief*, n°43, October 2011
ELLIOTT, Vittoria, PARKER, Ben, "Balancing act: anti-terror efforts and humanitarian principle, a conversation on how counter terrorist laws impede aid work", *The new humanitarian*, 26/11/2019
https://www.thenewhumanitarian.org/feature/2019/11/26/balancing-act-anti-terror-efforts-and-humanitarian-principles
« Les lois antiterroristes exposent les ONG humanitaires à la paralysie », *Le Monde*, 17/01/2020. https://www.lemonde.fr/idees/article/2020/01/17/les-lois-antiterroristes-exposent-les-ong-humanitaires-a-la-paralysie_6026151_3232.html
ANTOULY, Julien, « Quels sont les effets de la lutte contre le terrorisme sur l'humanitaire? », *Alternatives humanitaires*, n°18, 12/11/21 https://www.alternatives-humanitaires.org/fr/2021/11/12/quels-sont-les-effets-de-la-lutte-contre-le-terrorisme-sur-laction-humanitaire/

[1075] HAYES, Ben, "On shrinking space, a framing paper", *Transnational institute*, April 2017 https://www.brot-fuer-die-welt.de/fileadmin/mediapool/2_Downloads/Fachinformationen/Analyse/Analysis_68_The_impact_of_international_counterterrorism_on_CSOs.pdf

[1076] "India : Government weaponizing terrorism financing watchdog recommendations against civil society", Amnesty international, 27/09/2023 https://www.amnesty.org/en/latest/news/2023/09/india-government-weaponizing-terrorism-financing-watchdog-recommendations-against-civil-society/

[1077] FOLLOROU, Jacques, « En Afghanistan, les talibans utilisent des ONG pour contourner les sanctions », *Le Monde*, 25/10/2023https://www.lemonde.fr/international/article/2023/10/25/en-afghanistan-les-talibans-utilisent-des-ong-pour-contourner-les-sanctions_6196390_3210.html?utm_source=pocket_reader
HOOPER, Simon, « Charities warned that sending aid to Syria's Idlib could be a "terror offence", *Middle East Eye*, 08/12/2018
https://www.middleeasteye.net/news/charities-warned-sending-aid-syrias-idlib-could-be-terror-offence
Israel : l'ex-directeur de World Vision à Gaza reconnu coupable de détournement pour le Hamas", *le Figaro avec AFP*, 15/06/2022, https://www.lefigaro.fr/flash-actu/israel-l-ex-directeur-de-world-vision-a-gaza-reconnu-coupable-de-detournement-pour-le-hamas-20220615
BEHAR, Nissim, « En Israel, un humanitaire accusé d'être une "taupe du Hamas" », Libération, 05/08/2016
https://www.liberation.fr/planete/2016/08/05/en-israel-un-humanitaire-accuse-d-etre-une-taupe-du-hamas_1470409/
Israel sentences World Vision ex-Gaza chief to 12 years for aiding Hamas, AFP, France 24, 30/08/2022
https://www.france24.com/en/live-news/20220830-israel-sentences-world-vision-ex-gaza-chief-to-12-years-for-aiding-hamas
TRISKO, DARDEN, Jessica, "Humanitarian assistance has a terrorism problem. Can it be resolved?", *War on the Rocks*, 03/01/2019
https://warontherocks.com/2019/01/humanitarian-assistance-has-a-terrorism-problem-can-it-be-resolved/
Israel : l'ex-directeur de World Vision à Gaza reconnu coupable de détournement pour le Hamas", *le Figaro avec AFP*, 15/06/2022, https://www.lefigaro.fr/flash-actu/israel-l-ex-directeur-de-world-vision-a-gaza-reconnu-coupable-de-detournement-pour-le-hamas-20220615
BEHAR, Nissim, « En Israel, un humanitaire accusé d'être une "taupe du Hamas" », Libération, 05/08/2016
https://www.liberation.fr/planete/2016/08/05/en-israel-un-humanitaire-accuse-d-etre-une-taupe-du-hamas_1470409/
Israel sentences World Vision ex-Gaza chief to 12 years for aiding Hamas, AFP, France 24, 30/08/2022
https://www.france24.com/en/live-news/20220830-israel-sentences-world-vision-ex-gaza-chief-to-12-years-for-aiding-hamas
TRISKO, DARDEN, Jessica, "Humanitarian assistance has a terrorism problem. Can it be resolved?", *War on the Rocks*, 03/01/2019
https://warontherocks.com/2019/01/humanitarian-assistance-has-a-terrorism-problem-can-it-be-resolved/

autre : il s'agit de mettre en lumière les effets des mesures de lutte contre le financement du terrorisme en matière de protection des données [1078].

Pour entrer dans le vif de notre sujet, on remarquera d'abord que les institutions internationales comme le GAFI ou le conseil de Sécurité de l'ONU ont pris part à la criminalisation du secteur humanitaire, considéré comme étant à risque en ce qui concerne le financement du terrorisme. Cette position était traduite dans la 8e recommandation du GAFI. Cette instance a modifié depuis sa posture, mais cette conception du secteur humanitaire reste prégnante chez de nombreux acteurs[1079]. Et elle a différents impacts d'un point de vue opérationnel. En réaction, des programmes peuvent être modifiés ou annulés. Des populations ou des individus peuvent ne pas recevoir l'aide nécessaire à leur survie. Ceci peut être dû à un refus de financement par les bailleurs[1080] ou d'un blocage des transferts de fonds par une banque, ou bien du fait d'une forme d'autocensure par les humanitaires eux-mêmes. Ces derniers peuvent limiter leurs actions par peur d'être poursuivis sur le plan pénal. Ou bien certaines ONG peuvent elles-mêmes refuser de bénéficier de certains financements, afin de ne pas avoir à se plier à des clauses de contre-terrorisme trop restrictives. En effet, respecter les mesures de contre-terrorisme peut impliquer des délais supplémentaires et augmente le coût d'une opération, rendant les ONG moins souples et réactives à l'urgence[1081]. Notons au passage qu'il existe aussi des répercussions en matière de connectivité : les ONG peuvent être mises en difficulté lorsque leurs fournisseurs d'accès internet locaux sont sous le coup de sanction[1082].

---

[1078]CHARNY, R. Joel, "Counter-terrorism and humanitarian action : the perils of zero tolerance", *War on the rocks*, 20/03/2019 https://warontherocks.com/2019/03/counter-terrorism-and-humanitarian-action-the-perils-of-zero-tolerance/

[1079] CALLAMARD, Agnes, "Saving lives is not a crime, report of the Special Rapporteur of the Human Rights Council on extrajudicial, summary or arbitrary executions (A/73/314), 6/08/2018

[1080] « Most donors have not yet defined exactly how they require NGOs to comply. Our organisation as a recipient of funds is asked by the donors to explain how counter- terrorism requirements and sanctions will be complied with, but we receive no guidance from the donors." MCCARTHY, Gilian, "Adding to the evidence, the impacts of sanctions and restrictive measures on humanitarian action", VOICE, March 2021 https://voiceeu.org/publications/adding-to-the-evidence-the-impact-of-sanctions-and-restrictive-measures-on-humanitarian-action.pdf
MACKINTOSH, Kate, DUPLAT, Patrick, "Study of the impact of donor counter-terrorism measures on principled humanitarian action", Norwegian Refugee council, July 2013, https://www.nrc.no/globalassets/pdf/reports/study-of-the-impact-of-donor-counterterrorism-measures-on-principled-humanitarian-action.pdf

[1081]"Humanitarian action, counterterrorism measures and sanctions in Syria",Diakona International humanitarian law centre, August 2021 https://apidiakoniase.cdn.triggerfish.cloud/uploads/sites/2/2021/08/Diakonia_FactSheets-Sanctions_FullPacket.pdf
O'LEARY, Emma, "Politics and principles : the impact of counterterrorism measures and sanctions on principled humanitarian action, *International review of the red cross*, n°916-917, February 2022 https://international-review.icrc.org/articles/politics-and-principles-the-impact-counterterrorism-measures-on-principled-humanitarian-action-916
PANTULIANO, Sara, MACKINTOSH, Kate, ELHAWARY, Samir, METCALFE, Victoria, "Counter-terrorism and humanitarian action, tensions, impact and ways forward", HPG Policy Brief n°43, October 2011 http://cdn-odi-production.s3.amazonaws.com/media/documents/7347.pdf
"Detrimental impacts: how counter-terror measures impede humanitarian action, Interaction", April 2021 https://www.interaction.org/wp-content/uploads/2021/04/Detrimental-Impacts-CT-Measures-Humanitarian-Action-InterAction-April-2021.pdf
ROEPSTORFF, Kristina, FALTAS, Charlotte, HOVELMANN, Sonja, "Counterterrorism measures and sanction regimes, shrinking space for humanitarian aid organizations", Chaberlin, February 2020 https://www.chaberlin.org/wp-content/uploads/2020/02/2020-02-counterterrorism-en-online.pdf
SPARKS, Riley, "A year after Taliban return, Canadian anti-terror law still bars NGOs", *The New humanitarian*, 06/07/2022 https://www.thenewhumanitarian.org/analysis/2022/07/06/Afghanistan-anti-terrorism-Taliban-aid-and-law
ELLIOTT, Vittoria, PARKER, Ben, "Balancing act: Anti-terror efforts and humanitarian principles", *The New Humanitarian,* 26/11/2019 https://www.thenewhumanitarian.org/feature/2019/11/26/balancing-act-anti-terror-efforts-and-humanitarian-principles
THEILER, Zach, "How vague money laundering and counter-terror rules slow aid", *The New humanitarian*, 23/05/2023 https://www.thenewhumanitarian.org/analysis/2023/05/23/how-vague-money-laundering-and-counter-terror-rules-slow-aid
« Principes sous pression, l'impact des mesures antiterrorisme et de prévention/lutte contre l'extrémisme violent sur l'action humanitaire basée sur les principes, Conseil norvégien pour les réfugiés », 2018https://www.nrc.no/globalassets/pdf/principles-in-practice/principles-under-pressure-french.pdf

[1082] « Protéger les civils contre les menaces numériques lors des conflits armés », Conférence, Geode, 21/05/2024. https://geode.science/conference-proteger-les-civils-contre-les-menaces-numeriques-lors-des-conflits-armes/

En somme, comme la juriste Françoise Bouchet-saulnier l'alerte, les sanctions peuvent aller jusqu'à porter atteinte au droit international humanitaire : « les définitions de financement, de soutien matériel au terrorisme ou d'entente avec les terroristes recouvrent et criminalisent toutes les activités de secours que le droit humanitaire a pourtant rendues obligatoires au titre de l'action humanitaire dans les situations de conflit. Elles abolissent également la catégorie de "civils" victimes de conflit et lui substituent celle de soutiens, complices ou suspects de collusion avec les terroristes. » [1083]

En réaction, les humanitaires plaident pour un plus grand respect du DIH, en vue de garantir l'indépendance, la neutralité et l'impartialité des ONG[1084]. Et différentes coalitions d'ONG tentent d'obtenir une exception générale aux sanctions onusiennes et étatiques [1085]. Jusqu'alors, les exceptions accordées pouvaient être temporaires et concerner une crise spécifique (la Somalie en 2010) ; être données au cas par cas (comme le fait le département du Trésor américain, qui accorde des licences aux ONG). Or les ONG présentent ces dérogations temporaires comme pouvant conduire à de la surcharge administrative, du fait des démarches nécessaires pour les obtenir, pour comprendre leur interaction avec d'autres régimes de sanction. Ainsi, des États comme la Suisse, l'Australie, la Grande-Bretagne, les Philippines, le Tchad et l'Éthiopie ont adopté des aménagements plus larges pour les ONG. Certaines exceptions s'appliquent à toutes ONG humanitaires. D'autres s'appliquent qu'à certaines ONG. Certaines dérogations concernent l'ensemble du régime de sanction, comme en Suisse. D'autres se limitent à certains points : par exemple, les législations britanniques, australiennes et néozélandaises autorisent le fait de pénétrer dans des « no go zones ».

Comme on l'a dit, au sein du GAFI, les humanitaires ont été tout d'abord considérés comme étant une catégorie à haut risque en matière de financement du terrorisme. La recommandation 8 du GAFI cible directement les ONG. Mais le GAFI a cependant revu sa position en 2016, en défendant une posture plus nuancée, à la suite de longues négociations et échanges avec les ONG[1086]. Cela dit, cette évolution n'aurait pas été suivie de beaucoup d'effets au niveau des pratiques[1087]. Les ONG n'auraient pas perçu un changement franc et

---

[1083] BOUCHET-SAULNIER, Françoise, « La guerre contre le terrorisme ou le nouvel ordre in-humanitaire », *AOC*, 07/12/2018 https://aoc.media/opinion/2018/12/07/guerre-contre-terrorisme-nouvel-ordre-in-humanitaire/

[1084] "The interrelationship between counter-terrorism frameworks and international humanitarian law",United Nations security council counter-terrorism Committee Executive directorate, January 2022 https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2022/Jan/cted_ihl_ct_jan_2022.pdf
GILLARD, Emanuela-Chiara, "IHL and the humanitarian impact of counterterrorism measures and sanctions", *Chathamhouse*, September 2021 https://www.chathamhouse.org/sites/default/files/2021-09/2021-09-03-ihl-impact-counterterrorism-measures-gillard_0.pdf
LEWIS, Dustin A., MODIRZADEH, Naz K.,BLUM,Gabriella, "Medical Care in Armed Conflict: International Humanitarian Law and State Responses to Terrorism," Legal Briefing, Harvard Law School Program on International Law and Armed Conflict, September 2015. https://pilac.law.harvard.edu/mcac-report//front-matter
« Terrorisme, contreterrorisme et droit international humanitaire », 17e colloque de Bruges, 20-21 octobre 2016, College d'Europe, CICR, https://www.coleurope.eu/sites/default/files/uploads/page/collegium_47_v7.pdf
BOUCHET-SAULNIER, Françoise, "How counterterrorism throws back wartime medical assistance and care to pre-Solferino Times", *IRRC* n°916-917, February 2022
https://international-review.icrc.org/articles/how-counterterrorism-throws-back-wartime-medical-assistance-to-pre-solferino-times-916

[1085] MUNICHSDORFER, Ansgar, TERREY, Sofie-Marie, "Humanitarian exemptions: illusive progress in safeguarding humanitarian assistance in the international counterterrorism architecture? "AEL, 2022, Academy of European Law, european society of international law paperhttps://cadmus.eui.eu/bitstream/handle/1814/75025/WP_AEL_2022_15.pdf?sequence=1&isAllowed=y

[1086] VAN BROEKHOVEN, Lia, GOSWAMI, Sangeeta, "Can stakeholder dialogues help solve financial access restrictions faced by non-profit organizations that stem from countering terrorism financing standards and international sanctions?", *IRRC* n° 916-917, february 2022

[1087] HAYES, Ben, "The impact of international counter-terrorism on civil society organisations, Understanding the role of the Financial Action task Force", Brot Fur die Welt, April 2017
https://www.brot-fuer-die-welt.de/fileadmin/mediapool/2_Downloads/Fachinformationen/Analyse/Analysis_68_The_impact_of_international_counterterrorism_on_CSOs.pdf

massif sur la façon dont elles peuvent être perçues. Et comme le déplorent les membres de la coalition « Charity and Security », les bailleurs et les banques continuent d'éviter le risque plutôt que de le gérer[1088].

Concernant les instances onusiennes, la Stratégie des Nations unies adoptée en 2006 comprend en annexe un plan d'action qui traite dans son paragraphe 15 de l'octroi de dérogation pour raisons humanitaires. Toutefois, il manque de précision, et surtout n'impose pas de mise en œuvre de mesures spécifiques. Et certes, en Somalie, en 2011, une levée temporaire des sanctions contre le groupe Al Shabaad a été obtenue après de fortes activités de plaidoyer par des ONG auprès des instances onusiennes[1089]. Mais ce n'est que vingt ans après l'élaboration de l'architecture du contre-terrorisme que l'ONU a inscrit à son agenda l'impact des résolutions sur le secteur de la solidarité internationale.

En 2016, MSF avait alerté le comité contre le terrorisme du Conseil de sécurité de l'ONU sur ce sujet[1090]. Et fin 2019, ce dernier a reconnu ce danger et demandé aux États de limiter l'impact des mesures antiterroristes sur l'action humanitaire, afin d'être conforme au droit humanitaire en situation de conflit. Les Résolutions 2462 et 2482 de 2019 requièrent ainsi aux États « de tenir compte des effets potentiels des mesures antiterroristes sur les activités exclusivement humanitaires, y compris les activités médicales, qui sont menées par des acteurs humanitaires impartiaux d'une manière conforme au droit international humanitaire ». Mais elles ne sont absolument pas contraignantes, et ne comprennent pas d'indications plus claires sur la façon de mener à bien cet objectif[1091].

Et en 2021 en réaction à la prise de pouvoir des talibans s'en est suivi une discussion portant sur la nécessité d'actualiser les sanctions. L'Afghanistan était en effet visé par la sanction 1988 datant de 2011. À cette occasion, la sanction 2615 a été adoptée. Or cette dernière ménage une exception humanitaire[1092]. Les sanctions unilatérales sont cependant maintenues[1093], et la véritable évolution date de décembre 2022. La résolution 2664 ménage une exemption humanitaire pour les sanctions 1267 (1999), 1989 (2011) et 2253 (2015) relatives à l'EIIL (Daech), Al-Qaida et des entités associées pour une période de deux ans. La résolution se base sur une définition large de l'activité humanitaire, qui ne se restreint pas à l'intervention d'ONG dans des conflits armés, et englobe d'autres formes d'assistance que la dimension strictement

---

[1088]" FATF's recommendation 8 on non-profit organization: a new tool to unfairly and dangerously shrink civil society space", Working group, torture&terrorism, OMCT, SoS-Torture network, 10/07/2019 https://www.ohchr.org/sites/default/files/Documents/Issues/Terrorism/SR/Submissions/OMCT_GA74CT.pdf
"Event summary: the future of Fatf recommendation 8 : for financial integrity and for civil society", *Charity and Security*, 16/10/2023 https://charityandsecurity.org/news/event-summary-the-future-of-fatf-recommendation-8-for-financial-integrity-and-for-civil-society/

[1089] "Somalia: the 2011 Famine and its response", *Charity and Security*, July 2013https://charityandsecurity.org/humanitarian-safeguards/somalia-2011-famine-and-its-response/

[1090] BOUCHET-SAULNIER, Française, « Comment protéger les acteurs humanitaires dans le contexte des conflits armés antiterroristes: relégitimer ou sanctionner? », *Défis humanitaires*,27/11/2020 https://defishumanitaires.com/2020/11/27/lois-anti-terroristes-humanitaire/

[1091] Le Conseil de sécurité réfléchit aux moyens de mettre fin au rétrécissement de l'espace humanitaire dans les situations de conflits, CS/13760, 01/04/2019 https://press.un.org/fr/2019/cs13760.doc.htm

[1092] "the processing and payment of funds, other financial assets or economic resources, and the provision of goods and services necessary to ensure the timely delivery of such assistance or to support such activities. " Le Conseil de Sécurité décide « that humanitarian assistance and other activities that support basic human needs in Afghanistan are not a violation of paragraph 1 (a) of resolution 2255 (2015), and that the processing and payment of funds, other financial assets or economic resources, and the provision of goods and services necessary to ensure the timely delivery of such assistance or to support such activities are permitted"

[1093] SARFATI, Agathe, "An unfinished agenda : carving out space for humanitarian action in the UN security Council's counterterrorism resolutions and related sanctions, International Peace Institute, March 2022https://www.ipinst.org/wp-content/uploads/2022/03/Humanitarian-Action-in-UN-Sanctions-Regimes-PDF.pdf

médicale de l'aide. L'exemption ne concerne pas seulement les organisations de l'ONU, mais aussi l'ensemble des membres dotées du statut d'observateur auprès de l'assemblée générale de l'ONU ; et les ONG bénéficiant de financement bilatéral ou multilatéral. Cela dit, le chercheur Julien Antouly s'interroge sur son application à l'échelle régionale et nationale[1094].

Concernant les USA, le régime de sanction américain est un véritable mille-feuille bureaucratique. C'est d'abord le département du trésor et l'Office of Foreign Assets Control (OFAC) qui émettent leur propre liste de sanctions et des licences d'exemption à l'exportation de biens[1095]. Longtemps, ces dernières ont été édictées au cas par cas. [1096]On assisterait cependant à un assouplissement progressif du cadre pour les ONG. Le nombre de licences accordées par l'OFAC serait en augmentation, surtout depuis le mandat du président Joe Biden. Et en réponse à la résolution 2664 de l'ONU adoptée en décembre 2022, le département du Trésor et l'OFAC : **«** a délivré ou modifié des licences générales afin de faciliter l'acheminement de l'aide humanitaire dans la majorité des régimes de sanctions américaines. Les licences générales autorisent certaines transactions pour une catégorie entière d'acteurs — en l'occurrence, les organisations humanitaires — sans exiger de ces acteurs qu'ils fassent une demande de licence au cas par cas. »[1097]

Mais même en bénéficiant de licences générales d'exception de l'OFAC, les ONG risquent des poursuites pénales pour avoir fourni un soutien matériel, même occasionnel, à des entités ciblées en vertu de la loi de 1996 sur l'antiterrorisme et la peine de mort (AEDPA) et de la loi de 1977 sur les pouvoirs économiques en cas d'urgence internationale (IEEPA). Dernier point crucial, il va sans dire que le contexte dramatique et extrêmement tendu du conflit israélo-palestinien tend à modifier ce mouvement d'ouverture. À cette date l'OFAC a maintenu ces licences d'exception générale, même pour les ONG opérant à Gaza[1098]. L'OFAC a surtout ciblé des acteurs clefs[1099]. Ainsi, le financement à l'UNRWA a été suspendu depuis qu'Israël accuse l'organisme onusien d'avoir employé des membres du Hamas[1100]. La question de l'influence

---

[1094] « Comme cela a été précédemment souligné, la résolution 2664 a une portée contraignante et obligatoire pour l'ensemble des États membres de l'ONU. Toutefois, il convient de s'attarder sur les modalités de mise en œuvre par les États. En effet, dans de nombreux cas, l'application des régimes de sanctions et des mesures restrictives qui y sont associées (gel des avoirs, interdiction de voyage…) repose sur des instruments de droit interne ou régional. » ANTOULY, Julien, « La résolution 2664 du Conseil de sécurité : une étape historique vers une meilleure protection des activités humanitaires », *La Revue des droits de l'homme*, Actualités Droits-Libertés, http://journals.openedition.org/revdh/16070

[1095]MACKINTOSH, Kate, DUPLAT, Patrick, Study of the Impact of Donor Counter-Terrorism Measures on Principled Humanitarian Action, NRC, 2013https://www.nrc.no/globalassets/pdf/reports/study-of-the-impact-of-donor-counterterrorism-measures-on-principled-humanitarian-action.pdf

[1096] La definition du soutien materiel à un groupe terroriste est defini comme tel selon le code juridique américain : "Quiconque fournit un soutien matériel ou des ressources, ou dissimule ou déguise la nature, l'emplacement, la source ou la propriété d'un soutien matériel ou de ressources, en sachant ou en ayant l'intention de les utiliser pour préparer ou commettre un acte terroriste."US Code title 18§ 2339 Ahttps://uscode.house.gov/view.xhtml?req=(title:18%20section:2339B%20edition:prelim)

[1097] « issued or amended general licenses to ease the delivery of humanitarian aid across the majority of U.S. sanctions regimes. General licenses authorize certain transactions for an entire class of actors—in this case, humanitarian organizations—without requiring these actors to apply for licenses on a case-by-case basis." CRYSTAL, Caroline, "landmark humanitarian sanctions exemption is a massive win but needs more support",CARNEGIE Endowment for international peace, 20/03/2023 https://carnegieendowment.org/2023/03/20/landmark-un-humanitarian-sanctions-exemption-is-massive-win-but-needs-more-support-pub-89311

[1098] OFAC Issues compliance communiqué : guidance for the provision of humanitarian assistance to the Palestinian People 14/11/2023https://charityandsecurity.org/news/ofac-issues-compliance-communique-guidance-for-the-provision-of-humanitarian-assistance-to-the-palestinian-people/

[1099] LIS, SYLWIA, PETTERD, Anne, GODFRAY, Julian, ANDREEF, Daniel, FOLEY, Kristen, O'BRIEN, Rob, RUSSELL, Nicola, "US, UK, Australia Target Additional Hamas Financial Networks and Facilitators of Virtual Currency Transfers, Sanctionnews, Baker McKenzie, 08/02/2024 https://sanctionsnews.bakermckenzie.com/us-uk-australia-target-additional-hamas-financial-networks-and-facilitators-of-virtual-currency-transfers/

[1100] BERTHEMET, Tanguy, "Guerre Israel-Hamas : un rapport souligne le "rôle vital" de l'UNRWA malgré ses failles", 23/04/2024 https://www.lefigaro.fr/international/guerre-israel-hamas-un-rapport-souligne-le-role-vital-de-l-unrwa-malgre-ses-failles-20240423

de cette séquence historique sur le régime plus global d'exception humanitaire aux sanctions se pose. Mais elle dépasse évidemment le cadre de la thèse, cette dernière ayant été écrite concomitamment au conflit, nous ne disposons pas de sources sur le sujet.

L'architecture européenne de lutte contre le financement du terrorisme est plus légère, le terrorisme étant resté un temps de l'ordre du régalien[1101]. Précisons simplement qu'au niveau européen, la position commune 2001/931/PSC traduit directement la résolution onusienne 1373 de 2001, et depuis 2016, l'UE à sa propre liste de sanction contre l'EI/Daech et Al-Qaida. Mais ce n'est qu'en 2017 qu'une directive — pourtant critiquée par les associations pour les dérives qu'elle implique en matière de droits de l'homme[1102] — inclut une mesure d'exemption humanitaire. Si l'on prend le texte de loi dans sa généralité, il adopte une conception large de la pénalisation du financement du terrorisme, définie dans son article 11. Ce point a été dénoncé par les ONG de défense de droits de l'homme. Mais, l'article 9 de la directive 2017/541 comporte deux considérants introduits par le Parlement européen[1103]. Ils comprennent des mesures d'exemption humanitaires. Mais ce ne sont pas des paragraphes contraignants, d'où le fait qu'ils peuvent être laissés à l'interprétation des États. Et autre précision d'importance : cette exemption ne concerne que le contenu de la directive… et non pas l'ensemble des sanctions européennes (qui peuvent être cependant amendées par la résolution onusienne de décembre 2022, voir plus haut).
Enfin, on peut trouver quelques indications en faveur d'une prise en compte de l'exception humanitaire dans les conclusions sur l'aide humanitaire en novembre 2019 du conseil de l'Union européenne[1104]. Elles apparaissent aussi dans la politique sur l'action extérieure de

---

Nations unies, Israel n'a toujours pas fourni de preuves liant l'UNRWA au Hamas, selon un rapport indépendant, 23/04/2024 https://www.courrierinternational.com/article/nations-unies-israel-n-a-toujours-pas-fourni-de-preuves-liant-l-unrwa-au-hamas-selon-un-rapport-independant

MATHIEU, Luc, "Gaza : Israel n'a fourni aucune preuve à l'ONU de l'infiltration de l'UNRAW par le Hamas", 22/04/2024, https://www.liberation.fr/international/moyen-orient/gaza-israel-na-fourni-aucune-preuve-a-lonu-de-linfiltration-de-lunrwa-par-le-hamas-20240422_MUNTC6OY3BDTLJBQVPRJCMFZJY/

PAUPE, Marc, "Attention à ce nouvelles accusations d'Israel liant l'UNRWA et le Hamas", France24, Info-ou-Intox, 16/05/2024 https://www.france24.com/fr/%C3%A9missions/info-ou-intox/20240516-attention-%C3%A0-ces-accusations-d-isra%C3%ABl-liant-l-unrwa-et-le-hamas

[1101] JAKOB, Fabien. « L'Union européenne et la lutte contre le financement du terrorisme. » *Études internationales*, volume 37, number 3, septembre 2006, p. 423–437. https://doi.org/10.7202/014240ar

[1102] « the Directive, enacted in 2017 after an expedited legislative process, criminalizes a wide range of conduct related to terrorism. The Directive establishes an overly broad definition of terrorism and requires states to include in their criminal law offences that are often not closely linked to the perpetration of a terrorist act. These include offences of travel for the purpose of terrorism, participation in a terrorist group, and public provocation to commit acts of terrorism. Because the terms of the offences are so widely drawn, safeguards in national law and practice are essential to ensure that they are not applied where there is no clear link to a principal offence of terrorism and/or no intent to contribute to such a principal offence, to prevent arbitrary application, including action based on racial prejudices of perceived dangerousness » EU: counter-terrorism laws must comply with human rights obligations, European Center for not for profit law, Amnesty International, Fidh, ENAR, Internatonal coalition of jurist, 2021
https://www.enar-eu.org/wp-content/uploads/eu_combating_terrorism_directive_statement_160621final.pdf

Directive (EU) 2017/541 on combating terrorism, impact on fundamental rights and freedoms, European Agency for fundamental rights, 2021 https://policehumanrightsresources.org/content/uploads/2021/12/fra-2021-directive-combating-terrorism_en.pdf?x49094

European Commission's proposal for a Directive of the European Parliament and of the Council on Combating Terrorism and Replacing Council Framework Decision 2002/475/JHA on Combating Terrorism, 2016
https://icj2.wpenginepowered.com/wp-content/uploads/2016/02/EU-Directive-terrorism-Advocacy-Analysis-Brief-2016-ENG.pdf

[1103] https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=celex%3A32017L0541#d1e614-6-1

(37)La présente directive ne saurait avoir pour effet de modifier les droits, obligations et responsabilités des États membres découlant du droit international, y compris du droit international humanitaire. La présente directive ne régit pas les activités des forces armées en période de conflit armé, au sens donné à ces termes en droit international humanitaire, lesquelles sont régies par ce droit, ni les activités menées par les forces militaires d'un État dans l'exercice de leurs fonctions officielles, dans la mesure où elles sont régies par d'autres règles de droit international.

(38)Les activités humanitaires menées par des organisations humanitaires impartiales reconnues par le droit international, y compris le droit international humanitaire, ne relèvent pas du champ d'application de la présente directive, tout en prenant en considération la jurisprudence de la Cour de justice de l'Union européenne.

[1104] L'aide humanitaire et le droit international humanitaire - Conclusions du Conseil (25 novembre 2019) https://data.consilium.europa.eu/doc/document/ST-14487-2019-INIT/fr/pdf

l'UE en matière de lutte contre le terrorisme en juin 2020[1105]. Et l'UE a transposé la résolution 2664 pour les sanctions onusiennes, et a progressivement aménagé des exemptions pour une partie de ses sanctions des listes autonomes (d'après le CICR 27 sur 39)[1106].

Ces paragraphes sont à relier aux différentes discussions portant sur la façon de lier droit et régime d'exception. Tout un ensemble de chercheurs mène une réflexion sur les liens entre dérogation à la norme, état d'urgence et Etat de droit, sur l'articulation entre régime d'exception, souveraineté et démocratie[1107]. On remarquera simplement que les humanitaires ne négocient pas nécessairement une suppression générale du régime d'exception, mais la possibilité de se défaire de ce qui apparait comme un frein à l'action humanitaire d'urgence, qui serait empêchée par ce qui est parfois considéré par certains rapports d'ONG des contraintes bureaucratiques. Si elles plaident pour le fait de bénéficier d'un statut à part, les ONG ne mettent pas l'accent en premier chef sur une suspension générale des sanctions. Du moins, cet objectif n'est pas exprimé en tant que tel lors de différentes négociations menées par des organisations humanitaires. Leurs positionnements contrastent avec d'autres discours, portés par des acteurs attachés à la défense des droits de l'homme, comme la rapporteuse des Nations unies, qui évoque en premier lieu la nécessité de garantir de façon globale le caractère proportionné de l'ensemble des mesures de contreterrorisme, ainsi que leur mise en balance avec d'autres droits humains.

## Section 2 — Bailleurs humanitaires et lutte contre le financement du terrorisme

[1105]Dans sa « *Communication to the European Parliament and the Council on the EU's humanitarian action: new challenges, same principles* » du 10 mars 2021, la Commission européenne a également rappelé l'importance du soutien aux partenaires et la nécessité de renforcer son action pour garantir une inclusion systématique d'exemptions humanitaires dans les régimes de sanctions européennes.
https://www.consilium.europa.eu/fr/press/press-releases/2020/06/16/preventing-and-countering-terrorism-and-violent-extremism-council-adopts-conclusions-on-eu-external-action/
Communication de la Commission au Parlement européen et au Conseil sur l'action humanitaire de l'UE: nouveaux défis, mêmes principes
Conclusions du Conseil (20 mai 2021)https://data.consilium.europa.eu/doc/document/ST-8966-2021-INIT/fr/pdf
[1106]Humanitarian action: EU introduces exemptions to sanctions to facilitate the delivery of assistance, PRESS RELEASE 253/23 31/03/2023
https://www.consilium.europa.eu/en/press/press-releases/2023/03/31/humanitarian-action-eu-introduces-exemptions-to-sanctions-to-facilitate-the-delivery-of-assistance/pdf
Humanitarian action: EU introduces further exception to sanctions, 19/02/2024
https://www.consilium.europa.eu/en/press/press-releases/2024/02/19/humanitarian-action-eu-introduces-further-exception-to-sanctions/
The EU Delegation to the UN Office and other international organisations in Geneva presents its compliments to the Office of the High Commissioner and has the honour to refer to the joint communication dated 26 October 2022 (ref AL OTH 106/2022).
https://spcommreports.ohchr.org/TMResultsBase/DownLoadFile?gId=37290
HUVE, Sophie, MOULIN, Guillemette, FERRARO, Tristan, "Unblocking aid : the EU's 2023 shift in sanctions policy to safeguard humanitarian efforts, *Humanitarian law& policy,* 23/01/2024
https://blogs.icrc.org/law-and-policy/2024/01/23/unblocking-aid-eu-2023-sanctions-policy-humanitarian-efforts/
[1107] SULLIVAN, Gavin, HAYES, Ben, "Blacklisted: targeted sanctions, preemptive security and fundamental rights", ECCHR, 2010 https://www.ecchr.eu/fileadmin/Publikationen/Blacklisted.pdf
BIGO, Didier, "Security, exception, ban and surveillance", in: LYON, David (ed), Theorizing surveillance, the panopticon and beyond,Wilan publiching 2006, p.46-68
BIGO Didier, « De « l'état d'exception » », *NAQD*, 2007/1 (N° 24), p. 103-128. DOI : 10.3917/naqd.024.0103. URL : https://www-cairn-info.ezproxy.utc.fr/revue-naqd-2007-1-page-103.htm

Après avoir planté le décor, on peut en venir à notre objet d'étude : les répercussions des mesures de lutte contre le financement du terrorisme en matière d'exigence de criblage de la part des bailleurs de fonds. Pour commencer, il peut exister dans les contrats des bailleurs des clauses relatives au contreterrorisme[1108]. Par exemple, les clauses des contrats d'USAID contiennent un certificat antiterroriste[1109]. Ces dernières indiquent les modalités nécessaires pour s'assurer que l'ONG respecte le cadre législatif en vigueur, afin que les fonds ne bénéficient pas à une personne désignée comme étant terroriste par telle ou telle liste onusienne, régionale ou nationale.

Différents aspects de ces clauses peuvent être problématiques pour les ONG : l'obligation de notification d'un groupe terroriste au bailleur, le risque de politisation de l'aide, du fait que les ONG sont tenues de « s'engager dans la guerre contre le terrorisme », le manque de précision de la définition de ce qui constitue une forme de « soutien matériel »[1110], le fait qu'une ONG doit être tenue responsable d'un détournement de l'aide, quand bien même elle n'en avait pas connaissance, le fait que ces clauses se répercutent sur les partenaires de l'ONG[1111].

Ces exigences peuvent toutefois varier. Tout dépend du bailleur, du pays où doit se déployer le projet, de l'ONG et de son statut. Une ONG reconnue ou une agence de l'ONU ne feront pas face aux mêmes exigences qu'une plus petite structure ou une ONG que le bailleur ne connait pas. La nature de l'aide joue aussi, puisqu'il est question de contrôle de financement, les programmes de transferts monétaires sont logiquement suivis de façon plus stricte.

Cela dit, il existe certaines tendances. Des bailleurs comme le Danemark, la Norvège, la Suède ou la Suisse n'ont pas de clauses relatives aux mesures de contreterrorisme dans leurs contrats. A contrario, il est connu que les bailleurs américains, canadiens, australiens et britanniques ont les clauses de contreterrorisme les plus exigeantes. Et effectivement, selon un enquêté « *le Royaume-Uni fait partie des donateurs demandant beaucoup d'informations, le DFID, c'est eux qui fournissent, ils font partie des personnes qui donnent beaucoup d'argent et qui demandent beaucoup d'informations, ce sont des pays qui font partie des 5 eyes, qui surveillent le plus*. » [1112]

---

[1108] "An Analysis of Contemporary Counterterrorism-related Clauses in Humanitarian Grant and Partnership Agreement Contracts", Counterrorism and humanitarian engagement project, Harvard, May 2014, https://archive.blogs.harvard.edu/cheproject/files/2013/10/CHE_Project_-_Counterterrorism-related_Humanitarian_Grant_Clauses_May_2014.pdf

[1109] Ce dernier atteste que le porteur de projet « à sa connaissance, n'a pas apporté au cours des dix dernières années - et prendra toutes les mesures raisonnables afin de s'assurer qu'il n'apporte pas ni n'apportera pas sciemment, un soutien matériel à tout individu ou entité qui commet, tente de commettre, défend, facilite ou participe à des actions terroristes, ou a commis, tenté de commettre, défendu, facilité ou participé à des actions terroristes » USAID, Certifications, Assurances and Other Statements of the Recipient, 2013.

[1110] « A respondent noted that it is unclear whether these broader "associated with" terrorism provisions are meant to prohibit, for instance, transactions with people who dig latrines that are later used by designated terrorists, with family members of designated terrorists, or with cash-for-work program staff who construct houses or other buildings that are subsequently used by designated terrorists. »
"Screening of final beneficiaries of humanitarian programs", Diakona International humanitarian law Centre, August 2021 https://apidiakoniase.cdn.triggerfish.cloud/uploads/sites/2/2021/08/Diakonia_FactSheets_Screening.pdf

[1111] "An Analysis of Contemporary Counterterrorism-related Clauses in Humanitarian Grant and Partnership Agreement Contracts", Counterrorism and humanitarian engagement project, Harvard, May 2014, https://archive.blogs.harvard.edu/cheproject/files/2013/10/CHE_Project_-_Counterterrorism-related_Humanitarian_Grant_Clauses_May_2014.pdf

[1112] Entretien n°44, OI 2, DPO, 07/03/2021

Un aspect spécifique de ces contrats nous intéresse : les différentes mesures de « vigilance raisonnable » et de gestion du risque terroriste. Certains contrats de financement précisent en effet que des mesures doivent être prises pour satisfaire les exigences de redevabilité. Le plus souvent, il s'agit d'opérations de « screening ». Ce terme est traduisible par le mot « criblage » en français, et vise les différents acteurs impliqués dans un programme. Ces derniers peuvent être les membres de l'ONG ayant des responsabilités, des associations partenaires, et dans certains cas les bénéficiaires eux-mêmes. Sachant que malgré l'assouplissement des mesures de sanctions qu'on a décrit plus haut, des mesures de contrôle peuvent être malgré tout requises. Comme le note la chercheuse Beata Paragi, la résolution de 2022, elle consiste certes en une exemption humanitaire, sont autorisés et ne constituent pas une violation des mesures de gel des avoirs imposées par lui ou ses comités des sanctions »[1113]. Mais il est malgré tout exigé aux ONG qu'elles « efforts raisonnables pour que les avantages interdits par les sanctions que pourraient tirer des personnes ou entités désignées par lui ou l'un de ses comités, que ce soit à la suite d'une fourniture directe ou indirecte de l'aide ou d'un détournement, soient réduits au maximum, notamment en renforçant les stratégies et les processus de gestion des risques et de diligence raisonnable. »
1114

Par conséquent, les bailleurs peuvent exiger de la part des ONG de telles mesures. La demande de screening peut être explicite ou non dans le contrat du bailleur. Elle peut impliquer le fait que les bénéficiaires finaux soient exclus ou non de l'aide s'ils apparaissent sur une liste [1115]. Dans certains cas, il est nécessaire d'avoir l'autorisation d'un officier de l'USAID pour traiter avec tel ou tel bénéficiaire appartenant à un groupe sanctionné[1116].

Sachant que les opérations de « screening » consistent simplement au fait d'examiner quelqu'un pour détecter une faute ou une maladie. Dans le cadre professionnel, cela peut prendre la forme d'un « background check », une pratique assez courante dans le milieu de l'entreprise américaine, moins répandue en Europe et en France. Il existe plusieurs façons de procéder, mais le plus souvent ces opérations sont réalisées grâce à des logiciels de screening de listes de personnes ciblées par des sanctions. Il s'agit par exemple de logiciel comme Finscan, LexisNexis WorldCompliance, CSI WatchDOG Elite, Bridger Insight Online, and Visual Compliance System (VOICE 2021, 13), ainsi que le controversé Worldcheck [1117].Il existe deux

---

[1113] Résolution 2664 (2022), Nations Unies, Conseil de sécurité https://documents.un.org/doc/undoc/gen/n22/736/75/pdf/n2273675.pdf?token=c5p3YijIoYxDTYRFrj&fe=true

[1114] Ibid.

[1115] « Requirements to screen and/or exclude final beneficiaries from funded programs can either be implied or express. Most frequently, they are implicit in provisions that prohibit recipients from making available funds or assets to entities, individuals or groups of individuals designated under counterterrorism measures or sanctions. If these provisions do not expressly indicate that this requirement does not cover final beneficiaries, there is a real risk that the expression could be interpreted by the donor as including them. At other times, clauses leave no room for doubt that final beneficiaries must also be excluded from funded activities, as they are expressly mentioned" GILLARD, Emanuela-Chiara, GOSWAMI, Sangeeta, VAN DEVENTER, Fulco, "Screening of final beneficiaries - a red line in humanitarian operations. An emerging concern in development work", *International Review of the Red Cross*, n° 916-917, February 2022 https://international-review.icrc.org/articles/screening-of-final-beneficiaries-a-red-line-in-humanitarian-operations-916

[1116] ANYADIKE, OBI, "Aid workers question USAID counter-terror clause in Nigeria", *The New Humanitarian*, 05/11/2019,https://www.thenewhumanitarian.org/news-feature/2019/11/05/USAID-counter-terror-Nigeria-Boko-Haram

[1117] FAVAREL-GARRIGUES Gilles, GODEFROY Thierry, LASCOUMES Pierre, « 6. Le développement des instruments informatiques », dans : FAVAREL-GARIGUES, Gilles, THIERRY, GODEFROY, LASCOUMES, Pierre (dir), *Les sentinelles de l'argent sale. Les banques aux prises avec l'antiblanchiment*, Paris: La Découverte, « Cahiers libres », 2009, p. 141-157

sortes de criblage, soit c'est l'ONG qui mène ce type d'opération elle-même, soit l'ONG transmet au bailleur des informations sur son personnel, ses partenaires et parfois ses bénéficiaires, et c'est ce dernier qui se charge du criblage. Dans ce dernier cas, on parle en anglais de « vetting »[1118]. Seulement une minorité de bailleurs conditionnent leur financement à des opérations de ce type, et ce dans certains contextes sensibles. L'USAID impose par exemple des opérations de « vetting » en Afghanistan, en Iraq, au Liban, au Pakistan, en Syrie, au Yémen et à Gaza [1119].

Les ONG appliquent elles-mêmes des opérations de screening des personnels, et pour certaines, cela est une opération routinière, comme nous le raconte une enquêtée: « *Est-ce que les opérations de screening posent problème en matière de vie privée ? Si c'est le cas, j'en ai pas entendu parler. C'est une tâche obligatoire, si tu veux travailler avec nous, dans n'importe quel pays, c'est obligatoire, tu dois faire ce process.* »[1120] Mais parmi les ONG, il existe un consensus sur le fait de refuser de le faire sur des bénéficiaires : « *on est opposé à le faire, on ne crible pas nos bénéficiaires, on a eu un long processus interne, une analyse d'impact sur le criblage des personnels, des prestataires et des bénéficiaires, et on s'oppose à cribler les bénéficiaires. Mais il y a une pression dans ce sens-là, une pression au criblage des bénéficiaires.* » [1121] Si les opérations de screening ne font pas débat, le manque de transparence de ces outils participerait pour Beata Paragi de leur acceptation. Mais cribler les bénéficiaires consiste pour les ONG en une « ligne rouge » pour reprendre cette expression. Ce type d'opération pourrait en effet conduire à l'exclusion d'une personne de l'assistance humanitaire, en dépit de ses besoins, établis en fonction des critères d'éligibilité propre à l'ONG. Pour les humanitaires, cela contreviendrait au principe d'impartialité de l'aide, au principe de non-discrimination, et irait à l'encontre du DIH[1122].

En outre, les opérations de « vetting » sont perçues comme plus problématiques qu'un simple « screening ». La chercheuse Emanuela Chiara Gillard reconnait qu'il s'agit d'une opération acceptable pour s'assurer que quelqu'un n'est pas ciblé par une liste terroriste, mais les opérations de « vetting » soulèvent « des préoccupations supplémentaires en matière de contrôle, notamment pour ce qui est de la protection des données et de la vie privée en ce qui concerne les informations personnelles fournies au donateur. Le filtrage peut également nuire à la perception de l'indépendance des acteurs humanitaires qui fournissent ces informations par rapport à l'État donateur qui les demande. Si le donateur est impliqué dans

SOARES, Rita, ANWAR, Tasniem, WESSELING, Mara, « New tech, perpetual chalenge, how emerging technologies for financial compliance are impacting the nonprofit sector », ECNL, European Center for Not For Profit Law, june 2022 https://ecnl.org/sites/default/files/2022-09/ECNL%20FINTECH%20Report.pdf

[1118] PARAGI, Beata, Screening by international aid organizations operating in the Global South, mitigating risks of generosity, Springer, 2024, 200 p.

[1119] MACKINTOSH, Kate, DUPLAT, Patrick, "Study of the Impact of Donor Counter-Terrorism Measures on Principled Humanitarian Action"July 2013 https://www.nrc.no/globalassets/pdf/reports/study-of-the-impact-of-donor-counterterrorism-measures-on-principled-humanitarian-action.pdf

O LEARY, Emma, "Politics and principles: The impact of counterterrorism measures and sanctions on principled humanitarian action", *IRRC* n° 916 917 February 2022

[1120] Entretien n°86, ONG 22, DPO, 27/10/2022

[1121] Entretien n°88, ONG24, DPO, 15/11/2022

[1122] GILLARD, Emanuela-Chira, « IHL and the humanitarian impact of counterterrorism measures and sanctions", *Chathham House*, 21/09/2021 https://www.chathamhouse.org/2021/09/ihl-and-humanitarian-impact-counterterrorism-measures-and-sanctions

un conflit armé, la fourniture d'informations peut également affecter la perception de la neutralité des acteurs humanitaires. » [1123]

Mais les pratiques de screening comme de vetting reposent comme le surligne Beata Paragi sur l'utilisation massive de données. La chercheuse s'inquiète du manque de transparence et d'équité des traitements liés à ces opérations de la part des ONG[1124], qui contrevient aux exigences du RGPD en matière d'information aux personnes concernées, que ce soient les bénéficiaires ou les partenaires locaux des ONG internationales. Les opérations de criblage participeraient à la sécuritisation de l'aide et s'inscrivent dans différentes pratiques de surveillance menées par les ONG et techniques de gouvernance des populations ( comme l'usage de la biométrie, à des finalités de redevabilité et d'identification des bénéficiaires). Le criblage soulève donc un certain nombre d'enjeux en matière de vie privée. Toujours est-il qu'on verra que les ONG rechignent majoritairement à se plier aux exigences criblage des bénéficiaires, dénoncé en tant que violation des principes humanitaires et du DIH.

### § 1 — l'USAID

On a d'abord choisi de travailler sur le cas de l'USAID. Le bailleur américain est en effet connu pour ses exigences en matière de contrôle de financement du terrorisme. Il a progressivement mis en place un système de criblage des bénéficiaires finaux[1125]. On a vu que le régime américain des sanctions a été progressivement aménagé afin de garantir l'allocation de l'aide. Mais le système de « vetting » n'a été amendé qu'à la marge. Ceci est d'autant plus problématique au regard du poids de l'USAID dans l'aide humanitaire internationale et du large spectre d'application du programme de criblage. À la date de janvier 2020, l'USAID requiert des opérations de « vetting » dans les pays suivants : le Pakistan et l'Afghanistan ; l'Iraq et le Yémen ; le Liban ; la Syrie ; et Gaza. Ajoutons que « l'USAID se réserve le droit d'étendre son programme de vérification des partenaires, à tout moment, à d'autres pays et territoires dans lesquels elle fournit ou gère de l'aide. »[1126]

---

[1123]« raises additional concerns to screening, including in terms of data protection and privacy in relation to the personal information provided to the donor. Vetting can also undermine perceptions of the independence of humanitarian actors providing such information from the state donors requiring it. If the donor is a party to an armed conflict, the provision of information can also affect the perceived neutrality of humanitarian actors. » GILLARD, Emanuela-Chiara, GOSWAMI, Sangeeta, VAN DEVENTER, Fulco, "Screening of final beneficiaries - a red line in humanitarian operations. An emerging concern in development work", *International Review of the Red Cross*, n° 916-917, February 2022 https://international-review.icrc.org/articles/screening-of-final-beneficiaries-a-red-line-in-humanitarian-operations-916

[1124] PARAGI, Beata, "Opacity or transparency? Screening by NGOs in the context of aid work", Norwegian centre for humanitarian studies, 08/03/2023https://www.humanitarianstudies.no/resource/opacity-or-transparency-screening-by-ngos-in-the-context-of-aid-work/

PARAGI, Beata, " The ambiguous politics of screening, NGO as actors in the counterterrorism game?, Humanitarian studies, PRIO, 08/02/2022 https://www.humanitarianstudies.no/the-ambiguous-politics-of-screening/

PARAGI, Beata, the art of screening : reasonable efforts and measures at the nexus of aid work and counterterrorism, *Surveillance&Society*,2024, 22(2) : p.138-159

PARAGI, Beata, Screening by international aid organizations operating in the Global South, mitigating risks of generosity, Springer, 2024, 200 p.

[1125] "Counterterrorism and humanitarian engagement project, partner vetting in humanitarian assistance : an overview of pilot USAID and state department programs", Research and policy paper, november 2013
https://archive.blogs.harvard.edu/cheproject/files/2013/10/CHE-Project-Partner-Vetting-in-Humanitarian-Assistance-November-2013.pdf

[1126] « USAID reserves the right to expand our partner vetting program, at any time, to other countries and territories in which we deliver or manage assistance. »

L'USAID a commencé en 2001 à mener des opérations de « vetting » à Gaza, et cette procédure a été formalisée en 2006, à la suite d'un rapport critique du « government accountability office » (GAO)[1127]. Ces opérations s'appuient sur le Mission Order 21 de l'USAID[1128]. Et depuis 2011, l'organisation mène aussi officiellement des opérations de « vetting » en Afghanistan[1129]. L'agence a commencé à mettre en place ce type de programme après qu'un rapport des services de renseignement lui aurait indiqué qu'une partie de l'aide était détournée par des groupes d'insurgés dans certaines provinces afghanes[1130]. Mais des opérations de contrôle existerait a priori déjà depuis 2006[1131].

Pour l'ensemble de ses programmes, l'USAID commence par inclure dès mars 2002 une première clause contractuelle. Cette dernière rappelle aux ONG qu'il est interdit — selon l'Executive Order 13224 — de mener des transactions avec des organisations terroristes, et plus précisément avec les entités ciblées par l'Office of Foreign Assets Control (OFAC) du département du Trésor[1132]. En décembre 2002, l'USAID requiert que les ONG certifient qu'elles ne soutiennent pas matériellement des terroristes. Et en novembre 2005 a été publié un bulletin rappelant aux officiers de l'USAID le fait qu'ils sont responsables de la vérification des listes du département du trésor durant l'attribution des bourses. Parallèlement, en novembre 2002, le département du Trésor américain promulgue des lignes directrices sur le financement du terrorisme. Ces lignes directrices sont très critiquées par les ONG et il s'en suit une série d'échanges et de workshops sur ce sujet avec le département du Trésor[1133]. En décembre 2005, ce dernier édite de nouvelles guidelines, qui ne satisfont pas les ONG. Ces

---

[1127] Le "Government Accountability Office" est l'organisme d'évaluation du Congrès des États-Unis chargé du contrôle des comptes publics du budget fédéral des États-Unis.
https://www.gao.gov/products/gao-06-1062r foreign Assistance: Recent Improvements Made, but USAID Should Do More to Help Ensure Aid Is Not Provided for Terrorist Activities in West Bank and Gaza

[1128] USAID WEST BANK/ GAZA, Amended and restated Mission order n°21
https://www.usaid.gov/sites/default/files/2022-05/USAID_WBG_Mission_Order_21_2007.pdf
Counterterrorism and Humanitarian Engagement Project, "Partner Vetting in Humanitarian Assistance: An Overview of Pilot USAID and State Department Programs", Research and Policy Paper, November 2013https://archive.blogs.harvard.edu/cheproject/files/2013/10/CHE-Project-Partner-Vetting-in-Humanitarian-Assistance-November-2013.pdf
Counterterrorism and Humanitarian Engagement Project, "Partner Vetting in Humanitarian Assistance: An Overview of Pilot USAID and State Department Programs", Research and Policy Paper, November 2013https://archive.blogs.harvard.edu/cheproject/files/2013/10/CHE-Project-Partner-Vetting-in-Humanitarian-Assistance-November-2013.pdf

[1129] "Vetting in Afghanistan: Issues with the Defense Department, State and USAID", *Charity and Security*, 14/11/2013https://charityandsecurity.org/archive/vetting_in_afghanistan/

[1130] GAO, Report number GAO-11-355 "Afghanistan : U.S. Efforts to Vet Non-U.S. Vendors Need Improvement » , 2011 https://www.gao.gov/assets/a319435.html

[1131] "Special inspector General for Afghanistan Reconstruction, Contracting with the Enemy: State and USAID Need Stronger Authority to Terminate Contracts When Enemy Affiliations Are Identified", SIGAR Audit 13-14, July 2013https://www.sigar.mil/pdf/audits/SIGAR%20Audit%2013-14.pdf
https://www.gao.gov/assets/gao-11-886.pd
USAID mission order sets vetting process for Afghanistan Grant and contracts", *Charity and Security*, 14/11/2013 https://charityandsecurity.org/archive/usaid-mission-order-sets-vetting-process-for-afghanistan-grants-and-contracts/
Mission order, 201.06, USAID
https://imlive.s3.amazonaws.com/Federal%20Government/ID267114757590318456420793535821585579160/Attachment_J.1_-_Mission_Order_201.06_-Vetting_2015-06-07.pdf
SCHAHILL, Jeremy, DEVEREAUX, Ryan, "Blacklisted", *The Intercept*, 23/07/2014 https://theintercept.com/2014/07/23/blacklisted/

[1132] Il était précisé que : « The Recipient, to the best of its current knowledge, did not provide, within the previous ten years, and will take all reasonable steps to ensure that it does not and will not knowingly provide, material support or resources to any individual or entity that commits, attempts to commit, advocates, facilitates, or participates in terrorist acts, or has committed, attempted to commit, facilitated, or participated in terrorist acts »

[1133] Panel of experts explain how the work of charities counters terror", *Charity and Security*, 23/03/2009 https://charityandsecurity.org/news/March_panel_discussion_Friend_Not_Foe/
"The role of charities and NGO's in the financing of terrorist activities", Senate Hearing 107-988, 01/08/2002https://www.govinfo.gov/content/pkg/CHRG-107shrg89957/html/CHRG-107shrg89957.htm

dernières se regroupent en une coalition d'acteurs [1134] comprenant des organisations comme le « Charity and security network[1135] », le collectif « Interaction [1136]» ou encore l'organisation de défense des droits de l'homme, l'Union américaine pour les libertés civiles (« American Civil liberties Union », ACLU).

Mais en 2006, le Government accountability office (GAO) publie un rapport critique sur le financement d'ONG opérant à Gaza et en Cisjordanie[1137]. Le rapport déplore l'absence de mise en place systématique du dispositif et de ce qui lui semble être un manque de collecte systématique d'informations identifiantes sur les individus. L'UNRWA aurait en outre mené des opérations screnning sur son personnel, ses partenaires et bénéficiaires, mais en utilisant des listes du Conseil de Sécurité de l'ONU… qui n'avaient alors pas désigné le Hamas ou le Hezbollah comme des organisations terroristes[1138]. En réponse à ce rapport, en juillet 2007, l'USAID a annoncé qu'il mettrait en place un nouveau système de criblage, le Partner Vetting System (PVS)[1139]. S'en suit une mobilisation d'associations contre le PVS. Ces dernières critiquaient plusieurs points : le manque de transparence du PVS, rendant difficile la possibilité de contester des faux positifs et négatifs, des problèmes de vie privée, et plus généralement ce qui constitue à leurs yeux un manque de nécessité du programme[1140]. À la suite d'un long processus de négociation, le 26 juin 2015, l'USAID publie un règlement final étendant son programme de PVS[1141]. Ce dernier est d'abord mis en place au Guatemala, au Kenya, au Liban, aux Philippines et en Ukraine. Le motif du choix de ces pays n'est pas explicité dans les documents dont nous disposons. On notera que l'ensemble des activités de l'USAID ne sont pas soumises aux opérations de « vetting ». Toutefois, précisons que l'agence est légalement habilitée à procéder à un contrôle en dehors du programme pilote lorsqu'un programme

---

[1134] "U.s. department of the treasury anti-terrorist financing guidelines : voluntary best practices for U.S.-based charities",2003https://home.treasury.gov/system/files/136/archive-documents/tocc.pdf

[1135] https://charityandsecurity.org/ il s'agit d'une ONG parapluie regroupant des acteurs spécialisés dans le domaine des répercussions du contreterrorisme dans le secteur associatif.

[1136] https://www.interaction.org/ Il s'agit d'une des principale coalition d'ONG charitables américaines.

[1137]"Foreign Assistance: Recent Improvements Made, but USAID Should Do More to Help Ensure Aid Is Not Provided for Terrorist Activities in West Bank and Gaza", United States Government accountability office, 29/09/2006 https://www.gao.gov/assets/gao-06-1062r.pdf

[1138] Ibid, https://www.gao.gov/assets/gao-06-1062r.pdf

En 2023, un rapport du GAO conclut dans le respect des mesures de vetting par l'USAID à Gaza : « our analysis found that USAID generally complied with Mission Order 21 and that USAID took actions to ensure that awardees corrected the instances of noncompliance that external auditors found in the compliance reviews. As part of its effort to prevent inadvertently funding entities or individuals associated with terrorism, USAID is responsible for ensuring that prime awardees follow Mission Order 21 anti-terrorism policies and procedures, and that prime awardees ensure that their subawards comply with Mission Order 21 requirement », « notre analyse a révélé que l'USAID s'est généralement conformée à l'ordre de mission 21 et que l'USAID a pris des mesures pour s'assurer que les attributaires corrigent les les cas de non-conformité relevés par les auditeurs externes lors des dans le cadre des contrôles de conformité. Dans le cadre de ses efforts pour éviter de financer par inadvertance des entités ou des individus associés au terrorisme, l'USAID est chargée de s'assurer que les attributaires principaux respectent les politiques et procédures antiterroristes de l'ordre de mission 21 et des procédures antiterroristes, et que les bénéficiaires principaux veillent à ce que leurs les sous-traitants se conforment aux exigences de l'ordre de mission 21. » United States Government accountability office, Report to Congressional Committees, West Bank and Gaza aid, USAID generally ensured compliance with anti-terrorism policies and addressed instances of noncompliance", December 2023 https://www.gao.gov/assets/870/864341.pdf

[1139] Federal Register / Vol. 72, No. 136 / Tuesday, July 17, 2007 / Notices, 39043https://www.usaid.gov/sites/default/files/sor_27.pdf

[1140] PINCUS,Walter, "Foreign Aid Groups Face terror Screen", *Washington Post*, 23/08/2007https://www.washingtonpost.com/wp-dyn/content/article/2007/08/22/AR2007082202847.html

GUINANE, Kay, "US Counterterrorism developments impacting charities", *The international journal of Not-for-Profit-Law*, December 2007https://archive.globalpolicy.org/ngos/state/2007/12terrorngo.htm

[1141] Federal Register 36693 Vol. 80, No. 123, Friday, June 26, 2015 https://www.govinfo.gov/content/pkg/FR-2015-06-26/pdf/2015-15017.pdf

Federal Register / Vol. 78, No. 168 / Thursday, August 29, 2013 / Proposed Rules,53375 https://www.govinfo.gov/content/pkg/FR-2013-08-29/pdf/2013-20846.pdf

Partner Vetting System Pilot Program, USAID, US Department of State, 2011https://charityandsecurity.org/sites/default/files/PVS%20PUBLIC%20Mtg%20STATUS%20REPORT%2009082011%20FINAL.pdf

représente un certain niveau de risques[1142] et qu'en fonction de la politique de l'USAID l'organisation peut déterminer qu'une bourse particulière doit faire l'objet d'un examen approfondi « dans l'intérêt de la sécurité nationale. » [1143] Cette évaluation de risque comprend un certain nombre de facteurs contextuels : la nature du programme, la localisation géographique du programme, le montant de la bourse. En revanche, l'USAID spécifie qu'en cas d'urgence humanitaire, il n'est pas nécessaire de mener des opérations de VPS. Cela dit, l'USAID ne précise pas dans ses contrats ou dans les documents du règlement final quels sont les critères constitutifs d'une situation d'urgence. Et surtout les règles de 2015 indiquent que l'USAID se réserve la possibilité de mener des opérations de VPS a posteriori, une fois la situation de crise stabilisée. Enfin, il est tout bonnement noté que dans certains cas, la décision de procéder à une opération de « vetting » n'est pas négociable.

Comment se passe une opération de criblage ? Le processus de VPS est mené par un membre dédié de l'USAID. Cette opération de « vetting » s'applique à tous les « individus clefs » d'une organisation, à savoir des membres ayant des responsabilités au sein de l'ONG, tels que président, vice-président, comptable, etc. Des opérations de VPS ne sont pas requises pour les bénéficiaires finaux de programmes de cash, ou d'assistance en nature, comme de la nourriture, de l'eau, des soins médicaux, etc. Cependant, des opérations de VPS sont requises dans le cas où ces opérations excèderaient 25 000 dollars. Et des opérations de VPS sont exigées pour un hôpital recevant des médicaments ou des fournitures médicales. En outre, il est toujours précisé que l'USAID se réserve la possibilité de mener des opérations de VPS si l'organisation a des raisons de penser que le bénéficiaire peut être ciblé par des sanctions[1144]. Enfin, l'USAID se réserve aussi le droit de mener des opérations de « vetting » au sujet de personnes de nationalité américaine quand le bailleur soupçonne qu'elles ont soutenu ou bien se sont engagées dans une organisation terroriste[1145]. Mais il faut garder à l'esprit que l'USAID ne requiert pas d'opérations de vetting aux organisations internationales, et notamment aux agences onusiennes, en raison de leurs privilèges et immunités. Ces dernières ont généralement leurs propres mécanismes internes de contrôle des financements.

Le tableau suivant publié par le GAO synthétise les différents cas de figure pour les opérations de « vetting » à Gaza.

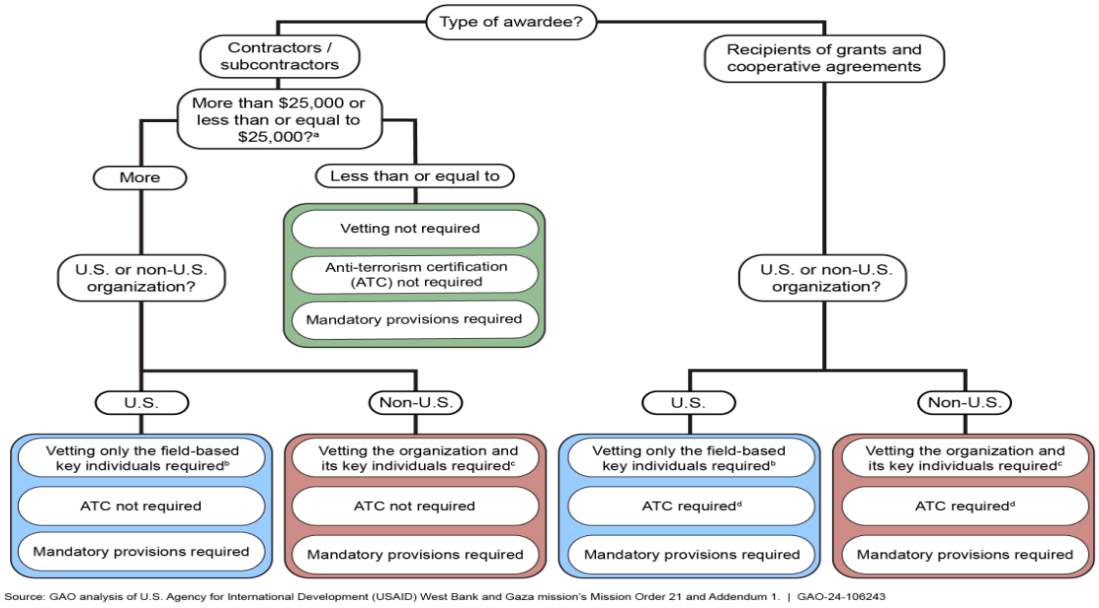
[1142] "The agency has the legal authority to conduct vetting outside the pilot program "where a risk assessment indicates that vetting is an appropriate higher level safeguard".

[1143] "USAID policy that USAID may determine that a particular award is subject to vetting in the interest of national security."

[1144]"Other situations: Even if vetting would not otherwise be required under these rules, vetting will be conducted whenever USAID has reason to believe that the Awardee or Sub-awardee could be a Prohibited Party. USAID may also conduct vetting pursuant to any internal or external audits. "

[1145] Précisons que pour le cas de Gaza : « depuis 2007, les politiques de l'USAID exigent de la mission qu'elle veille au respect des contrôles antiterroristes pour les bénéficiaires principaux et les sous-bénéficiaires, conformément à l'ordre de mission 21. Les politiques de la mission en Cisjordanie et à Gaza sont restées largement cohérentes depuis 2007, date de la dernière modification de l'ordre de mission 21. Cependant, en 2017, la mission a ajouté l'addendum 1, qui est entré en vigueur en 2021 lorsque le programme a repris. Cet addendum a élargi le contrôle aux personnes clés des organisations américaines basées sur le terrain, ce qui n'était pas exigé auparavant. » »Since 2007, USAID policies have required the mission to ensure compliance with the anti-terrorism controls for prime awardees and subawardees as established in Mission Order 21. The West Bank and Gaza mission's policies have largely remained consistent since 2007, when it last amended Mission Order 21. However, in 2017, the mission added Addendum 1, which went into effect in 2021 when the program resumed. This addendum expanded vetting to include field-based key individuals of U.S. organizations, which was not previously require." https://www.gao.gov/assets/870/864341.pdf

**Figure 2: USAID West Bank and Gaza Mission Order 21 and Addendum 1 Requirements by Awardee and Subawardee Type**




Source: GAO analysis of U.S. Agency for International Development (USAID) West Bank and Gaza mission's Mission Order 21 and Addendum 1. | GAO-24-106243

#### OPERATIONS DE CRIBLAGE DES BENEFIAIRES EXIGEES PAR L'USAID POUR DES ONG OPERANT A GAZA ET EN CISJORDANIE[1146]

Les données requises sont les suivantes : nom, adresse, date et lieu de naissance, citoyenneté. Mais des informations supplémentaires peuvent être demandées, par exemple pour des personnes ne disposant pas de moyens d'identification usuels comme des passeports ou des cartes d'identité[1147]. L'USAID maintient que le PVS « n'a pas vocation à être invasif, mais à compléter les mécanismes de diligence raisonnable existants. »[1148] Il est assuré que si un partenaire se trouve faire partie d'une liste de sanction, il recevra une notification. Précisons toutefois que « l'USAID déterminera quelles informations peuvent être divulguées conformément à la loi et aux décrets applicables, et avec l'accord des agences concernées. »[1149] S'il apparait que le match est valide, l'ONG ne peut recevoir de fonds. L'USAID doit motiver son refus, en donnant « avec un niveau de détail raisonnable compte tenu de la nature, de la source et de la sensibilité de l'information. Dans les sept jours suivant la réception d'une demande de réexamen, l'USAID déterminera si les informations supplémentaires fournies par le demandeur justifient une révision de la décision. »[1150] Et l'USAID garantit qu'une ONG dont les fonds ont été refusés n'est pas « blacklistée » et qu'elle peut à l'avenir postuler à nouveau pour des financements. Cela dit, l'USAID n'assure pas textuellement le fait qu'elle ne partage pas des données de l'ONG avec d'autres organisations.

Malgré toutes ces précisions, les ONG de la coalition Charity&Security contestent le dispositif. Tout d'abord, il n'est pas toujours simple de déterminer pour une ONG ce que signifie le fait

[1146] « WEST BANK AND GAZA AID USAID Generally Ensured Compliance with Anti-terrorism Policies and Addressed Instances of Noncompliance », GAO, December 2023 https://www.gao.gov/assets/870/864341.pdf

[1147] Partner Vetting System (PVS) Privacy Impact Assessment (PIA), USAID, 17/01/2017https://www.usaid.gov/sites/default/files/2022-08/Partner_Vetting_System_PVS_PIA_Summary_January_17_2017.pdf

[1148] "PVS is not intended to be invasive, but instead complements existing due diligence mechanisms"ibid

[1149] 'USAID will determine what information may be released consistent with applicable law and Executive Orders, and with the concurrence of relevant agencies"ibid

[1150] "with a reasonable amount of detail given the nature, source and sensitivity of the information. Within seven days of receiving a request for reconsideration, USAID will determine whether the applicant's additional information merits a revised decision."ibid

de soutenir un individu « associé » à un groupe terroriste. Il est certes indiqué que « l'USAID définit les individus ou les entités ayant des « affiliations » ou des « liens » avec le terrorisme comme « des individus connus ou soupçonnés d'être ou d'avoir été engagés dans un comportement constituant, préparant, aidant ou lié au terrorisme. » [1151] Ces indications semblent vagues pour les ONG. Et on peut lire dans un article de 2019 publié par la revue The New Humanitarian, que : « L'USAID n'a pas fourni de définitions ou d'indications sur ce que signifie avoir été "anciennement affilié" à un groupe désigné. Toutefois, il s'agira probablement d'un groupe plus large que celui des personnes listées, de sorte que des personnes qui ne sont même pas listées pourraient potentiellement être exclues des programmes humanitaires. L'USAID n'a pas non plus fourni d'indications sur ce qui constitue une "connaissance affirmative" de l'ancienne affiliation d'une personne. » [1152] Cela est d'autant plus inquiétant pour les ONG qu'en pratique l'USAID ne leur ferait que peu de retours d'information : leur serait communiqué le simple fait que le financement a été refusé, sans préciser quel individu du programme est « blacklisté », d'où peu de possibilités de contestation de la décision [1153]. Le Congrès a pourtant rappelé que « toutes les personnes et organisations faisant l'objet d'un contrôle doivent être pleinement informées de la manière dont les informations seront stockées et utilisées par le gouvernement américain, y compris de la manière dont les informations relatives à une "correspondance positive" seront traitées et de la manière de faire appel d'une telle correspondance. »[1154]

En tout cas, il est tout à fait clair que les données PVS peuvent être partagées avec le Terrorist screening center (TSC) du FBI en cas de « match positif » : « Les informations personnelles conservées par les agents de "vetting" ne peuvent être partagées avec le Centre de dépistage du terrorisme (TSC) du FBI que lorsqu'il existe un « match positif » entre une personne figurant dans la base de données du PVS et la base de données du TSC. L'USAID et le FBI gèrent cette relation de partage de données dans le cadre d'un protocole d'accord. »[1155] Précisons qu'en théorie, le FBI n'a pas un accès direct aux bases de données, c'est une personne chargée des opérations de VPS qui lui transmet l'information. En outre, la base de données du FBI est la Terrorist Screening Database. Il s'agit d'une liste qui n'est pas publique. Mais elle est connue pour être en croissance exponentielle et pour comprendre des données d'individus qui ne sont pas nécessairement accusés de façon directe de terrorisme : « les noms figurant sur la liste sont confidentiels et ne se limitent pas aux personnes et entités désignées comme

---

[1151]"USAID defines individuals or entities with ''affiliations'' or ''linkages'' to terrorism as ''individuals known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism.''Federal Register, 36693, Vol. 80, No. 123 Friday, June 26, 2015, https://www.govinfo.gov/content/pkg/FR-2015-06-26/pdf/2015-15017.pdf

[1152]« USAID has not provided definitions or guidance of what amounts to having been "formerly affiliated" with a designated group. However, this is likely to be a larger group than those who are designated, so people who are not even designated could potentially be excluded from humanitarian programs. USAID has also not provided guidance on what constitutes "affirmative knowledge" of a person's former affiliation. "ANYADICKE, Obi, "Aid Workers Question USAID Counter-terror Clause in Nigeria", *The New Humanitarian*, 5/11/2019, https://www.thenewhumanitarian.org/news-feature/

[1153] "Screening of final beneficiaries of humanitarian programmes" Diakoniaa international humanitarian law centre, August 2021 https://apidiakoniase.cdn.triggerfish.cloud/uploads/sites/2/2021/08/Diakonia_FactSheets_Screening.pdf

"This leaves the door open for the government to reject an individual based on secret information, while having no obligation to give reasoning, and offering little opportunity for the individual to contest the determination.Panel of Experts Explain How the Work of Charities Counters Terror", *Charity and Security network*, 23/03/2009 https://charityandsecurity.org/news/March_panel_discussion_Friend_Not_Foe/

[1154]« All individuals and organizations being vetted should be provided with full disclosure of how information will be stored and used by the U.S. Government, including how information regarding a « positive match "will be handled and how to appeal such a match. » The Senate Committee on Appropriations report accompanying the Fiscal Year 2014 State and Foreign Operations Appropriations Bill from July 2013

[1155] « VS-maintained PII can be shared with the FBI Terrorist Screening Center (TSC) only when there is a positive match between an individual in the PVS database and the TSC database. USAID and FBI manage this data sharing relationship through an MOU. Authorities for the MOU are provided therein. » ibid

terroristes par le gouvernement américain, qui sont déjà identifiées sur des listes rendues publiques par les départements du Trésor et d'État. »[1156] La « Watchlist » est potentiellement partagée avec un grand nombre d'acteurs, et l'organisation de défense des droits de l'homme, l'ACLU n'hésite pas à avancer que peuvent y avoir accès rien moins que « des milliers d'agents chargés de l'application de la loi à tous les niveaux de gouvernement et avec 22 gouvernements étrangers. Dans certains cas, les informations sont partagées avec des personnes du secteur privé. »[1157] Au-delà de cette large estimation, l'American civil liberties union (ACLU) estime également qu'il n'y a pas de garantie sur la façon dont le FBI peut stocker les données personnelles du programme de VPS[1158]. Et il est évidemment difficile de déterminer quel usage en fait le Terrosrism Screening Center du FBI. Le chercheur Ben Hayes rapporte cependant que : « Selon des documents divulgués par Edward Snowden et publiés en juillet 2014 par The Intercept, les données fournies aux agences de renseignement américaines lors de l'examen des partenaires par l'USAID ont été utilisées pour développer la base de données Terrorist Identities Datamart Environment (TIDE)[1159], qui contient désormais des dossiers sur plus d'un million de personnes, dont 95 % sont des étrangers (Boon-Kuo et al. 2015, 42). Ce type de cadre antiterroriste ne se contente pas de créer une charge administrative pour les ONG ; il les fait participer activement aux processus de collecte de renseignements. »[1160]

L'USAID se défend des critiques à l'égard du PVS le réduisant à des opérations de « renseignement ». Elle argue qu'elle n'est pas juridiquement habilitée à le faire : « Le PVS n'est pas un programme américain de collecte de renseignements. En outre, l'USAID n'est pas une agence relevant du titre 50 et n'est pas autorisée par la loi à collecter des informations de renseignement. »[1161] Mais, au-delà de la réalité juridique, le PVS impacte la façon dont les ONG sont perçues. Et il se trouve qu'il peut arriver que les humanitaires soient soupçonnés par les différentes parties prenantes d'un conflit de s'adonner à des « activités

---

[1156]« the names on the list are secret and are not limited to individuals and entities designated as terrorists by the U.S. government, which are already identified on lists that are made public by the Departments of Treasury and State. » ibid

[1157] « thousands of law enforcement officers at every level of government and with 22 foreign governments. In some cases the information is shared with private-sector individuals. »

[1158] lettre de l'ACLU du 30 septembre 2013 sur la politique de vetting de l'USAID, Laura W, Murphy, Dena Shre, Hina, Shamsihttps://www.charityandsecurity.org/sites/default/files/ACLU%20Comments%20re%20USAID%20PVS%20-%20RIN%200412--AA71.pdf

[1159] Terrorist Identities Datamart Environment (TIDE) https://www.dni.gov/files/Tide_Fact_Sheet.pdf

[1160] « According to documents leaked by Edward Snowden and released in July 2014 by The Intercept, data supplied to US intelligence agencies during partner vetting by USAID has been used to expand the Terrorist Identities Datamart Environment (TIDE) database, which now holds records on more than one million people, 95 per cent of them foreigners (Boon-Kuo et al. 2015, 42). These kinds of counterterrorism frameworks do not merely create an administrative burden for NGOs; they actively enrol them in intelligence-gathering processes ». HAYES, Ben, "The impact of international counter-terrorism on civil society organisations, Understanding the role of the Financial Action task Force", Brot Fur die Welt, April 2017 https://www.brot-fuer-die-welt.de/fileadmin/mediapool/2_Downloads/Fachinformationen/Analyse/Analysis_68_The_impact_of_international_counterterrorism_on_CSOs.pdf

« La liste de sélection soumet les personnes à un examen approfondi et à des interrogatoires dans les aéroports et aux frontières. Le gouvernement a également créé plusieurs autres bases de données. La plus importante est le Terrorist Identities Datamart Environment (TIDE), qui rassemble des informations sur le terrorisme provenant de sources militaires et de renseignements sensibles du monde entier. Parce qu'elle contient des informations classifiées qui ne peuvent être largement diffusées, il existe une autre liste, la Terrorist Screening Database (TSDB), qui a été dépouillée des données classifiées de TIDE afin de pouvoir être partagée. Lorsque les responsables gouvernementaux parlent de "liste de surveillance", ils font généralement référence à la base de données TSDB. (TIDE est sous la responsabilité du National Counterterrorism Center ; la TSDB est gérée par le Terrorist Screening Center du FBI). »
SCHAHILL, Jeremy, DEVEREAUX, Ryan, "Blacklisted", *The Intercept*, 23/07/2014 https://theintercept.com/2014/07/23/blacklisted/

[1161] « PVS is not a U.S. intelligence collection program. Moreover, USAID is not a Title 50 Agency and is not authorized by law to collect intelligence information. » Le titre 50 du US Code, chapitre 36, sert de principal cadre légal à l'administration pour la collecte d'informations de renseignement extérieur aux USA.

d'espionnage »[1162]. Le programme du PVS renforcerait cette perception. Et en 2012, le Département d'État avait partiellement reconnu ce point : « L'État ne peut évidemment pas contrôler la perception qu'ont les autres parties des activités du gouvernement américain et doit reconnaître la possibilité d'une telle perception ; toutefois, les organisations dont les activités sont financées par le gouvernement américain sont déjà confrontées à de tels soupçons parmi les parties hostiles. »[1163]

De surcroit, l'USAID justifie un tel traitement de données en vertu de l'Executive order 13224 de 2001, relatif aux mesures de contreterrorisme. Mais le collectif d'ONG InterAction craint qu'il ne contrevienne aux lois européennes relatives à la défense de la vie privée, il n'a pu cependant obtenir de réponse d'USAID à ce sujet : « À ce jour, l'USAID n'a pas répondu aux préoccupations selon lesquelles le PVS pourrait violer les lois sur la protection de la vie privée et des données des États membres de l'Union européenne ou d'un pays pilote. Actuellement, l'USAID ne prévoit pas d'exempter les opérations de "vetting" dans ces circonstances. »[1164] Des échanges de données avec des ONG européennes peuvent cependant être courants au regard du poids du bailleur à l'international. En tout cas, des juristes de Harvard, le PVS viole le droit de la protection des données européen. Leur analyse date de 2013, soit avant l'entrée en vigueur du RGPD et de la directive Police/Justice[1165]. Et les juristes ont montré qu'il n'existait alors pas de base légale adéquate selon la Directive de 1995 couvrant les opérations de « vetting ». Par exemple, recourir à la base légale de l'intérêt légitime ne serait pas pertinent. Selon eux, il est surtout dans l'intérêt des ONG de ne pas être exposé à un danger physique, le fait d'être perçu comme des « agents de l'occident » n'est pas sans risques pour les travailleurs humanitaires. Ce point surpasse pour l'ONG l'intérêt qu'il peut exister à partager des données avec l'USAID. Cela pourrait être l'intérêt public ? Mais dans le cas d'une ONG européenne, il n'est pas pour les juristes dans l'intérêt national de l'Angleterre de partager des données avec un pays tiers, en l'occurrence les USA. Le traitement de données peut se faire dans le cadre d'une obligation légale, puisque ce dernier est dû à une obligation américaine. Or en cas de transfert de données hors USA, cela ne peut se faire que sous consentement, qu'au nom d'un intérêt public, d'un accord de transfert de données, qui doit contenir des garde-fous suffisamment solides, ce qui n'est pas le cas pour les auteurs.

[1162] A titre d'exemple, Michiel Hofman décrit ainsi la situation de MSF en Afghanistan : l'ONG est critiquée par l'armée américaine pour ses contacts avec les Talibans, ces derniers les considèrent comme étant potentiellement des espions en raison de leur interaction avec les GI. HOFMAN, Michiel, "Non-State Armed Groupes and Aid Organisations", in MAC GINTY, Roger, PETERSON H, Jenny, *the Routledge companion to humanitarian action*, New York: Routledge, 2015, p.324-337

[1163] « [State] cannot, of course, control the perceptions of other parties about U.S. government activities and must acknowledge the possibility of such a view; however, those organizations relying on U.S. government funding for their operations already face such suspicions among hostile parties. » The Senate Committee on Appropriations report accompanying the Fiscal Year 2014 State and Foreign Operations Appropriations Bill from July 2013

[1164] « To date, USAID has not addressed the concerns that PVS may violate either European Union member states' or a pilot country's privacy and data protection laws. Currently, USAID does not plan to exempt vetting under these circumstances. » The Assistant Administrator's reply confirmed this: "Your recollection of stated policy regarding … European Union privacy and data protection laws is correct."DARTER, Kimberly," Partner Vetting, Independant assessment : insufficient justification for a global rollout, Interaction", December 2016 https://www.interaction.org/wp-content/uploads/2020/02/Independent-Partner-Vetting-Assessment_FINAL.pdf

[1165]La directive « Police-Justice » établit des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces. https://www.cnil.fr/fr/directive-police-justice-de-quoi-parle-t

Conclusion, les juristes sont clairs, pour eux le PVS viole le cadre légal européen[1166]. Cela dit, on peut ajouter qu'en 2024, c'est plutôt au regard de la Directive Police/Justice qu'il faut se référer. Et dans ce cas, un traitement de données est licite en vertu du fait qu'il permette « l'exécution d'une mission d'intérêt général par une autorité compétente, fondée sur le droit de l'Union ou le droit d'un État membre, à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces. »[1167] Sachant que dans ce cas, encore une fois, les mesures d'intérêt général ne sont pas menées par une autorité compétente de droit européen, mais par l'USAID.

Malgré tout, les ONG ne contestent pas la nécessité de contrôler l'allocation des fonds. Et si le programme de « vetting » n'est pas justifié, c'est que les humanitaires mèneraient déjà des opérations de « vigilance raisonnable » fondées sur une connaissance directe du terrain. Des membres du « Security&Charity Network » font la remarque que : « Le système de vérification des partenaires, tel qu'il a été conçu par le département d'État et l'USAID, repose sur des hypothèses erronées quant à l'efficacité de la vérification. Les agences ont poursuivi une stratégie qui s'appuie sur des bases de données gouvernementales secrètes plutôt que sur l'expérience acquise sur le terrain et les relations personnelles développées au fil du temps. Cette stratégie ne tire pas profit de l'expérience et de l'expertise du secteur des ONG. »[1168] Des membres du « Security&Charity Network » rétorquent que « Le modèle de "vérification" du PVS suppose que les ordinateurs qui passent au crible de multiples bases de données sont supérieurs aux éléments humains essentiels de la diligence raisonnable : les relations personnelles, l'expérience sur le terrain et le contrôle financier approfondi. » [1169] Ces controverses illustrent l'opposition entre deux modalités de connaissance et de gestion du risque terroriste. Mais du point de vue juridique, cela n'est pas sans conséquence en matière de protection des données. Selon le RGPD et la Directive Police/Justice, un traitement de données est légitime à partir du moment où il est proportionnel, et qu'il n'existe pas d'autres moyens moins intrusifs d'arriver aux mêmes fins. L'USAID rétorque cependant qu'il s'agit d'une précaution supplémentaire, mais surtout que « les partenaires de mise en œuvre de l'USAID n'ont pas accès à ces bases de données non publiques et ne peuvent donc pas se prévaloir du même corpus d'informations que l'USAID lorsqu'elle procède à des vérifications en Afghanistan, en Cisjordanie/Gaza et ailleurs. Pour protéger les ressources du contribuable américain contre le risque de détournement, l'importance de l'accès aux informations des

[1166] COHEN, Neal, HASTY, Robert, WINTON, Ashley, "Allocations of the USAID partner vetting system and state department risk analysis and management system under european union and united kingdom data protection and privacy law", counterterrorism and humanitarian engagement project, research and policy paper, march 2014
https://archive.blogs.harvard.edu/cheproject/files/2013/10/CHE-Project-US-Partner-Vetting-under-EU-and-UK-Data-Protection-and-Privacy-Law.pdf

[1167] DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données.

[1168] « The Partner Vetting System, as conceived and designed by the Department of State USAID, is built on flawed assumptions about how effective vetting is conducted. The agencies have pursued a strategy that relies on secret government databases rather than on-the-ground experience and personal relationships developed over time. It fails to take advantage of the experience and expertise of the NGO sector. »USAID's Partner Vetting System, *Charity and security network*, 16/02/2016 https://charityandsecurity.org/issue-briefs/pvs_issue_brief/

[1169] "Comments of Nonprofit Organizations on Proposed Partner Vetting in USAID Acquisitions", *Charity and security network*, 25/08/2009 https://charityandsecurity.org/partner-vetting-system/comments_nonprofit_proposed_partner_vetting_usaid_acquisitions_pvs/
The PVS model of "vetting" assumes that computers that sift through multiple databases are superior to the essential human elements of due diligence: personal relationships, on the ground experience and thorough financial oversight",
"NGOs Explain How USAID's Partner Vetting System Hurts Humanitarian Action & Is Contrary to U.S. Interests", *Charity and security network*, 14/01/2012 https://charityandsecurity.org/partner-vetting-system/comments_filed_pvs_winter_2011_2012/

bases de données non publiques à des fins de contrôle a été clairement démontrée. »[1170] En accédant aux bases de données du gouvernement américain, l'USAID peut consulter et analyser des informations sur le terrorisme qui ne sont pas accessibles au public pour des raisons de sécurité nationale[1171]. Et plutôt que d'être une mesure redondante, le PVS serait pour l'USAID une démarche complémentaire. Le bailleur ne précise pas de quelle source d'information il s'agit. Mais il semblerait, sans qu'on puisse rentrer dans les détails, que cet accès serait encore limité, du moins pour l'Office of General Inspector de l'USAID. L'agence déclare en janvier 2020 que : « les contraintes interagences sur l'accès de l'USAID aux informations de sécurité nationale, ainsi que les obstacles à l'obtention d'habilitations de sécurité appropriées et opportunes, ont limité l'activité de contrôle de l'USAID dans ce domaine et ont eu un impact sur la capacité de l'USAID à évaluer pleinement, à atténuer et à répondre aux menaces pesant sur ses programmes d'assistance humanitaire et de stabilisation. Dans un avis classifié, nous avons alerté l'USAID sur ces vulnérabilités et l'avons encouragé à évaluer sa stratégie de contrôle des programmes d'aide humanitaire et de surveillance des informations relatives à la sécurité nationale. »[1172]

Toujours est-il que le programme de VPS semble malgré tout avoir connu un relatif assouplissement. Courant 2020, est en effet communiquée une version amendée de ce dernier. D'après le réseau « Charity and security network », les changements portent sur les points suivants : la réduction du caractère rétroactif (de 10 ans à 3 ans) concernant le soutien à des entités terroristes ; la reformulation des contrats, il n'est plus question de limiter l'assistance aux bénéficiaires lorsqu'un bailleur ou une ONG a des raisons de croire qu'il est ciblé par des mesures de contre-terrorisme, mais seulement s'il en a directement connaissance[1173]. Cependant, le programme de vetting a connu d'autres évolutions : une refonte de la gouvernance, avec un plus grand rôle pour l'office de sécurité de l'USAID. La nouvelle politique de vetting entend aussi étendre des mesures de contrôle aux opérations de transfert d'argent informel, comme l'hawala, qu'on abordera dans les sections qui suivent. Elles sont en effet considérées comme étant des voies de financement du terrorisme.

Derniers points concernant l'USAID, comme on l'a déjà évoqué, il va sans dire que le conflit israélo-palestinien aura des répercussions certaines sur ce type de mesures, bien qu'on ne puisse pour le moment les objectiver. Pour le moment, il est simplement possible de noter que les financements de l'UNRWA ont été suspendus par plusieurs bailleurs, dont l'USAID.

---

[1170] "In conducting due diligence, USAID's implementing partners do not have access to these non-public databases and therefore cannot avail themselves of the same universe of information as USAID does in conducting vetting in Afghanistan, West Bank/Gaza and elsewhere. In protecting U.S. taxpayer resources from diversion, the importance in accessing information from non-public databases for the purposes of vetting has been clearly demonstrated."Federal Register 36693 Vol. 80, No. 123 Friday, June 26, 2015https://www.govinfo.gov/content/pkg/FR-2015-06-26/pdf/2015-15017.pdf

[1171] Ibid. https://www.govinfo.gov/content/pkg/FR-2015-06-26/pdf/2015-15017.pdf

[1172] « Interagency constraints on USAID's access to national security information, as well as obstacles to obtaining appropriate and timely security clearances, have limited USAID's monitoring activity in this area and impacted USAID's ability to fully assess, mitigate, and respond to threats to its humanitarian assistance and stabilization programs. In a classified advisory, we alerted USAID to these vulnerabilities and encouraged the Agency to evaluate its strategy for vetting humanitarian assistance programs and monitoring national security information »Limits in Vetting and Monitoring of National Security Information Pose Risks for USAID Humanitarian Assistance and Stabilization Programs, 15/01/2020, Office of inspector general, USAIDhttps://oig.usaid.gov/node/3696

[1173] "USAID Revises Grantee Documents Relating to Anti-Terrorism Requirements", *Charity and Security network*, 21/05/2020, https://charityandsecurity.org/false-claims-act-lawsuits/usaid-revises-grantee-documents-relating-to-anti-terrorism-requirements/

Toutefois, l'agence de développement américaine a rétabli des financements destinés à d'autres agences onusiennes opérant dans la bande de Gaza, comme le WFP[1174].

Plus généralement, elle ne conteste donc pas publiquement les différentes mesures de screening ou de vetting existantes, contrairement à d'autres coalitions d'acteurs qu'on a évoquées, qui revendiquent d'autres modalités de connaissance de la menace terroriste. Pour l'UNRWA, le processus de « screening » constitue un « régime de vérité » devant établir sa légitimité, un mécanisme dont la validité est toutefois contestée. Il se trouve effectivement que l'UNRWA est une organisation internationale, dotée de privilèges et immunités, donc comme le rappellent les rapports du Government Accountability Office américain de décembre 2023, l'organisation onusienne n'a pas eu à ce titre à appliquer les mesures de vetting de l'USAID relatives au Mission Order 21[1175].

Toutefois, l'action de l'UNRWA est contrôlée par différents mécanismes de contrôle, notamment au nom de la section 301 (c) du Foreign Assistance Act de 1961. Cette dernière requiert qu'« aucune contribution des États-Unis ne sera versée à [l'UNRWA] à moins que [l'UNRWA] ne prenne toutes les mesures possibles pour s'assurer qu'aucune partie de la contribution des États-Unis ne sera utilisée pour fournir une assistance à un réfugié qui reçoit une formation militaire en tant que membre de la soi-disant Armée de libération de la Palestine ou de toute autre organisation de type guérilla ou qui s'est engagé dans un quelconque acte de terrorisme. »[1176]D'où l'obligation pour l'UNRWA de communiquer au département d'État américain des indicateurs annuels relatifs à la « neutralité » de l'agence, ainsi que des résultats d'opération de screening de son personnel et de bénéficiaires, et ce tous les 6 mois. L'UNRWA opère elle-même des opérations de screening de bénéficiaires, contractuels, ou toutes organisations lui étant affiliées en se fondant sur la liste consolidée onusienne de sanctions. Pour ce faire, l'agence s'est dotée d'un logiciel interne de screening, LexisNexis Risk Solutions system. Cependant, point important, la liste onusienne ne comprend pas le Hamas (malgré des pressions allant dans le sens de son inclusion).

Concernant les salaires des personnels de l'UNRWA, ces derniers sont gérés par la Banque de Palestine, qui mène elle-même des opérations de screening, en se fondant sur des listes de sanction européennes (qui comprennent le Hamas). En plus de ces opérations de screening, l'UNRWA partage le nom et la fonction de son personnel annuellement aux pays hôtes (notamment avec le Liban, la Jordanie), ainsi qu'avec Israël et les USA. C'est alors à l'État d'alerter si un nom du personnel contrevient au cadre juridique local, pénalement

---

[1174] MIOLENE, Elisa, LYNCH, Colum, "USAID announces funding for Gaza, but not UNRWA", *Devex*, 28/02/2024 https://www.devex.com/news/usaid-announces-funding-for-gaza-but-not-unrwa-107154

[1175] "WEST BANK AND GAZA AID USAID Generally Ensured Compliance with Anti-terrorism Policies and Addressed Instances of Noncompliance", United States Government accountability office, December 2023, https://www.gao.gov/assets/D24106243.pdf
OFFICE of Inspector General, US Agency for international development, Assessment of USAID's Oversight Policies to Prevent the Diversion of Assistance to Hamas and Other Terrorist Organizations, 25/07/2024 https://oig.usaid.gov/sites/default/files/2024-08/USAID%20OIG%20Advisory%20on%20Gaza%20Oversight%207-25-2024.pdf

[1176]" No contributions by the United States shall be made to [UNRWA] except on the condition that [UNRWA] take all possible measures to assure that no part of the United States contribution shall be used to furnish assistance to any refugee who is receiving military training as a member of the so-called Palestine Liberation Army or any other guerrilla type organization or who has engaged in any act of terrorism." Department of State and United Nations Relief and Works Agency Actions to Implement Section 301(c) of the Foreign Assistance Act of 1961, "Briefing to the Staffs of The Senate Appropriations Subcommittee on Foreign Operations The House Appropriations Subcommittee on Foreign Operations, Export Financing, and Related Programs, 06/11/2023 https://www.gao.gov/assets/gao-04-276r.pdf

poursuivable. D'après le rapport Colonna, Israël n'aurait pas émis d'avis négatif sur les noms que l'UNRWA lui a communiqués depuis 2011. Jusqu'à mars 2024, Israël a reçu une liste de personnel de l'UNRWA sans documents d'identification, contrairement à mars 2024 : Israël reçoit une liste d'employés, et accuse l'UNRWA qu'un nombre significatif d'employés serait des membres du Hamas. Selon l'enquête, dirigée par Catherine Colonna, Israël n'aurait pas établi de preuves de liens entre le Hamas et l'UNRWA, mais selon le rapport, les mesures de vetting et de screening menées par l'agence humanitaire ne seraient pas suffisantes : « En dépit d'un ensemble complet de mesures visant à contrôler le personnel et d'autres personnes ou organisations affiliées à l'UNRWA, ces mesures ne permettent pas de procéder à des vérifications suffisantes. Les listes de sanctions des Nations Unies sont limitées à un petit nombre d'individus et l'UNRWA n'a pas le soutien des services de renseignement pour entreprendre des vérifications efficaces et complètes. »[1177] Parallèlement, en aout 2024, l'ONU a publié les résultats d'une enquête interne menée par le Bureau des services de contrôle interne de l'ONU, aboutissant à la conclusion de la possible implication de 9 membres de l'UNRWA dans l'attaque du 7 octobre[1178].

## § 2 — l'AFD

Si les pratiques de vetting par les organismes de la coopération internationale américaine ont une longue histoire, d'au moins une vingtaine d'années, la volonté de mettre en place des politiques de criblage de bénéficiaires par des bailleurs français est beaucoup plus récente. La mise à l'agenda du criblage des bénéficiaires s'inscrit dans l'évolution du champ d'action de l'Agence française de développement (AFD). En effet, si son mandat se restreint initialement aux politiques de développement, dans le cadre du nexus humanitaire/développement, l'AFD intervient tendanciellement dans des zones de crise, et se confronte à des enjeux sécuritaires relativement inédits pour l'agence, et donc à de nouveaux risques en matière de détournement de l'aide[1179], ainsi qu'un contexte plus difficile pour les « intérêts français » ,notamment en Afrique. Différents mécanismes d'audits sont cependant déjà bien implantés au sein de l'organisation. C'est en 2006 qu'a été créé un département du contrôle et de la conformité. Il est responsable de la lutte contre le blanchiment et le financement du terrorisme et il émet un avis préalable à toute décision de financement. L'Inspection générale de l'AFD, prend en outre différentes mesures : élaboration de rapports

[1177] « Despite a comprehensive set of measures to screen and vet staff and other individuals or organizations affiliated with UNRWA, these measures do not allow sufficient verifications. The UN sanctions lists are limited to a small number of individuals, and UNRWA lacks the support of intelligence services to undertake efficient and comprehensive vetting." FINAL REPORT FOR THE UNITED NATIONS SECRETARY-GENERAL Independent Review of Mechanisms and Procedures to Ensure Adherence by UNRWA to the Humanitarian Principle of Neutrality, 20/04/2024 https://www.un.org/sites/un2.un.org/files/2024/04/unrwa_independent_review_on_neutrality.pdf

[1178] NOOTEN, Carrie, REMY, Jean-Philippe, « L'ONU confirme la possible implication de neuf salariés de l'UNRWA dans l'attaque du 7 octobre », Le Monde, 06/08/2024
https://www.lemonde.fr/international/article/2024/08/06/l-onu-confirme-la-possible-implication-de-neuf-salaries-de-l-unrwa-dans-l-attaque-du-7-octobre_6269835_3210.html

[1179] L'AFD peut soutenir des projets humanitaires notamment via le programme dit la facilité d'atténuation des vulnérabilités, renommée « fonds paix et résilience » - FPR – dit « Minka »), décidée par le Comité interministériel de la Coopération internationale et du Développement (CICID) du 30 novembre 2016
DE GEOFFROY, Véronique, CATTEAU, Thomas, FOIN, Thomas, GRUNEWALD, François, « bilan des engagements de la stratégie humanitaire de la république française 2018-2022 : une aide humanitaire plus efficace face aux crises de demain ? », Groupe URD, Janvier 2023 https://www.diplomatie.gouv.fr/IMG/pdf/meae_2023_06_01_bilan_shrf_2018_-_2022_urd_cle0c7f11.pdf

de risques, élaboration de procédures de contrôle. Et surtout, il est chargé d'émettre un avis avant toute demande de financement, concernant les risques de type LBA/FT. À ce titre, il est en lien avec la cellule de renseignement financier TRACFIN (Traitement du renseignement et action contre les circuits financiers clandestins), et peut communiquer à l'agence des rapports de déclarations de soupçon[1180].

Il est surligné que les risques de type LBC/FT sont aussi pris en compte par le Département de la conformité, et en lien avec l'évolution du contexte sécuritaire « en plus des diligences classiques, l'AFD veillera à élaborer, en lien avec les services de la Direction générale du Trésor, un cadre de diligences anticorruption/antiterrorisme ad hoc, pouvant s'appliquer spécifiquement aux opérations d'appui aux OSC en zones sensibles. » Cette orientation est confirmée dans le « cadre d'intervention transversal » OSC 2018-2023[1181] et dans le guide de la Direction générale Trésor du ministère de l'Économie français *:* « Risque de financement du terrorisme : Guide de Bonne Conduite à l'attention des associations » *[1182].* On y retrouve des références à la recommandation n° 8 du GAFI, pointant le risque que représenteraient les ONG en matière de financement du terrorisme. Le GAFI a d'ailleurs a pris note de ces mesures. Dans un rapport de mai 2022, on peut lire qu'il se félicite que les autorités françaises aient « renforcé le contrôle exercé par le Centre de crise et de soutien (CDCS) du Ministère de l'Europe et des Affaires étrangères et l'Agence française de développement (AFD), principaux bailleurs de l'aide humanitaire publique française, sur leurs partenaires de mise en œuvre. La CDCS et l'AFD veillent à ce que ses partenaires agissent en conformité avec la loi et les conditions pour la subvention publique. En 2018, une cellule audit/évaluation a été créée au sein du CDCS en parallèle à l'augmentation des budgets alloués par les bailleurs publics français à l'action humanitaire. Les risques de FT sont pris en compte dans les termes contractuels avec les partenaires. »[1183] Mais le GAFI reste prudent sur les dispositions de l'AFD : « Des mesures spécifiques de sensibilisation ont été prises. Certaines des mesures spécifiques restent cependant récentes et leur efficacité pourra être évaluée à l'avenir. »[1184]

D'ailleurs, dans un premier temps dans les clauses des contrats de financement de l'AFD, il n'est pas encore question de criblage des bénéficiaires finaux de l'aide. Le criblage concernait tout d'abord un nombre plus restreint d'individus : les acteurs clefs, comme le comptable, le responsable des relations humaines, ou des employés de l'ONG. Ces mesures ont toutefois

---

[1180] « Rapport annuel, Agence française de développement », 2006 https://medias.vie-publique.fr/data_storage_s3/rapport/pdf/084000430.pdf

[1181] « Dans de nombreuses zones d'intervention, l'AFD doit faire face à des risques de détournements des fonds à destination des OSC notamment à des fins de financement de terrorisme. En dépit des nombreux et croissants efforts entrepris par les OSC, appuyées par l'AFD, afin de promouvoir et renforcer les diligences sur leurs opérations, certaines peuvent rester vulnérables à leur exploitation et détournement par des organisations terroristes afin de se procurer ou de faire circuler des fonds, de fournir un soutien logistique, d'encourager ou de faciliter le recrutement de terroristes, ou encore de soutenir des terroristes ou des organisations/opérations terroristes. « Cadre d'intervention stratégie : l'AFD partenaire des Organisations de la société civile 2018/ 2023

*[1182]* https://www.tresor.economie.gouv.fr/Ressources/File/433045

Rapport d'information sur la lutte contre le financement du terrorisme international, Co-rapporteures Mme Valérie BOYER, Mme Sonia KRIMI,2017https://www.assemblee-nationale.fr/dyn/docs/RINFANR5L15B1833.raw

"Rapport d'information sur la mise en œuvre des conclusions du rapport d'information (n° 1822) du 28 mars 2019 sur l'évaluation de la lutte contre la délinquance financière Présenté PAR MM. Ugo BERNALICIS et Jacques MAIRE
https://www.assemblee-nationale.fr/dyn/docs/RINFANR5L15B4314.raw

[1183] « Mesures de lutte contre le blanchiment de capitaux et le financement du terrorisme France », Rapport d'évaluation mutuelle,GAFI, mai 2022, https://acpr.banque-france.fr/sites/default/files/medias/documents/20220518_gafi_lcf_ft_rapport_evaluation_mutuelle_france.pdf

[1184] « Mesures de lutte contre le blanchiment de capitaux et le financement du terrorisme France », Rapport d'évaluation mutuelle,GAFI, mai 2022, https://acpr.banque-france.fr/sites/default/files/medias/documents/20220518_gafi_lcf_ft_rapport_evaluation_mutuelle_france.pdf

été ensuite étendues aux partenaires des ONG en cas de refinancement supérieur à 5 000 euros. Et dans son Cadre d'intervention stratégie 2018/2019, il est fait référence à la nécessité de renforcer ce type de mesures : « Devant la persistance de la menace dans les zones sensibles où l'AFD opère de manière renforcée en appui à des OSC (Facilité Crises et Vulnérabilités et régions du Sahel, Irak-Syrie, autres), il est nécessaire d'approfondir la prise en compte de ces risques dans les opérations de l'Agence. En conséquence, en plus des diligences classiques, l'AFD veillera à élaborer, en lien avec les services de la Direction générale du Trésor, un cadre de diligences LCB-FT ad hoc, pouvant s'appliquer spécifiquement aux opérations d'appui aux OSC en zones sensibles. »[1185]

C'est l'ordonnance n° 2020-1342 qui aurait ouvert la porte au criblage des bénéficiaires : elle élargit le champ des individus devant respecter la mesure des gels des avoirs, et touche désormais les ONG humanitaires. Elle transpose en droit français la directive (UE) 2015/849 concernant la lutte contre le blanchiment d'argent et le financement du terrorisme (LBA/FT) et modifie l'article 562-4 du Code monétaire et financier. L'article impose pour toute personne morale de droit français de vérifier qu'elle n'utilise ni ne met à disposition directement ou indirectement des fonds et ressources économiques au profit de personnes ciblées une mesure de gel d'avoir[1186]. Dans un document datant de juin 2021, la coalition d'ONG Coordination Sud, argue que cet article est en contradiction avec l'article 9 de la directive européenne 2017/541 qui ménage une exemption humanitaire aux mesures de lutte contre le financement du terrorisme[1187]. Cela dit, cette exemption ne concerne que le contenu de la directive et non pas l'ensemble des sanctions européennes[1188]. Autre point, Coordination Sud regrette aussi que cette clause d'exemption est comprise dans la directive européenne 2017/541 au préambule de la directive et non comme article, ce qui fait que le droit de l'UE n'oblige pas à transposer cette dernière dans le droit interne des États

[1185] Cadre d'intervention stratégie : l'AFD partenaire des Organisations de la société civile 2018/2023

[1186] Article L562-4, Code monétaire et financier https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000045250683
Article L562-5, Code monétaire et financierhttps://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000045250670

[1187] Contribution D'Action contre la Faim, CARE France, Coordination Sud1, la Croix- Rouge française, Electriciens sans Frontières, HAMAP-Humanitaire, Handicap International, La Chaîne de l'Espoir, Médecins du Monde, Première Urgence International, Secours Islamique France, Solidarités International À l'évaluation de la Directive relative à la lutte contre le terrorisme
[Directive (UE) 2017/541 https://www.coordinationsud.org/wp-content/uploads/ONG-francaises_Contribution-a-evaluation-directive-UE-2017-541_VF-1.pdf

[1188] Article 11 - Financement du terrorisme
1. Les États membres prennent les mesures nécessaires pour que soit punissable en tant qu'infraction pénale, lorsqu'il est commis de manière intentionnelle, le fait de fournir ou de réunir des fonds, par quelque moyen que ce soit, directement ou indirectement, avec l'intention que ces fonds soient utilisés ou en sachant qu'ils seront utilisés, en tout ou en partie, en vue de commettre l'une des infractions visées aux articles 3 à 10 ou de contribuer à la commission d'une telle infraction.
2. Lorsque le financement du terrorisme visé au paragraphe 1 du présent article concerne l'une des infractions prévues aux articles 3, 4 et 9, il n'est pas nécessaire que les fonds soient effectivement utilisés, en tout ou en partie, en vue de commettre l'une de ces infractions ou de contribuer à la commission d'une telle infraction, pas plus qu'il n'est nécessaire que l'auteur de l'infraction sache pour quelle infraction ou quelles infractions spécifiques les fonds seront utilisés. https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32017L0541
DIRECTIVE (UE) 2017/541 Art : (37) La présente directive ne saurait avoir pour effet de modifier les droits, obligations et responsabilités des États membres découlant du droit international, y compris du droit international humanitaire. La présente directive ne régit pas les activités des forces armées en période de conflit armé, au sens donné à ces termes en droit international humanitaire, lesquelles sont régies par ce droit, ni les activités menées par les forces militaires d'un État dans l'exercice de leurs fonctions officielles, dans la mesure où elles sont régies par d'autres règles de droit international.
Art : (38) Les activités humanitaires menées par des organisations humanitaires impartiales reconnues par le droit international, y compris le droit international humanitaire, ne relèvent pas du champ d'application de la présente directive, tout en prenant en considération la jurisprudence de la Cour de justice de l'Union européenne.
https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32017L0541

membres[1189]. Et ce n'est que fin 2022 qu'a été adoptée la résolution 2664 qui aurait impulsé une adoption progressive des exemptions des listes autonomes (et donc européennes) pour une partie de ses sanctions (d'après le CICR ces exemptions concernent 27 listes sur 39.)[1190]

En tout cas, courant 2020, en cohérence avec l'évolution du Code monétaire et financier, l'AFD commence à imposer des mesures de criblage ciblant les bénéficiaires de l'aide. Il est toutefois difficile de déterminer à quand exactement remonte cette pratique. En tout cas, d'après le témoignage de Thierry Mauricet, à la date du 30 novembre 2021, une dizaine d'ONG avaient refusé de signer des conventions de subvention, du fait de clauses antiterroristes exigeant ce type d'opération[1191].

La préservation de l'espace humanitaire est pourtant à l'agenda politique. En février 2017, un groupe de travail — « accès humanitaire et système bancaire » a été créé au sein de la Coordination Humanitaire & Développement. Il impulse une série d'échanges entre les ONG et les ministères touchés par ces enjeux : le ministère de l'Europe et des Affaires étrangères, le ministère des Armées, le ministère de l'Intérieur et le ministère de l'Économie et des Finances. Ce groupe était cependant dédié moins aux problématiques liées aux contrats des bailleurs qu'aux difficultés croissantes en matière de transferts bancaires. Son objectif est d'atteindre un consensus entre les ONG, l'État et les banques. Ont été aussi impliqués la DG du Trésor, l'Autorité de Contrôle prudentiel et de Résolution, le Tracfin, et enfin des responsables des services de conformités de banques.

Un autre groupe de plaidoyer s'est constitué autour de Coordination SUD (regroupant 180 ONG françaises), soit un réseau déjà bien implanté depuis 1994, qui plaide pour le respect du DIH et à la préservation de l'espace humanitaire. On verra qu'il s'agit d'un des acteurs majeurs impliqués sur le sujet du criblage des bénéficiaires[1192]. Plus généralement, le sujet semble faire consensus parmi les ONG françaises, qui y sont unanimement opposées. Carine Roland, présidente de Médecins du Monde, alerte en 2022 dans un article du monde : « Cela revient à externaliser le risque en transformant les acteurs humanitaires en acteurs

---

[1189] Contribution D'Action contre la Faim, CARE France, Coordination Sud1, la Croix- Rouge française, Electriciens sans Frontières, Handicap International, La Chaîne de l'Espoir, Médecins du Monde, Première Urgence International, Secours Islamique France, Solidarités International À l'évaluation de la Directive relative à la lutte contre le terrorisme [Directive (UE) 2017/541], Juin 2021 https://www.premiere-urgence.org/wp-content/uploads/2021/06/ONG-fran%C3%A7aises_Contribution-%C3%A0-%C3%A9valuation-directive-UE-2017-541_VF.pdf

[1190] Humanitarian action: EU introduces exemptions to sanctions to facilitate the delivery of assistance, PRESS RELEASE 253/23 31/03/2023 https://www.consilium.europa.eu/en/press/press-releases/2023/03/31/humanitarian-action-eu-introduces-exemptions-to-sanctions-to-facilitate-the-delivery-of-assistance/pdf

Humanitarian action: EU introduces further exception to sanctions, 19/02/2024 https://www.consilium.europa.eu/en/press/press-releases/2024/02/19/humanitarian-action-eu-introduces-further-exception-to-sanctions/

The EU Delegation to the UN Office and other international organisations in Geneva presents its compliments to the Office of the High Commissioner and has the honour to refer to the joint communication dated 26 October 2022 (ref AL OTH 106/2022). https://spcommreports.ohchr.org/TMResultsBase/DownLoadFile?gId=37290

HUVE, Sophie, MOULIN, Guillemette, FERRARO, Tristan, "Unblocking aid : the EU's 2023 shift in sanctions policy to safeguard humanitarian efforts, *Humanitarian law& policy*, 23/01/2024 https://blogs.icrc.org/law-and-policy/2024/01/23/unblocking-aid-eu-2023-sanctions-policy-humanitarian-efforts/

[1191]« L'humanitaire sanctionné ?, Une interview avec Thierry Mauricet sur les conséquences des mesures anti-terroristes sur les transferts bancaires des ONG », *Défis humanitaires*, 30/11/2020 https://defishumanitaires.com/2020/11/30/mauricet-transferts-bancaires-humanitaire/

[1192] Recommandations de Coordination SUD et de ses membres : Protéger et garantir un espace humanitaire pour les populations civiles et les acteurs et actrices de la solidarité internationale, 10/09/2020 https://www.coordinationsud.org/wp-content/uploads/Recommandations-de-Coordination-SUD-et-membres-protection_espace-humanitaire-10-09-20.pdf

sécuritaires, c'est philosophiquement problématique.» [1193] Après avoir fait appel au respect du droit humanitaire, Alain Boinet, dans un éditorial publié le 30 novembre 2020, relie le criblage des bénéficiaires à de potentielles atteintes en matière de vie privée : « Mais, il est une réflexion plus vaste qui doit nous interpeler. Est-ce que le terrorisme, qui est toujours condamnable, les technologies de l'intelligence artificielle, l'insécurité ambiante, le délitement de la cohésion sociale et nationale ne nous conduisent pas sur la pente dangereuse du traçage et du contrôle généralisé inspiré du modèle chinois où la liberté est en question comme nous l'annonçait, déjà, l'écrivain Georges Orwell ? »[1194] Cet argument est repris en partie par Pierre Micheletti — président d'Action contre la faim (ACF). Ce dernier déclare dans un article pour Alternatives humanitaire que : « L'intention avouée vise à vérifier que les bénéficiaires de notre aide ne figurent pas sur des listes de personnes identifiées comme ayant appartenu à des groupes terroristes. Cette mesure expose les humanitaires, dans des environnements parfois ultra-violents, à passer pour des "mouchards" et des indicateurs aux yeux des groupes rebelles. »[1195] Mais plus généralement, l'objectif majeur des ONG reste la protection des travailleurs humanitaires et la garantie de l'accès au terrain de crises ainsi qu'une allocation impartiale de l'aide. Et dans un entretien publié sur le blog de l'ONG Solidarité International, le directeur général de Première urgence internationale rapporte que : « Cribler les bénéficiaires "ultimes" reviendrait à ne plus les sélectionner sur la base de leurs besoins, ce qui ferait perdre aux ONG leur impartialité, une grave entorse aux principes humanitaires, et aurait pour conséquence de les priver de leur capacité d'accès. »[1196] Enfin, le CICR s'est distancié de l'AFD, en déclarant que si la collaboration avec l'agence avait été riche d'enseignement, le défi majeur à l'établissement d'un partenariat durable avec l'agence concerne « l'ensemble des mesures de restrictions (sanctions, contre-terrorisme, mesures anti-blanchiment, droit bancaire et financier, etc.) qui obligent des organisations de développement telles que l'AFD à adopter des stratégies de gestion des risques très conservatrices. Celles-ci limitent de fait les possibilités de partenariat avec une organisation comme le CICR. Son rôle mais aussi sa valeur ajoutée est d'apporter une réponse impartiale, c'est-à-dire uniquement basée sur les besoins. »[1197]

Quant à la position officielle du gouvernement, elle semble tout d'abord aller — dans une certaine mesure — dans le même sens que les ONG. Déjà en 2019, la France s'était engagée en faveur de la protection de l'espace humanitaire avec l'Appel à Action humanitaire. Ce dernier vise à une meilleure application du DIH, et a été lancé avec l'Allemagne dans le cadre

---

[1193] « La traçabilité de l'aide humanitaire débattue devant le Conseil d'État », *le Monde*, 16/03/2022 https://www.lemonde.fr/societe/article/2022/03/16/la-tracabilite-de-l-aide-humanitaire-debattue-devant-le-conseil-d-etat_6117709_3224.html

[1194] BOINET, Thierry, « Monsieur le Président de la République, protégeons l'aide humanitaire qui est en danger ! », *Défis humanitaires*, 30/11/2020 https://defishumanitaires.com/2020/11/30/edito-47-alain-boinet/

[1195] MICHELETTI, Pierre, « L'humanitaire au risque de l'empêchement : quelles analyses pour quelles stratégies correctives ? », *Alternatives humanitaires*, n°16, 2021 https://www.alternatives-humanitaires.org/fr/2021/03/25/lhumanitaire-au-risque-de-lempechement-quelles-analyses-pour-quelles-strategies-correctives/

[1196] « L'humanitaire sanctionné ?, Une interview avec Thierry Mauricet sur les conséquences des mesures anti-terroristes sur les transferts bancaires des ONG », *Défis humanitaires*, 30/11/2020 https://defishumanitaires.com/2020/11/30/mauricet-transferts-bancaires-humanitaire/

[1197] « Moyen-Orient : CICR et AFD, un partenariat riche d'enseignements, Entretien avec Fabrizio Carboni (CICR) et Catherine Bonnaud (AFD) », CICR, 15/12/2020 https://www.icrc.org/fr/document/liban-cicr-et-afd-un-partenariat-riche-denseignements

de l'Alliance pour le multilatéralisme[1198]. De surcroit, début janvier 2020, lors d'une réunion sur la situation syrienne impliquant des ONG et le Président de la République, ce sujet a été à nouveau abordé. Il a été demandé à la cellule diplomatique de l'Élysée de se saisir du problème. Ces premiers échanges concernent la thématique plus large des transferts bancaires. Ils ont connu un nouveau développement lors de la Conférence nationale humanitaire de 2020. L'objet des échanges était de garantir la sécurité des humanitaires, le financement de l'aide et l'accès aux banques et la prise en compte de l'impact des mesures de contreterrorisme. Et donc la position officielle est tout d'abord de ne pas exclure les bénéficiaires de l'aide pour cause d'appartenance ou de soutien à un groupe armé terroriste. Emmanuel Macron y a d'abord déclaré, dans son discours de clôture, que la France appliquerait : « totalement le principe de non-discrimination dans l'attribution de l'aide suivant les besoins des populations ». Les ONG avaient alors espéré y voir un signe d'une possible exemption humanitaire à l'ordonnance du 4 novembre 2020 leur imposant des mesures de contrôle supplémentaires[1199].

Leurs revendications semblent avoir été dans un premier temps entendues. En 2021 est discuté un projet de loi sur la préservation de l'espace humanitaire. Ses articles 2 et 3 prévoient de créer « un nouvel article 226223 au sein du Code pénal qui réprime le refus à l'accès au système bancaire aux organisations non gouvernementales et associations humanitaires sur le seul critère de l'exigence de la procédure de contrôle et de filtrage dite du "criblage" des bénéficiaires finaux des programmes humanitaires. » [1200] La Commission nationale consultative des droits de l'homme (CNCDH) a été saisie pour un avis sur ce sujet[1201]. Verdict de la Commission : cet article est bienvenu, mais trop restrictif. Pénaliser les refus de financement qu'en cas de criblage laisse la porte ouverte à trop de motifs supplémentaires d'opposition[1202]. Toujours est-il que la loi sur l'espace humanitaire est restée à l'état de proposition et n'a fait l'objet que d'une première lecture à l'Assemblée nationale.

---

[1198] « Appel à l'action humanitaire, Alliance pour le multilatéralisme », 26/09/2019 https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/la-france-et-les-nations-unies/l-alliance-pour-le-multilateralisme/appel-a-l-action-humanitaire/

[1199] « Nous retenons, par ailleurs, l'engagement du Président à appliquer pleinement le principe de non-discrimination des populations bénéficiaires dans l'attribution de l'aide publique française. Nous attendons désormais que cet engagement essentiel soit décliné par toutes les administrations et bailleurs publics de l'aide au développement et de l'action humanitaire, en levant par conséquent toute obligation de criblage des bénéficiaires finaux destinataires de cette même aide. De plus, nous adhérons pleinement à la proposition énoncée par le commissaire européen M. Janez Lenarcic que tous les bailleurs s'alignent derrière le principe de non-criblage des bénéficiaires finaux. »
« Conférence Nationale humanitaire : premières réactions des ONG humanitaires », Carefrance, 24/12/2020https://www.carefrance.org/actualites/cnh-premieres-reactions-ong-coordination-sud/

[1200] Proposition de loi n° 4354 relative à la préservation de l'espace humanitaire, 13/07/2021https://www.assemblee-nationale.fr/dyn/15/textes/l15b4354_proposition-loi#
Article 2 « L'infraction de refus d'assistance dans la préparation ou la réalisation d'une transaction visée par les articles L. 5611 à L. 5642 du code monétaire et financier est constituée dès lors que ce refus se fonde exclusivement sur l'exigence par l'une des personnes visées à l'article L. 5612 du même code que l'organisation non gouvernementale ou l'association humanitaire impartiale susvisée procède au contrôle et au filtrage de l'identité des bénéficiaires effectifs au sens de l'article L. 56122 du même code, de ses programmes d'aide humanitaire, aux fins de vérification que ces bénéficiaires, personnes physiques, ne soient pas recensées sur une liste portant mesures restrictives dans le cadre de la lutte contre le terrorisme ou impliquées dans des violations du droit international, par la mise en œuvre d'un outil automatisé de détection. »

[1201] Les banques pourraient choisir de refuser d'assister les organisations humanitaires impartiales plutôt que de s'exposer à d'éventuels risques supplémentaires.

[1202]« Avis sur la proposition de loi relative à la préservation de l'espace humanitaire », 25/11/2021, Commission nationale consultative des droits de l'hommehttps://www.cncdh.fr/sites/default/files/2021-11/A%20-%202021%20-%2011%20-%20Pr%C3%A9servation%20de%20l%27espace%20humanitaire%2C%20novembre%202021.pdf
Avis sur la proposition de loi relative à la préservation de l'espace humanitaire (A — 2021- 11) NOR : CDHX2135633V JORF n°0283 du 5 décembre 2021 Texte n° 119 https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000044413483

Or, ce premier mouvement en faveur d'un retrait des mesures de criblage va connaitre un infléchissement certain lors de l'examen de la loi 2021/n° 1031 du 4 aout 2021 de programmation relative au développement solidaire et à la lutte contre les inégalités mondiales. Initialement, cette dernière n'entérine pas en soi ce type de mesure. Les premières versions du texte ne mentionnent à vrai dire pas directement le sujet, qui n'est abordé que lors des discussions sur le texte et lors des débats à l'Assemblée nationale[1203]. Coordination Sud défend plusieurs propositions d'amendements lors de l'examen de la loi. Sa stratégie est de défendre le principe de « non-discrimination » afin d'assurer l'interdiction du criblage : un bénéficiaire se révélant être ciblé par une liste de sanction serait — potentiellement — exclu d'un programme d'aide[1204]. Ce principe a d'abord été voté lors de l'adoption de l'article 1 A[1205].

En effet, cet article dispose expressément que : « La France s'engage à ce que les actions menées sur financement de son aide publique au développement puissent être mises en œuvre dans le respect du principe de non-discrimination de l'attribution de l'aide aux populations.» [1206] L'Article 1A de la loi a été préservé lors du vote le 17 mai 2021. Mais lors du vote en commission paritaire en juin de la même année, il a été remplacé par une expression plus vague et ne désigne plus les populations dans leur ensemble, mais simplement celles éligibles à l'aide humanitaire[1207]. Et pour le journal d'investigation Disclose publié en octobre 2021 « à ce jour, l'interdiction du criblage n'est pas inscrite dans la loi française. »[1208]

Et surtout, la version définitive de la loi impose dans un nouvel article numéro 17 la publication d'un rapport sur la condition de faisabilité de dispense de criblage des bénéficiaires : « pour certaines actions de stabilisation à l'intérieur de périmètres géographiques définis caractérisés par une situation de crise persistante et l'existence de groupes armés non étatiques. »[1209] Et donc si Coordination Sud plaide pour une exemption totale du criblage[1210], il a été retenu que les mesures de criblages pourraient certes ne pas s'appliquer aux projets humanitaires, mais pourraient concerner des projets de développement. C'est la position de

---

[1203] LOI n° 2021-1031 du 4 août 2021 de programmation relative au développement solidaire et à la lutte contre les inégalités mondiales https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043898536

[1204] https://www.coordinationsud.org/wp-content/uploads/Feuillet-damendement-Edition_Senat.VF_.pdf
Loi de programmation relative au développement solidaire et à la lutte contre les inégalités mondiales, Coordination Sud, Février 2021 https://www.coordinationsud.org/wp-content/uploads/Note-dAnalyse-LOP-DSLIM-Coordination-SUD.pdf
Projet de loi de programmation relatif au développement solidaire 1ère lecture, AMENDEMENT présenté par MM. SAURY et TEMAL, rapporteurs, 09/04/2021
https://www.senat.fr/amendements/commissions/2020-2021/404/jeu_complet.html
Loi de Programmation lutte contre les inégalités mondiales - (N° 3699 AMENDEMENT N° AE296 présenté par Mme Poletti, M. Quentin, M. Teissier, M. Cordier et M. Herbillon, 05/02/2021 https://www.assemblee-nationale.fr/dyn/15/amendements_alt/3699/CION_AFETR/AE296

[1205] Note de position, loi programmation relative au développement solidaire et à la lutte contre les inégalités mondiales, Coordination Sud, juin 2021https://www.coordinationsud.org/wp-content/uploads/17.06.2021_Note-de-position-CSUD-CMP.VF_.pdf
Feuillet d'amendements Pour une loi dotée d'un budget à la hauteur des ambitions et qui reconnaisse pleinement la place de la société civile. loi de programmation relative au développement solidaire et a la lutte contre les inégalités mondiales
https://www.coordinationsud.org/wp-content/uploads/Feuillet-damendement-Edition_Senat.VF_.pdf
Amendement, projet de loi PJL de programmation relatif au développement solidaire (1ère lecture) (n° 404 )
https://www.senat.fr/amendements/commissions/2020-2021/404/Amdt_COM-9.html

[1206] « Loi Développement solidaire|Exclusion définitive, par la loi, du criblage des bénéficiaires finaux ! », Coordination Sud, 21/05/2021, https://www.coordinationsud.org/communique-de-presse/loi-developpement-solidaire-coordination-sud-et-ses-membres-se-felicitent-de-lexclusion-definitive-par-la-loi-du-criblage-des-beneficiaires-finaux/

[1207] https://www.assemblee-nationale.fr/dyn/15/textes/l15b4279_texte-adopte-commission#D_Article_1er_A

[1208] BRABANT, Justine, FOUCHARD, Anthony, "L'État tente d'imposer le traçage des bénéficiaires de l'aide humanitaire", *Disclos*e, 01/10/2021 https://disclose.ngo/fr/article/etat-renforce-controle-aide-humanitaire

[1209] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043898536

[1210] Note de position, loi programmation relative au développement solidaire et à la lutte contre les inégalités mondiales, Coordination Sud, juin 2021https://www.coordinationsud.org/wp-content/uploads/17.06.2021_Note-de-position-CSUD-CMP.VF_.pdf

Jean-Yves Le Drian[1211], et un courrier du Premier ministre au ministère des Affaires étrangères et au ministère de l'Économie confirmerait cette orientation. On peut y lire que : « ne doit pas être exigé le criblage des bénéficiaires finaux de l'aide, y compris pour les remises de fonds, dans les situations où les principes de l'action humanitaire s'appliquent, c'est-à-dire lorsque les projets, notamment ceux financés par l'État et ses opérateurs, répondent aux besoins essentiels des populations en situation de risque humanitaire. »[1212] L'objectif serait de restreindre l'exemption de criblage simplement à certaines zones. Notons que l'USAID a mis en place des mesures de criblage en priorité dans des zones sensibles : en Afghanistan, à Gaza, au Nigeria. Alors que dans le cas français, la sécurité des humanitaires est mentionnée comme l'argument prioritaire en faveur d'une non-application de mesure de criblage dans des zones en crise : « Dans ces zones caractérisées par une situation de crise persistante et l'existence de groupes armés non étatiques, les mesures de criblage peuvent faire porter en effet des risques sécuritaires et juridiques sur les ONG humanitaires. »[1213]

Il reste cependant un point crucial : préciser l'étendue de ces zones. Pour ce faire, le ministère des Affaires étrangères publie en décembre 2021 des lignes directrices qui fixent les conditions de définition d'une zone de crise devant être exemptée de criblage, et permettre, selon le ministère, d'exclure de telles opérations : « la grande majorité des projets mis en œuvre par les organisations de la société civile. »[1214] Le recueil de « faisceaux d'indices » permettrait d'identifier les projets « répondant directement aux besoins essentiels des populations en situation de risque humanitaire. » Et l'aide humanitaire est distinguée des programmes plus « politiques » ou en lien avec une dimension sécuritaire : les projets d'appui à la sécurité et de « State building », des projets comportant des activités en lien avec les armées françaises (des opérations de déminage par exemple).

Le ministère a une lecture positive de ces lignes directrices, qui : « constituent un guide dans l'instruction des dossiers, ouvrant la possibilité d'une appréciation politique de chaque cas. »[1215] Il se réjouit également que : « deux projets, au Niger et au Tchad, avaient été octroyés lors du dernier Conseil d'administration de l'AFD, les lignes directrices ayant permis de lever l'avis négatif initial de la Direction de la conformité. »[1216]

---

[1211] « S'agissant des ONG concernées par des aides ou des partenariats de projets utilisant des outils français, nous sommes très clairs : il faut un criblage des bénéficiaires pour éviter le blanchiment d'argent ou des détournements à des fins terroristes, sauf en ce qui concerne l'aide humanitaire. Cette aide urgente pour des populations dans le désarroi ou en détresse n'est pas soumise au criblage : nous n'avons pas le temps - ni la volonté - de le réaliser. Ce sont les normes internationales, de l'OCDE, auxquelles tout le monde doit se plier. » Déclaration de M. Jean-Yves Le Drian, ministre de l'Europe et des affaires étrangères, sur le projet de loi de programmation relatif au développement solidaire et à la lutte contre les inégalités mondiales, à l'Assemblée nationale le 2 février 2021https://www.vie-publique.fr/discours/278478-jean-yves-le-drian-02022021-aide-au-developpement

[1212] DE GEOFFROY, Véronique, CATTEAU, Thomas, FOIN, Thomas, GRUNEWALD, François, « bilan des engagements de la stratégie humanitaire de la république française 2018-2022 : une aide humanitaire plus efficace face aux crises de demain ? », Groupe URD, Janvier 2023 https://www.diplomatie.gouv.fr/IMG/pdf/meae_2023_06_01_bilan_shrf_2018_-_2022_urd_cle0c7f11.pdf

[1213] Ibid.

[1214] Obligation de criblage des bénéficiaires de l'aide publique au développement Question écrite n°00104 - 16e législature, Question de M. BONNE Bernard (Loire - Les Républicains) publiée le 07/07/2022 https://www.senat.fr/questions/base/2022/qSEQ220700104.html

[1215] Conseil national du développement et de la solidarité internationale, Compte rendu de la session plénière, 17/12/2021 https://www.diplomatie.gouv.fr/IMG/pdf/2022_01_06_cr_pleniere_17_12_2021_cm_cle41c15e.pdf

[1216] Conseil national du développement et de la solidarité internationale, Compte rendu de la session plénière, 17/12/2021 https://www.diplomatie.gouv.fr/IMG/pdf/2022_01_06_cr_pleniere_17_12_2021_cm_cle41c15e.pdf

Quant au rapport, il a été remis au Parlement le 13 décembre 2021. Et il conclut également à la pertinence des lignes directrices, pourtant contestées par les ONG[1217]. En effet, pour Coordination Sud, elles ne donneraient qu'une définition floue de la différence entre programme humanitaire et programme de développement. L'AFD elle-même convient que distinguer contexte d'urgence et contextes de « stabilisation » ou de « développement » n'est pas une tâche simple[1218]. Pour autant, le rapport conclut que les lignes directrices émises par le ministère sont particulièrement claires et bien développées. En janvier 2022, elles entrent donc en vigueur, imposant le criblage des bénéficiaires, dans des cas précis, hors actions d'urgence et hors certaines exceptions (personnes sans état civil, personnes mineures, exposées à des formes de persécution, etc.). Cependant, pour les ONG, ces exceptions sont floues : « Les OSC rencontrées par la Cour, tout en maintenant leurs critiques antérieures, soulignent l'imprécision des exceptions mentionnées dans les lignes directrices. (…) Si le directeur général de l'AFD a tenu à rassurer les OSC en promettant une interprétation souple des lignes directrices, il est fait état de différences d'approche entre la DPA/OSC et les services administratifs et financiers de l'AFD, ce qui contraint le qui contraint les OSC à des négociations difficiles projet par projet sur l'application du criblage. »[1219] Pour tout dire, le criblage mettrait à mal la volonté d'un continuum entre l'aide d'urgence et les programmes de développement. Pourtant, le criblage est inscrite à l'article 1er de la loi de programmation relative au développement solidaire et à la lutte contre les inégalités mondiales de 2021[1220]. En effet, l'aide d'urgence s'entrecroise souvent avec des dispositifs d'aide au développement, au regard de la complexité des environnements dans lesquels elles sont déployées. Les humanitaires craignent donc que les analyses aux cas par cas ne se transforment en bourbiers administratifs, contraires à la souplesse nécessaire à l'intervention d'urgence[1221]. Ce cas français fait écho aux travaux d'Emanuela Chiara Gillard, qui s'inquiète d'une tendance à l'adoption de mesures de criblage dans les politiques de développement. Elle craint qu'elles ne soient d'autant plus difficiles à contrer, les organisations ne pouvant faire appel au DIH et aux principes éthiques d'impartialité, d'indépendance et de neutralité comme le font les ONG humanitaires[1222]. En somme, la coalition de causes regroupée autour de l'organisation

[1217] Rapport d'information déposé en application de l'article 145-7 du Règlement par la commission des affaires étrangères sur l'application de la loi n° 2021-1031 du 4 août 2021 de programmation relative au développement solidaire et à la lutte contre les inégalités mondialeshttps://www.assemblee-nationale.fr/dyn/15/rapports/cion_afetr/l15b5110_rapport-information.pdf

[1218] BRABANT, Justine, FOUCHARD, Anthony, « L'État tente d'imposer le traçage des bénéficiaires de l'aide humanitaire », *Disclos*e, 01/10/2021 https://disclose.ngo/fr/article/etat-renforce-controle-aide-humanitaire

[1219]« L'agence française de développement (afd) et les organisations de la société civile (osc), de 2009 à 2021 », Cour des comptes, S-2023-0502 https://www.ccomptes.fr/fr/documents/65037

[1220] « La politique de développement solidaire et de lutte contre les inégalités mondiales veille à assurer, lorsque cela est possible, la continuité entre les phases d'urgence, de reconstruction et de développement. L'action humanitaire, qui vise à secourir les populations vulnérables, et la préservation de l'espace humanitaire, qui constitue l'une des conditions majeures de cette action, s'inscrivent pleinement dans la politique de développement solidaire et de lutte contre les inégalités mondiales, selon des principes et modes d'action conformes au droit international humanitaire. » LOI n° 2021-1031 du 4 août 2021 de programmation relative au développement solidaire et à la lutte contre les inégalités mondiales https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043898536

[1221] BRABANT, Justine, FOUCHARD, Anthony, « L'État tente d'imposer le traçage des bénéficiaires de l'aide humanitaire », *Disclos*e, 01/10/2021 https://disclose.ngo/fr/article/etat-renforce-controle-aide-humanitaire

[1222] « In pushing back against problematic restrictions in funding agreements humanitarian actors can rely on a well-established and clearly articulated regulatory framework: IHL and humanitarian principles. In contexts where development activities are being conducted these are not applicable; consequently, it is necessary to rely upon arguments based on human rights law and development principles – and neither offers as firm a basis" GILLARD, Emanuela-Chiara, GOSWAMI, Sangeeta, VAN DEVENTER, Fulco, "Screening of final beneficiaries - a red line in humanitarian operations. An emerging concern in development work", *International Review of the Red Cross*, n° 916-917, February 2022 https://international-review.icrc.org/articles/screening-of-final-beneficiaries-a-red-line-in-humanitarian-operations-916

Coordination Sud plaide donc pour le retrait de ces lignes directrices,(« manifestement poussées par Bercy et Tracfin », commente le journal Le Monde)[1223].

Pour ce faire, les ONG ont donc posé un référé en urgence et un recours en annulation devant le Conseil d'État. Une double charge est reconnue : excès de pouvoir de la part du ministère des Affaires étrangères, qui ne serait pas légitime pour appliquer ces mesures, et l'absence de base légale de ces dernières. Selon un article du journal Le Monde : « Pour soutenir sa démarche, le gouvernement affirme qu'il met en œuvre les recommandations de l'Union européenne et de l'Organisation de coopération et de développement économiques en matière de lutte contre le financement du terrorisme, ce que dément le plus fermement Me Spinosi, selon qui les "personnes morales à but non lucratif n'entrent nullement dans le champ d'application de l'obligation de criblage". La France aurait surinterprété ces textes. L'avocat en voit pour preuve le fait qu'aucun autre pays européen n'a mis en place de telles obligations de criblage. »[1224] L'avocat a mis en avant l'urgence de supprimer ces lignes directrices, afin : « de ne pas avoir à appliquer cette mesure, les acteurs intéressés sont contraints soit de modifier substantiellement leurs propositions de projets, renonçant ainsi à tout ou partie des objectifs poursuivis par leur mission statutaire, soit de renoncer à solliciter le financement public. »

Mais le 31 mars 2022, Coordination Sud a reçu une ordonnance de rejet relative au recours en référé. Le Conseil d'État argue que ne sont concernés qu'une minorité des projets de l'AFD, que les mesures de criblages ne devaient être mises en œuvre qu'en juillet 2022. D'où une absence d'urgence pour l'agence[1225]. Un deuxième recours est donc déposé. Et celui-ci aboutit finalement à l'annulation des lignes directrices en matière de criblage. La réponse du Conseil d'État est qu' : « au motif que l'obligation de criblage n'existe pas en l'état du droit, et que les bailleurs institutionnels ne peuvent pas exiger la mise en œuvre d'une telle mesure par les OSC pour verser leurs subventions. (…) Dans ses travaux, le Conseil d'État a précisé qu'à la différence des institutions bancaires (entre autres), la loi ne prévoit pas de moyens spécifiques applicables aux OSC pour respecter les sanctions internationales et les mesures de gel des avoirs. Cette décision confirme la position des ONG. » Il est aussi stipulé que « l'obligation de criblage des bénéficiaires finaux apparaît injustifiée et disproportionnée dès lors qu'elle a un impact néfaste, d'une part, sur l'efficacité des actions des personnes morales à but non lucratif dans les États où elles interviennent, et d'autre part, sur la sécurité de leurs membres et interlocuteurs, portant ainsi atteinte aux droits et libertés fondamentaux tels que le droit d'aider autrui dans un but humanitaire et la liberté d'association. » [1226]

---

[1223] « La traçabilité de l'aide humanitaire débattue devant le Conseil d'État », *le Monde*, 16/03/2022 https://www.lemonde.fr/societe/article/2022/03/16/la-tracabilite-de-l-aide-humanitaire-debattue-devant-le-conseil-d-etat_6117709_3224.html

[1224] « La traçabilité de l'aide humanitaire débattue devant le Conseil d'État », *le Monde*, 16/03/2022 https://www.lemonde.fr/societe/article/2022/03/16/la-tracabilite-de-l-aide-humanitaire-debattue-devant-le-conseil-d-etat_6117709_3224.html

[1225]« Il résulte ainsi des simulations non contestées réalisées par le ministre de l'Europe et des Affaires étrangères dans le cadre de la présente instance que la quasi-totalité des projets financés par le centre de crise et de soutien du ministère et 70 % des projets de développement financés par l'Agence française de développement à l'initiative des organisations de la société civile ne sont pas concernés par la mesure de criblage contestée, laquelle ne sera mise en œuvre par l'Agence qu'à compter seulement de juillet 2022. « Conseil d'État, Juge des référés, 31 mars 2022, 461972, Inédit au recueil Lebon https://www.doctrine.fr/d/CE/2022/CE6C6FE8B76D4B23DDB2A5

[1226] Conseil d'État, 9ème - 10ème chambres réunies, 10/02/2023, 461486, Inédit au recueil Lebon https://www.legifrance.gouv.fr/ceta/id/CETATEXT000047121728

Les mesures de criblage n'étant plus imposées, d'autres modalités de contrôle des financements de l'aide humanitaire sont recherchées. D'après un rapport de la Cour des comptes en date de juin 2023 : « Les services compétents du Ministère de l'Europe et des Affaires étrangères, du Ministère de l'Economie et de l'AFD, en dialogue avec les représentants des OSC, ont donc repris les échanges sur une base différente : prise en compte des spécificités des acteurs et projets du développement par rapport aux acteurs/projets humanitaires, approche privilégiant l'analyse et l'atténuation des risques par les OSC en amont du financement du projet, audit par sondage. Cette approche devrait pouvoir être finalisée dans les prochaines semaines et notifiée à l'agence. Cela lui permettra de pouvoir continuer à respecter ses obligations en tant qu'organisme bancaire et celles de la France en matière LCB-FT, tout en responsabilisant les OSC qui ne se verront pas imposer le criblage systématique des bénéficiaires. »[1227]

Notons pour finir que cette ouverture contraste avec le climat plus général de resserrement du contrôle du monde associatif en France[1228], dans le cadre du contrat d'engagement républicain notamment[1229]. Cela dit, l'organisation Cartong indique que si les lignes directrices ont été annulées, dans les faits, la pression reste présente : « De plus en plus, des mesures de restriction à l'encontre des partenaires et des bénéficiaires sont demandées par les bailleurs de fonds, dans le cadre de la lutte contre le terrorisme ou de politique de sanctions. Les ONG françaises ont réussi en février 2023 à faire annuler les lignes directrices du gouvernement concernant le criblage des bénéficiaires, mais la pression à leur égard demeure, et d'autres bailleurs (comme l'USAID) continuent d'imposer le criblage. »[1230] Dernier point, l'annulation des lignes directrices n'a pas été suivie par le vœu de Françoise Bouchet Saulnier — ancienne directrice juridique de MSF international d'« intégrer une clause d'exemption humanitaire dans le droit pénal national » qui « est la seule façon de reconnaitre et de faire reconnaitre la légitimité et le statut protégé du personnel humanitaire sur les terrains de conflit. »[1231]

Ces négociations mettent en évidence la façon dont des acteurs étatiques tentent d'imposer leur lecture de la menace face aux ONG qui revendiquent alors une forme de légitimité à assurer la gestion du risque terrorisque sans en passer par des opérations de criblage des bénéficiaires et selon leur procédure respectant leurs propres principes éthiques. .

Et quant à nous, notons bien que dans l'ensemble des négociations et échanges, de nombreux arguments ont été invoqués en matière de respect du DIH, mais celui de la défense de la vie privée des bénéficiaires a été nettement moins cité. La mobilisation de coordination Sud s'est

---

[1227] L'agence française de développement (afd) et les organisations de la société civile (osc), de 2009 à 2021 », Cour des comptes, S-2023-0502https://www.ccomptes.fr/sites/default/files/2023-10/20230622-S2023-0502-AFD-et-organisations-societe-civile-rep-MEAE.pdf

[1228]PRADIER, Vincent, GRISARD, Roxane, » Le soutien sous contrôle des acteurs de la société cvile : le cas des organisations de solidarité internationale française et européennes », *Alternatives humanitaires,* 16/08/2022https://www.alternatives-humanitaires.org/fr/2022/08/16/le-soutien-sous-controle-des-acteurs-de-la-societe-civile-le-cas-des-organisations-de-solidarite-internationale-francaises-et-europeennes/

[1229] HOURDEAUX, Jérôme, « Le contrat d'engagement républicain, outil de mise au pas du monde associatif », *Mediapart,* 16/05/2024 https://www.mediapart.fr/journal/france/160524/le-contrat-d-engagement-republicain-outil-de-mise-au-pas-du-monde-associatif

[1230] « Le criblage et la traçabilité de l'aide », *Cartong*, 23/06/2023 https://cartong.pages.gitlab.cartong.org/learning-corner/fr/5_human_affected_pop_RD/5_5_screening

[1231] « Comment protéger les acteurs humanitaires dans le contexte des conflits armés anti-terroristes : relégitimer ou sanctionner ? », 27/11/2020, *Défis humanitaires* https://defishumanitaires.com/2020/11/27/lois-anti-terroristes-humanitaire/

inscrit dans des débats concernant la protection de l'espace humanitaire et l'indépendance des ONG. On trouve quelques références au fait qu'il faut éviter que les ONG soient perçues comme des « mouchards » pour ne pas les mettre en danger ou pour éviter de générer de la méfiance vis-à-vis des travailleurs humanitaires. Ceci ferait obstacle à l'allocation de l'aide et mettrait en danger les humanitaires. Les enjeux de protection des données sont donc formulés selon une problématique de sécurité et non pas selon le référentiel des droits de l'homme.

## Section 3 — L'impact en matière de protection des données des ONG des mesures de conformité bancaire relatives à la lutte contre le terrorisme

On a largement évoqué les pratiques des bailleurs, il est donc maintenant d'évoquer d'autres acteurs impliqués dans la lutte contre le financement du terrorisme : les banques. En effet, elles ont été chargées de mettre en place des mesures de vigilance raisonnables et de s'assurer que les fonds de leurs clients ne sont pas destinés à des organisations faisant l'objet de sanctions. Notre deuxième partie est consacrée aux enjeux de souverainetés étatiques. Mais la lutte contre le terrorisme implique également des acteurs privés. Et comme le surligne Anthony Amicelle, le renseignement financier serait symptomatique de nos sociétés de vigilance, impliquant la société civile dans des opérations sécuritaires, habituellement de l'ordre du régalien. Le rôle des GAFAM dans la lutte contre-terroriste est documenté, cela est moins le cas de celle des banques et des instituts financiers, qui occupent pourtant aussi une place — plus discrète — dans le capitalisme de surveillance[1232]. Mais Anthony Amicelle et Gilles Favarel Garrigues observent que ce sujet n'occasionne pas de large mouvement de contestation, et ce malgré l'existence d'enjeux en matière de droits humains[1233]. Les inquiétudes restent concentrées sur les listes de sanctions et les discriminations pouvant leur être associées. L'ambiguïté du sujet peut expliquer sa non-inscription à l'agenda militant : il se situe au croisement du secret bancaire et de la protection des données. Le mouvement droit l'hommiste est identifié~~s~~ par les chercheurs comme étant proche des anticapitalistes, peu enclins donc à militer pour moins de transparence bancaire. Au début des années 2000, un acteur s'y est cependant intéressé : la CNIL. Mais, elle serait restée pour Anthony Amicelle et Gilles Favarel Garrigues frileuse. Le contre-terrorisme est un dossier délicat. La Quadrature du Net, généralement plus offensive sur ces enjeux, ne s'en également est pas emparé. Notons cependant que Privacy international a publié différents rapports sur l'impact des recommandations du GAFI en matière de vie privée, sans que cela devienne une campagne de premier plan. Et surtout, comme on a commencé à le voir, les humanitaires se sont saisis du sujet. On a déjà évoqué différentes coalitions d'acteurs, à l'échelle nationale, régionale et internationale plaidant pour une exemption humanitaire aux mesures de lutte contre le financement du terrorisme. On a vu que des ONG se sont mobilisées afin d'être mieux prises en compte dans le régime de sanction onusien. On verra que les humanitaires tentent également de faire bouger les lignes en ce qui concerne les banques. Les ONG ont affaire à ces dernières pour transférer leurs fonds sur le théâtre des opérations, et mettre en place des programmes de transfert monétaire. Or, les opérations de vigilance raisonnable impliquent le

[1232] MALLARD, Grégoire, SUN, Jin, "Viral Governance: How Unilateral U.S. Sanctions Changed the Rules of Financial Capitalism",*American journal of sociology*, n°1 vol 128,2022

[1233] AMICELLE Anthony, FAVAREL-GARRIGUES Gilles, « La lutte contre l'argent sale au prisme des libertés fondamentales : quelles mobilisations ? », *Cultures & Conflits*, 2009/4 (n° 76), p. 39-66. https://www.cairn.info/revue-cultures-et-conflits-2009-4-page-39.htm

partage d'informations auprès d'instituts financiers. Ceci n'est pas sans enjeux en matière de protection des données. D'ailleurs, le cadre législatif de LCB/CT peut rentrer en contradiction avec le RGPD. On détaillera donc dans les lignes qui suivent comment les ONG perçoivent ces sujets.

## § 1 — Banques et contrôle du financement du terrorisme

Gilles Favarel Garrigues ainsi qu'Anthony Amicelle décrivent l'enrôlement de banques dans la gouvernance de la menace terroriste, et la collaboration de deux univers professionnels aux codes distincts, d'où un travail de traduction/intériorisation des exigences de contrôle des flux financiers qui ne s'est pas fait sans tensions, ajustements, etc. [1234] Au départ, il s'agissait pour les banques de mettre en place une simple activité de veille dans le cadre de la prévention du blanchiment d'argent. L'objectif des contrôles était de détecter des transactions sortant des normes établies, des mouvements de fonds suspects constituant la signature d'un échange frauduleux, sans qu'il y ait besoin d'imposer des mesures de confirmation des identités des clients. Il s'est cependant opéré une personnalisation grandissante des actions de surveillance. Les banques ont dû mettre en place un contrôle plus fin des mouvements financiers et de l'identité de leur clientèle. La lutte contre le terrorisme a été progressivement déléguée aux établissements financiers : « Ainsi est-on passé d'un régime global de prohibition à une autorégulation surveillée, qui laisse aux acteurs professionnels l'essentiel de la responsabilité d'une évaluation des risques fondée sur des outils qu'ils ont eux-mêmes construits. »[1235]

Les banques se sont alors dotées de dispositifs de surveillance, qui permettent d'identifier en amont des profils et des comportements suspects. Et afin d'opérer ce travail de détection, une industrie du logiciel d'analyse de données financières s'est développée. Cette dernière inclut des firmes comme World check, Logica Unilog, Mantas, SAS. Ces logiciels fonctionnent en recourant à plusieurs modèles de gestion de risque, qu'ont décrit Gilles Favarel Garrigue, Thierry Godefroy et Pierre Lascoumes[1236]. Ils peuvent être relativement « basiques », et reposer sur du filtrage de liste et sont donc prescriptifs : une occurrence détectée impose une décision, comme le fait de refuser un client. D'autres outils sont plus indicatifs et sont fondés sur des analyses comportementales. Certains outils ont recours à des techniques de « data mining ». Ils permettent de fouiller des séquences de données pour identifier des mouvements de fonds correspondant à des « patterns » de transactions récurrentes d'un

[1234] « L'imposition de principes hétéronomes au sein de l'industrie bancaire a des conséquences notables sur son fonctionnement et ses membres qui, pour continuer de faire affaire, doivent formellement être les yeux et les oreilles de l'État sécuritaire. Le recours aux machines soupçonnantes participe de la prise en compte et de l'intériorisation de ces principes de sécurité dans l'univers financier. Cela ne témoigne pas pour autant d'une indifférenciation des logiques — financières et sécuritaires — à l'œuvre, avec une mise en algorithmes des opérations de surveillance sous-tendue par des mécanismes, des instruments et des objectifs toujours en tension et rarement complémentaires. Il en ressort une politique du « ni trop ni trop peu » qui, si elle donne lieu à une surveillance automatisée, constante et généralisée, apparaît autant éloignée des ambitions répressives affichées que des visions dystopiques associées aux *big data.* »
AMICELLE, Anthony, « Policing & big data. La mise en algorithmes d'une politique internationale », *Critique internationale*, 2021/3 (N° 92), p. 23-48. https://www-cairn-info.ezproxy.utc.fr/revue-critique-internationale-2021-3-page-23.htm

[1235] FAVAREL-GARRIGUES Gilles, GODEFROY Thierry, LASCOUMES Pierre, « 2. D'une liste l'autre : les cibles des années 2000 », dans : FAVAREL-GARRIGUES Gilles, GODEFROY Thierry, LASCOUMES Pierre (dir), *Les sentinelles de l'argent sale. Les banques aux prises avec l'antiblanchiment*, Paris, La Découverte, « Cahiers libres », 2009, p. 49-62. https://www.cairn.info/les-sentinelles-de-l-argent-sale--9782707154217-page-49.htm

[1236] FAVAREL GARRIGUE, Gilles, GODEFROY, Thierry, LASCOUMES, Pierre, "Tools and securitization, the instrumentation of AML/CFT policies in French Banks", In HELGESSON, Karin Svedberg, MORTH Ulrika ed, *Accountability and risk management, transforming the public security domain*, London: Routledge, Taylor & Francis Group, 2012, 192 p. https://static1.squarespace.com/static/5e399e8c6e9872149fc4a041/t/624c339b2bb62359821fa1dd/1649161117463/Bit+By+Bit.pdf

compte. Certains outils sont fondés sur des algorithmes de clustering pour trier des comptes ayant des modalités de transactions similaires. D'autres utilisent de l'analyse de réseaux, pour déterminer des liens entre comptes, à partir du suivi de transferts de fonds. Ils reposent parfois sur des algorithmes d'analyse régressive pour prédire la possibilité qu'un compte soit utilisé pour du blanchiment d'argent. Un des objectifs est de constituer pour un détenteur de compte une côte de risque, construite à partir de différents critères : profession, zone géographique, activités ou intérêts à l'étranger, lien avec des pays à haut risque, antécédents judiciaires. Le fait d'avoir déjà fait l'objet d'une déclaration de soupçon joue aussi, ainsi que divers détails du compte et la nature des transactions passées.

D'après Anthony Amicelle, le problème majeur de ces outils reste la mauvaise qualité des données sur lesquels les logiciels construisent leurs modèles, d'où le besoin d'informations supplémentaires pour améliorer leur qualité et confirmer les analyses par des sources humaines, parfois policières[1237]. De surcroit, ces outils ne sont évidemment pas neutres et matérialisent la représentation d'une menace de ce que constitue pour les acteurs un risque financier, ainsi que les moyens de les réguler. Il s'agit aussi de fixer un seuil de risque tolérable, de déterminer un profil suspect à partir de mouvements bancaires, de périodes d'inactivités, de retrait de liquide, d'utilisation inhabituelle de chéquiers. Ces opérations de profiling tendent à produire des discriminations. Or, les faux positifs dans la détection de profils à risque ne sont pas rares. Et les agents de conformité bancaire n'en sont pas dupes, toujours selon les travaux d'Anthony Amicelle et Gilles Favarel Garrigues. Malgré des degrès d'adhésion parfois faible à ces outils, l'usage de ces derniers n'est pas nécessairement remis en cause, ce qui est pour les chercheurs significatif d'un besoin de conformité plutôt que d'efficacité. Cela ne signifie pas pour autant pour l'auteur que l'exercice est réduit à une simple opération strictement formelle : il a des effets directs sur les clients, qui peuvent être alors exclus du système bancaire.

En tout cas, ces logiciels permettent de se conformer aux obligations de « vigilance raisonnable » (« due dilligence » en anglais) qui sont définies comme suit : « Pour garantir que le système financier ne soit pas utilisé pour acheminer des fonds d'origine criminelle, les banques doivent s'efforcer, avec la diligence requise, de vérifier l'identité de tous les clients faisant appel à leurs services. Un soin particulier doit être mis à identifier le titulaire de chaque compte et les locataires de coffres. Toutes les banques doivent instaurer des procédures efficaces pour obtenir de leurs nouveaux clients la présentation de documents d'identité. Elles doivent se donner formellement pour règle qu'aucune opération significative ne soit effectuée avec des clients qui ne justifient pas de leur identité. » (*Déclaration de principes, Prévention de l'utilisation du système bancaire pour le blanchiment de fonds d'origine criminelle*, Comité de Bâle, décembre 1988).

La recommandation n° 10 du GAFI porte sur les opérations de « vigilance raisonnable » à mettre en place. Chaque pays peut déterminer la façon dont il impose ce type d'obligations. Une partie des opérations de « vigilance raisonnable » consiste simplement à connaitre le profil du client. En anglais, on parle d'opération de type « Know your client » (KYC). Les

[1237] FAVAREL GARRIGUE, Gilles, GODEFROY, Thierry, LASCOUMES, Pierre, *ibid.*

procédures de KYC passent par plusieurs étapes : identifier le client et vérifier son identité grâce à différents documents et données, obtenir des informations sur l'objectif et la nature des transactions effectuées sur les comptes.

Ces opérations peuvent requérir la collecte de documents d'identité du client, de son nom, de sa date de naissance, de son adresse, etc. Les recommandations du GAFI et les directives européennes de lutte contre le blanchiment d'argent laisseraient une marge de manœuvre sur le type d'informations à collecter[1238], qui diffère sensiblement d'un pays sur l'autre[1239]. D'autres informations peuvent être donc requises selon la législation de la banque, le degré de mise en œuvre des mesures, selon les profils des clients, le degré de soupçon dont ils font l'objet, selon le type de compte, le montant de transaction, selon différentes caractéristiques de l'organisation, et la localisation des transferts financiers. Les informations recueillies dans les opérations de devoir de vigilance doivent être conservées pendant au moins 5 ans, voire plus selon les recommandations du GAFI (cf. recommandation n° 10). Évidemment quand les transactions impliquent de transiter vers des pays à risques (ce qui peut être le cas pour les humanitaires), les procédures de diligence raisonnable peuvent être plus lourdes (cf. recommandation n° 19 du GAFI). Cela dit, la mise en place de telles mesures dans des pays en voie de développement reste inégale. Une minorité de pays du Sud sont considérés comme ayant un niveau de compliance substantiel et une mise en œuvre efficace des mesures de lutte contre le financement du terrorisme.

Autre point important à noter : différentes recommandations du GAFI visent à favoriser les échanges de données entre les acteurs de la lutte contre le financement du terrorisme. Par exemple, la recommandation n° 9 requiert que les opérations d'échange d'informations dans le cadre du renseignement financier ne soient pas bloquées par le secret bancaire ; la recommandation n° 40 requiert que doivent être facilités la coopération et l'échange d'informations à l'international. Les autorités compétentes devraient disposer de procédures claires et efficientes pour l'établissement des priorités et l'exécution en temps opportun des demandes, ainsi que pour la protection des informations reçues[1240].

En cas de profil prêtant à soupçon, les données collectées par les institutions financières sont partagées avec différents acteurs : d'autres banques, des cellules de renseignement financier, des policiers, voire des services de renseignement. En effet, les agents de conformité bancaire maintiennent un contact régulier avec le milieu des forces de l'ordre. Cette coproduction de renseignement financier est révélatrice du brouillage des frontières entre le régalien et le secteur privé et est propre aux formes de surveillances contemporaines. Et les canaux de transmission de données s'opèrent aussi de façon plus informelle, que ce soit à l'échelle nationale ou internationale[1241]. Selon le chercheur Anthony Amicelle, ce type d'échanges de

---

[1238]BREWCZYNSKA,Magdalena, KOSTA, Eleni, "From the fight against Money Laundering and financing of terrorism", in Matsumi, hideyuki, HALLINAN, Dara, DIMITROVA, Diana, KOSTA, Eleni, DE HERT, PAUL, *Data protection and privacy, Volume 15, in transitional Times*, 15th annual International Conference on Computers, Privacy and Data Protection (CPDP), Brussells, 2022

[1239] "Know Your Customer: Quick Reference Guide", January 2016, PWC https://www.pwc.com/gx/en/financial-services/publications/assets/pwc-anti-money-laundering-2016.pdf

[1240]« Normes internationales sur la lutte contre le blanchiment de capitaux et le financement du terrorisme et de la prolifération, les recommandations du GAFI », novembre 2023 https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/Recommandations%20du%20GAFI%202012.pdf.coredownload.pdf

[1241] AMICELLE, Anthony, "Migrant remittances in the face of securitization", In T. BASARAN, T, GUILD (eds.), *Global Labour and the Migrant Premium : The Cost of Working Abroad*, New York : Routledge,2018, p 101-110.

données avec les forces de l'ordre serait courant[1242], et leur informalité fait qu'ils tendraient à collecter plus d'informations que le prévoie le cadre juridique.

Ce dernier spécifie généralement que les agents de conformités doivent transmettre des Rapports de soupçon à une cellule de renseignement financier, dans le cas où ce dernier ait des raisons de douter de la licéité du client, des fonds et des opérations financières. Or, il ne serait pas toujours clair pour les agents de conformité quand ils doivent partager des rapports aux cellules de renseignement financier (CRF). Certains agents utilisent volontiers une parade : la multiplication des « déclarations parapluies » pour se couvrir [1243]. De surcroit, ces déclarations de soupçon sont confidentielles, et les clients ne peuvent y avoir accès, et l'identité des agents de conformité bancaires n'est pas révélée. Enfin, les directives européennes sur le LCB/FT accordent aux États la liberté de fixer la durée de conservation de ces documents, généralement établie à 5 ans en moyenne après la fin de la relation commerciale. Sachant que les directives ménagent la possibilité de renouveler cette durée de conservation pour cinq ans supplémentaires.

Les CRF ont trois tâches : la réception et l'analyse des rapports de suspicion qui lui sont transmis par les institutions financières, et la transmission de ces analyses aux autorités compétentes, définies par la loi. Les CRF sont tenues de coopérer à l'échelle internationale, notamment au sein du « groupe Egmont », qui facilite les échanges entre ses membres. Cette coopération se fait aussi via le dispositif FIU-NET (effectif depuis 2000). Il s'agit d'un système sécurisé et décentralisé (chaque pays reste détenteur et seul propriétaire de ses propres données) d'échange de données opérationnelles entre les CRF des États membres. Depuis 2016, la plateforme est intégrée à Europol. Les CRF peuvent ainsi recevoir des informations d'autres sources (administration d'États) et d'autres CRF. Point important : initialement, les CRF ne peuvent lancer une investigation que lorsqu'un rapport de soupçon est édité par une banque[1244].

## § 2 — Protection des données et contrôle du financement du terrorisme

[1242] FAVAREL-GARRIGUES, Gilles, GODEFROY, Thierry, LASCOUMES, Pierre, "Reluctant Partners ? Banks in the Fight against Money Laundering and Terrorism Financing in France." *Security Dialogue* 42, no. 2, 2011, p. 179–96. http://www.jstor.org/stable/26301759

[1243] AVAREL-GARRIGUES, Gilles, GODEFROY, Thierry, LASCOUMES Pierre, « 9. Les dilemmes pratiques de la LAB et la disciplinarisation du réseau », dans : FAVAREL-GARRIGUES Gilles, GODEFROY Thierry, LASCOUMES Pierre (dir.) , *Les sentinelles de l'argent sale. Les banques aux prises avec l'antiblanchiment*, Paris : La Découverte, « Cahiers libres », 2009, p. 185-200.

[1244] CARPENTIER, Jean-Baptiste, « Tracfin », in MOUTOUH, Hugues, POIROT, Jérôme, (dir.), *Dictionnaire du renseignement*, Paris : Perrin, 2018,1570 p.

SOUDAT, Théodore, "Tracfin : quelle place dans le monde du renseignement français? ", Portail IE, 02/01/2018 https://www.portail-ie.fr/univers/defense-industrie-de-larmement-et-renseignement/2018/tracfin-quelle-place-dans-le-monde-du-renseignement-francais/

D'emblée s'impose la question de l'articulation entre contreterrorisme et préservation du droit à la vie privée. Cette articulation peut s'envisager comme une balance, un équilibre à trouver, précaire et glissant, pouvant déboucher à un renoncement à la protection des droits des personnes concernées[1245]. Pour les autorités de protection des données européennes, il est nécessaire d'établir un cadre « proportionné » comprenant des garde-fous pour préserver les droits des individus. Reste à voir si ces garde-fous sont suffisamment solides et s'ils sont correctement mis en œuvre. En France, c'est dès 2003 que la CNIL s'est emparée des enjeux de protection des données associées à la lutte contre le blanchiment d'argent et le financement du terrorisme. Mais selon Antony Amicelle, l'engagement de cette dernière est resté limité, la CNIL n'investissant pas le terrain du contreterrorisme, un dossier au sujet duquel l'institution serait trop fragile. En outre, les problématiques de protection des données financières sont délicates. Et Anthony Amicelle s'interroge : « doit-on défendre le secret bancaire pour protéger les citoyens contre les excès de la surveillance gouvernementale ? L'existence de deux positions critiques difficilement conciliables, associées à des univers professionnels distincts, pèse sur le développement d'une mobilisation contre la surveillance opérée par les institutions financières privées au nom d'objectifs gouvernementaux. »[1246]

Cependant, lors des trois dernières années, le comité européen de protection de données (CEPD) a publié quelques documents de travail relatifs aux implications en matière de vie privée des mesures de LCB/CT. Privacy International a également en 2019 rédigé un rapport sur l'action du GAFI. Ces sujets ne sont pas au cœur de leur action de plaidoyer, mais les deux organisations y font part de leurs inquiétudes. D'autant que le cadre juridique en vigueur est loin de respecter le principe de proportionnalité : les différentes directives européennes [1247] ont progressivement élargi les possibilités de partage de données entre les acteurs impliqués. Ajoutons que les données traitées dans le cadre de la lutte contre le blanchiment d'argent et le financement du terrorisme sont évidemment extrêmement sensibles, et les données financières elles-mêmes peuvent en dire beaucoup sur un individu. Le CEPD estime à ce titre que le projet de directive européenne LCB/CT n'est pas assez protecteur. Le CEPD pointe le fait que l'article 55 de la proposition de loi de la 6e directive LCB/CT portée par la Commission européenne soit trop vague. Il autorise en effet le traitement de données sensibles si c'est « strictement nécessaire » dans le cadre de mesure AML/CFT. Or, la définition de la nécessité de ce dernier est laissée à la discrétion des responsables de traitement, ce qui laisse alors la porte ouverte à des collectes massives de données[1248].

Ajoutons que les chercheurs Winston Maxwell et Astrid Bertrand ont mis à l'épreuve les directives européennes LCB/CT à des « tests de proportionnalité ». Notons que l'obligation du caractère proportionné de ce type de traitement est évoquée par exemple dans le récital 19 du RGPD portant spécialement sur les opérations de lutte contre le blanchiment d'argent et

---

[1245]« Affaire du 8 décembre : le chiffrement des communications assimilé à un comportement terroriste », La Quadrature du net, 05/06/2023 https://www.laquadrature.net/2023/06/05/affaire-du-8-decembre-le-chiffrement-des-communications-assimile-a-un-comportement-terroriste/

[1246] AMICELLE, Anthony, FAVAREL-GARRIGUES, Gilles, **«** La lutte contre l'argent sale au prisme des libertés fondamentales : quelles mobilisations ? », *Cultures & Conflits*, 76, 2009,p. 39-66.

[1247] Cinq directives ont été votées en Europe depuis 1991 encadrant la lutte contre le blanchiment d'argent et le financement du terrorisme. Une sixième est en cours de vote.

[1248]FRASHER, Michelle, "Data protection and the EU's anti-money laundering regulation", IAPP, 23/11/2021 https://iapp.org/news/a/data-protection-and-the-eus-anti-money-laundering-regulation/

le financement du terrorisme[1249]. L'article 64 de la directive AML/CFT évoque également la même nécessité[1250]. Or, première évidence, les traitements de données opérés dans les opérations de LCB/CT sont massifs dans le sens où ils concernent potentiellement un nombre assez conséquent de personnes, soit l'ensemble des individus détenant un compte bancaire[1251]. Plus précisément, différents points paraissent problématiques aux chercheurs : la durée de conservation des données et le manque de transparence des traitements[1252]. Par voie de conséquence, il est difficile de s'assurer qu'un autre moyen moins intrusif peut être utilisé. En effet, les rapports d'activité des agents de conformité ne sont pas rendus publics ou communiqués aux personnes concernées, et ce pour ne pas remettre en cause le déroulé de l'enquête et pour protéger l'agent de conformité. Or, pour la Cours de justice de l'Union européenne (CJUE) les individus doivent être informés en cas de traitement des données dans le cadre d'une enquête pénale, notamment pour contre-terrorisme, une fois que cela ne fait plus obstacle au développement de l'enquête. Ce principe est également au cœur du RGPD [1253]. C'est d'autant plus le cas selon la CJEU pour de traitement automatique de données (ce qui peut être le cas dans le cadre de mesures d'AML/CFT)[1254]. Au regard de ces différents points, il parait pour les chercheurs évident que les directives européennes en matière de LCB/CT ne passent pas le test de proportionnalité prescrit par le RGPD.

Bien au contraire. Comme on l'a déjà vu, l'échange d'information est au cœur de la lutte contre le blanchiment d'argent et le financement du terrorisme ; la recommandation numéro 31 est d'ailleurs une porte ouverte à la collecte massive de données [1255]. La

---

[1249] « lorsque le traitement de données à caractère personnel par des organismes privés relève du champ d'application du présent règlement, celui-ci devrait prévoir la possibilité pour les Etats membres, sous certaines condition, de limiter par la loi certaines obligations et certains droits lorsque cette limitation constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir des intérêts spécifiques importants tels que la sécurité publique, ainsi que la prévention et la détection des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces. Cela est pertinent, par exemple, dans le cadre la lutte contre le blanchiment d'argent ou des activités des laboratoires de police scientifique. »

[1250] « Étant donné que l'objectif de la présente directive, à savoir protéger le système financier contre le blanchiment de capitaux et le financement du terrorisme par des mesures de prévention, de détection et d'enquête, ne peut pas être atteint de manière suffisante par les États membres, puisque l'adoption de mesures individuelles par les États membres pour protéger leurs systèmes financiers pourrait être incompatible avec le fonctionnement du marché intérieur, les règles de l'État de droit et l'ordre public de l'Union, mais peut, en raison des dimensions et des effets de l'action envisagée, l'être mieux au niveau de l'Union, celle-ci peut prendre des mesures, conformément au principe de subsidiarité consacré à l'article 5 du traité sur l'Union européenne. Conformément au principe de proportionnalité tel qu'énoncé audit article, la présente directive n'excède pas ce qui est nécessaire pour atteindre cet objectif.
(65) La présente directive respecte les droits fondamentaux et observe les principes reconnus par la charte, en particulier le droit au respect de la vie privée et familiale, le droit à la protection des données à caractère personnel, la liberté d'entreprise, l'interdiction de toute discrimination, le droit à un recours effectif et à accéder à un tribunal impartial, la présomption d'innocence et les droits de la défense. » DIRECTIVE (UE) 2015/849 DU PARLEMENT EUROPÉEN ET DU CONSEIL, du 20 mai 2015 https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32015L0849

[1251] MAXWELL, Winston, BERTRAND, Astrid, VAMPARYS, Xavier, "Are AI-based Anti-Money Laundering (AML) Systems Compatible with European Fundamental Rights?", ICML 2020 Law and Machine Learning Workshop, Jul 2020, Vienne, Austria.

[1252] PARAGI, Beata, Screening by international aid organizations operating in the Global South, mitigating risks of generosity, Springer, 2024

[1253] PARAGI, Beata, ibid

[1254] Concernant la nécessaire « explicabilité « des algorithmes, le fait d'être considéré comme des boites noires n'aide pas à respecter les exigences de transparence du RGPD. Tout dépend aussi du type d'algorithme. Sur ce point, Anthony Amicelle a une analyse plus nuancée : les algorithmes utilisés par les instituts financiers ne seraient pas d'une grande complexité (il ne s'agit pas d'algorithmes de types neurones profonds, plus complexes et opaques). D'où une possibilité de conserver une forme de transparence entre acteurs l'implantant (service informatique, agents conformités bancaires). Il n'est cependant pas question dans son article d'une éventuelle communication du fonctionnement de ces algorithmes aux clients. AMICELLE Anthony, « *Policing* & *big data*. La mise en algorithmes d'une politique internationale », *Critique internationale*, 2021/3 (N° 92), p. 23-48. https://www-cairn-info.ezproxy.utc.fr/revue-critique-internationale-2021-3-page-23.htm

[1255] Recommandation 31 du GAFI : « Les pays devraient s'assurer que les autorités compétentes qui mènent des enquêtes peuvent utiliser une vaste gamme de techniques d'enquêtes spécifiques adaptées aux enquêtes sur le blanchiment de capitaux, les infractions sous-jacentes associées et le financement du terrorisme. Ces techniques d'enquêtes comprennent : les opérations sous couverture, l'interception de communications, l'accès aux systèmes informatiques et la livraison surveillée. En outre, les pays devraient disposer de mécanismes efficaces

réglementation LCB/CFT va dans le sens d'un élargissement du type de données partagées, notamment entre cellules de renseignement financier. Selon la 5e directive AML/CFT datant de 2018, les cellules de renseignement financier peuvent exiger d'obtenir des données auprès des institutions financières même si aucun rapport d'activité suspicieuse n'a été émis. La directive 2019/1153 fluidifie encore davantage le cadre d'échange d'informations[1256]. De surcroit, la dimension multilatérale de la lutte contre le terrorisme joue aussi et influe sur le niveau de protection approprié en cas d'échange de données à l'international, notamment en cas de coopération judiciaire. Échanger des informations entre cellules de renseignement financier dans un pays ne disposant pas du même degré de protection accroit les risques de réutilisations de données de renseignement financier à d'autres finalités[1257].

Privacy international a soumis un rapport au GAFI allant dans le sens du CEPD. En substance, il est reproché à l'organisation internationale d'avoir favorisé l'émergence d'un vaste système de collecte de données, d'avoir recours au « reporting préventif » et au profilage d'individus en amont d'une suspicion avérée, et enfin de soutenir le développement de système d'identification invasif. D'autant que d'après Privacy international, les gouvernements vont au-delà de ce qui est nécessaire en matière de KYC, entrainant des dérives en matière de protection des données[1258].

On peut citer un autre gros point d'inquiétude pour Privacy International : l'influence du GAFI sur l'adoption de système d'identité pour assurer les opérations de KYC. L'organisation n'impose pas un type d'identification en particulier, mais édicte des recommandations et de la « soft law ». Ces avis poussent à l'adoption de dispositifs d'identification jugés comme « fiables », comme la biométrie, considérée par le GAFI comme étant un des moyens les plus surs d'identification. En réaction, Privacy International plaide pour un assouplissement des standards d'identification, en raison de la nécessaire protection de la vie privée des individus, mais aussi pour favoriser l'inclusion financière de personnes dépourvues de papiers d'identité.

En 2017, le GAFI édicte un cadre plus souple, mais sans adresser le fond du problème. L'organisation plaide pour l'adoption de dispositifs d'identité invasifs, reposant sur des données biométriques. Le GAFI supporte par exemple des initiatives comme Aadhaar, une base de données biométrique indienne ainsi que son dispositif de KYC numérique. Pour

leur permettant de déterminer en temps opportun si des personnes physiques ou morales détiennent ou contrôlent des comptes. Ils devraient également assurer que les autorités compétentes disposent d'un mécanisme d'identification des biens sans notification préalable au propriétaire. Lors de la conduite d'enquêtes sur le blanchiment de capitaux, les infractions sous-jacentes associées et le financement du terrorisme, les autorités compétentes devraient pouvoir demander toutes les informations pertinentes détenues par la CRF » « Normes internationales sur la lutte contre le blanchiment de capitaux et le financement du terrorisme et de la prolifération, les recommandations du GAFI », novembre 2023
https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/Recommandations%20du%20GAFI%202012.pdf.coredownload.pdf

[1256] EU context of anti-money laundering and countering the financing of terrorism https://finance.ec.europa.eu/financial-crime/eu-context-anti-money-laundering-and-countering-financing-terrorism_en

[1257]"FATF Guidance, private sector information sharing", november 2017, https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Private-Sector-Information-Sharing.pdf.coredownload.pdf

[1258]" Submission to the financial action task force public consultation on FATF draft guidance on digital identity", *Privacy international*, november 2019 https://privacyinternational.org/sites/default/files/2020-11/PI%20submission%20FATF_November%202019.pdf

Privacy International : « le discours actuel du GAFI met davantage l'accent sur l'inclusion financière que le régime précédent, mais conserve la même approche basée sur le risque. »[1259]

Autre point important en matière de protection des données : la surveillance des flux financiers implique un brouillage des frontières entre privé et public en matière de politique sécuritaire, ce qui n'est pas sans effets en matière de protection des données[1260]. Le renseignement financier passe ainsi par l'implication d'acteurs n'appartenant pas a priori au secteur sécuritaire, comme des banques, ou des éditeurs de logiciels, ou des firmes spécialisées dans le risque financier, comme Acxiom, Choicepoint ou Lexis Nexis, Thompson Reuters, etc. Pour effectuer leur travail, les agents de conformité peuvent dépendre de sources externes, également des « watchlist » qui sont procurées par des sous-traitants. Ces firmes se spécialisent dans l'analyse de données massives, leurs outils permettent de vérifier si telle ou telle personne ne représente pas un risque financier, en se basant sur des listes préétablies ou en constituant leurs propres listes [1261], notamment de personnes « politiquement exposées »[1262]. Le CEPD enjoint aux banques de s'assurer de l'exactitude des données contenues dans ces listes, régulièrement dénoncées pour leur manque de transparence et leur caractère parfois erroné [1263]. Et ce type d'entreprise représente de véritables « pots de miel » pour les services de renseignement, soit une porte ouverte à la possibilité d'une réutilisation de données à d'autres finalités, d'autant que les frontières entre les deux mondes professionnels peuvent être minces [1264]. Ajoutons que le journal d'investigation The Intercept a révélé l'existence d'échange de données entre l'entreprise de renseignement financier — Thomson Reuters Corporation — et l' agence fédérale de contrôle de migration américain, l'Immigration and Customs Enforcement (ICE), qui dépend du département de la sécurité intérieure des USA[1265]. Il n'est donc pas étonnant que Thomson Reuters ait pu nouer en 2010 un partenariat avec la firme décriée Palantir, afin de développer un logiciel d'analyse de données massives financières, QA Studio [1266].

---

[1259] « The current discourse from FATF places more emphasis on financial inclusion than the earlier regime, but still retains the same risk-based approach. »
Submission to the financial action task force public consultation on FATF draft guidance on digital identity, Privacy international, november 2019 https://privacyinternational.org/sites/default/files/2020-11/PI%20submission%20FATF_November%202019.pdf

[1260] AMICELLE, Anthony, « *Policing* & *big data*. La mise en algorithmes d'une politique internationale », *Critique internationale*, 2021/3 (N° 92), p. 23-48. https://www-cairn-info.ezproxy.utc.fr/revue-critique-internationale-2021-3-page-23.htm

[1261] HAYES, B. « Spying in a see- through World: the 'Open Source' intelligence industry », *Statewatch Journal*, 2010, vol. 20 no. 1.

[1262] Une personne exerçant (ou ayant exercé) une haute fonction publique, ou qui est intimement associée à une telle personne. Du fait de cette fonction et de l'influence qu'elle peut avoir, on postule qu'il y a un risque qu'une PPE soit impliquée dans la corruption
Personne politiquement exposée, Wikipedia, https://fr.wikipedia.org/wiki/Personne_politiquement_expos%C3%A9e

[1263] Opinion 12/2021, on the anti-money laundering and countering the financing of terrorism ( AML/CFT) package of legislative proposals, EDPS, 22/09/2021https://edps.europa.eu/system/files/2021-09/21-09-22_edps-opinion-aml_en.pdf

[1264] Concernant la firme Thomson Reuteurs, cela est flagrant. Son équipe est en effet composée en partie d'anciens membres de services de renseignement, de l'agence de contrôle des frontières américaines, l'Immigration and Customs Enforcement Agency (ICE), et du département de la Défense américain.

[1265]"Press release: Privacy international asks Thomson Reuters if it will stop facilitating the US government's "zero tolerance" policy", *Privacy International*, 21/06/2018 https://privacyinternational.org/press-release/2078/press-release-privacy-international-asks-thomson-reuters-if-it-will-stop « Documentation shows that Thomson Reuters Corporation is selling access to highly sensitive and personal data to the US Immigration and Customs Enforcement (ICE) agency, the authority responsible for implementing the US government's zero tolerance immigration policy, including the separation of families at detention centres" CURRIER, Cora, "Lawyer and scholars to lexisnexis, Thomson Reuters : stop helping ICE deport people", *The Intercept*, 14/11/2019 https://theintercept.com/2019/11/14/ice-lexisnexis-thomson-reuters-database/
JAHLAWAT, Archana, ORTIZ, Ana, SHAH, Anuj," The data broker to deportation pipeline : how Thomson Reuters & LexisNexis Share utility & commercial data with ICE", 2021

[1266] Thomson Reuters QA studio powered by Palantir https://www.thomsonreuters.com/content/dam/openweb/documents/pdf/tr-com-financial/fact-sheet/qa-studio.pdf

Tout ceci à plusieurs conséquences en matière de protection des données. Tout d'abord, selon qu'on a affaire à un acteur privé ou public, le cadre législatif n'est pas le même. Et les chercheurs ne s'accordent pas sur le type de loi à appliquer aux traitements de données effectuées dans le cadre d'opérations de LCB/CT : faut-il se référer au RGPD ou à la directive Police/Justice[1267] ? Les banques, en tant qu'acteurs privés, devraient appliquer le RGPD, mais le brouillage de leur rôle, leur implication dans des actions de renseignement financier, et leurs interactions accrues avec des agences policières complexifient cette question[1268]. Quant aux cellules de renseignement financier, leur statut juridique varie de pays en pays, d'où un manque d'homogénéité du cadre à appliquer[1269]. Ce point est d'autant plus problématique en cas de transferts de données à l'international et de transfert de données d'organisation privées (une ONG par exemple) à une banque et/ ou à une cellule de renseignement financier. Clarifier cette question est donc primordial : la directive Police/Justice laisse la possibilité de limiter les droits des personnes concernées, dans des conditions bien spécifiques, les personnes doivent notamment être informée des traitements de données les concernant.

## §3 — Humanitaire, banque et contrôle du financement du terrorisme

On a donc un premier aperçu du monde du renseignement financier. Reste maintenant à voir quelle est la place du secteur de la solidarité internationale dans ce paysage. Tout d'abord, les humanitaires — du fait qu'ils ont été associés par les organisations d'AML/CT à un profil à risque — connaissent des difficultés de gestion de leurs fonds : les banques sont tendanciellement réticentes à entretenir des relations commerciales avec les ONG humanitaires. Elles adoptent des mesures de « de-risking »[1270], soit des stratégies d'évitement de risque, qui vont parfois jusqu'au refus d'ouverture de compte ou à leur fermeture. Ce phénomène est renforcé par le manque de clarté du cadre législatif, la marge de manœuvre laissée aux agents de conformité bancaire, la crainte de la sanction, le manque de connaissance du secteur humanitaire par les institutions financières, les propres préconceptions des banques et des représentations parfois simplifiées du réel et des zones de crises, etc. Pour faire court, les facteurs de « derisking » des banques d'après le chercheur

[1267] DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces donnée https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX%3A32016L0680
BREWCZYŃSKA, Magdalena, KOSTA, Eleni, « From the Fight Against Money Laundering and Financing of Terrorism Towards the Fight for Fundamental Rights: Role of Data Protection » Tilburg Law School Research Paper nr. 2/2023, https://ssrn.com/abstract=4328464

[1268] « Garanties pour les partenariats publics-privés en matière de surveillance », *Privacy international*, décembre 2021 https://privacyinternational.org/sites/default/files/2022-05/PI%20PPP%20Safeguards%20FR.pdf

[1269] QUINTEL, T. « Data protection rules applicable to Financial Intelligence Units: still no clarity in sight », *ERA Forum* 23, 53–74,2022.

[1270] "Les banques s'engagent dans le "de-risking" en cessant de s'engager dans des types d'activités considérées comme plus risquées de manière générale, plutôt que d'évaluer les risques des clients au cas par cas.
au cas par cas. Les banques peuvent agir rationnellement en ne servant pas certains types de clients, en raison de divers facteurs. Cependant, la mise en œuvre de la LBC/FT semble avoir créé des catégories de clients dont l'activité ne peut justifier les coûts de mise en conformité associés. "Banks are engaging in "de-risking" by ceasing to engage in types of activities that are seen to be higher risk in a wholesale fashion, rather than judging the risks of clients on a case-by-case basis. Individual banks may be acting rationally in not serving certain types of clients, due to a variety of factors. However, the implementation of AML/CFT appears to have created categories of clients whose business cannot justify the associated compliance costs. The financial exclusion of such clients creates yet another obstacle for poverty alleviation and economic growth, especially in poor countries."
LOWERY, C. (Chair), "Unintended Consequences of Anti-Money Laundering Policies for Poor Countries", A CDG Working Group Report. Center for Global Development, 2015

Stuart Gordon sont les suivants : l'absence ou le manque d'infrastructure bancaire établie (comme en Afghanistan, en Syrie, Somalie, Corée du Nord, etc.) ; des sanctions (Syrie, Iran) ; l'existence de conflits ou de groupes terroristes (Syrie, Afghanistan, Somalie, Nigeria, Gaza, Mali) ; la proximité de ce type de zone, ou des zones servant de corridor d'accès à des zones d'instabilité (entre la Jordanie et la Turquie en tant que zone d'accès à la Syrie) ; le fait d'être une ONG locale et peu connue de banques, d'être une ONG de confession musulmane [1271]. La possibilité d'ouverture de compte dépend aussi du degré d'internalisation d'une banque : plus une banque est internationalisée, plus elle tendrait — du moins selon les rapports sur le sujet — à respecter le cadre législatif et les standards globaux [1272]. Les ONG humanitaires représenteraient trop de risques, engager des relations commerciales avec ce type d'acteur serait trop couteux et rapporterait trop peu d'avantages matériels en retour[1273].

Par voie de conséquence, les humanitaires tentent en réaction soit de créer des liens de confiance avec les bailleurs et les banques, soit de changer d'institutions financières ou d'utiliser d'autres canaux financiers que les banques traditionnelles (hawala ou espèces liquides), et de faire des transferts par petites sommes, etc. Il peut aussi arriver que les ONG renoncent aux programmes de transferts monétaires, passent à de l'aide en nature, ou encore suppriment des programmes, au détriment des bénéficiaires[1274].

---

[1271] GORDON, S., ROBINSON, A., GOULDING, H., MAHYUB, R., "The risk of de-risking: the impact of counterproductive financial measures on the humanitarian response to the Syrian crisis", *HPG Working papers*, 2018http://eprints.lse.ac.uk/102025/1/crp_2019_03_20_the_risk_of_de_risking_the_syrian.pdf
GORDON, Stuart, ROBINSON, Alice, GOULDING, Harry, MAHYUB, Rawaad, "The impact of bank de-risking on the humanitarian response to the Syrian crisis", Humanitarian Policy Group, August 2018, https://www.calpnetwork.org/wp-content/uploads/2020/03/the-impact-of-bank-de-risking-on-the-humanitarian-response-to-the-syrian-crisis-1.pdf
EL TARABOULSI-MCCarthy, Sherine, "WHose risk? Bank-risking and the politics of interpretation and vulnerability in the Middle East and North Africa", *International Review of the Red Cross*, 2021, 103 (916-917), p.747-762
[1272] DURNER, Tracey, SHETRET, Liat, "Understanding bank de-risking and its effects on financial inclusion",Global center on cooperative security, November 2015 https://www-cdn.oxfam.org/s3fs-public/file_attachments/rr-bank-de-risking-181115-en_0.pdf
MORET, Erica," Safeguarding humanitarian banking channels : how, why and by whom?", Norwegian Refugee Council, January 2023, https://www.nrc.no/globalassets/pdf/reports/safeguarding-humanitarian-banking-channels/safeguarding-humanitarian-banking-channels.pdf
WALKER, Justine, "Risk Management Principles Guide for Sending Humanitarian Funds into Syria and Similar High-Risk Jurisdictions", May 2020, http://files.acams.org/pdfs/2020/The-Risk-Management-Principles-Guide-for-Sending-Humanitarian-Funds-into-Syria-and-Similar-High-Risk-
WALKER, Justine, "Risk management principles guide for sending humanitarian funds into Syria and similar high risk juridictions", Geneva Graduate Institution, may 2020 https://www.graduateinstitute.ch/research-centres/global-governance-centre/compliance-dialogue-syria-related-humanitarian-payments
MORET, Erica, "life and death: NGO access to financial services in Afghanistan", NRC January 2022, https://www.nrc.no/globalassets/pdf/reports/life-and-death/financial-access-in-afghanistan_nrc_jan-2022.pdf
MALLARD, G., SABET, F.,SUN, J."The Humanitarian Gap in the Global Sanctions Regime: Assessing Causes, Effects, and Solutions", *Global Governance: A Review of Multilateralism and International Organizations*, *26*(1), p.121-153. https://doi.org/10.1163/19426720-02601003
[1273] BURNISKE, Jessica S., MODIRZADEH, Naz K., "Pilot Empirical Survey Study on the Impact of Counterterrorism Measures on Humanitarian Action", Cambridge, MA: Harvard Law School Program on International Law and Armed Conflict, 2017.
HAUSMANN, Paul, PEARSON, Elodie, "Assessing the impact of sanctions on humanitarian work", Geneva Graduate Institute, December 2022, https://voiceeu.org/publications/assessing-the-impact-of-sanctions-on-humanitarian-work.pdf
"Detrimental impacts: how counter-terror measures Impede humanitarian action", Interaction, April 2021https://www.interaction.org/wp-content/uploads/2021/04/Detrimental-Impacts-CT-Measures-Humanitarian-Action-InterAction-April-2021.pdf
ALTMAN, Jonathan, CACHAY, Brenda, MILLER, Zach, MORNEAU, Clare, MOSCOSO, Nico, ORIENTALE, Steven, "Using data to understand the impact of AML/CFT sanction on the delivery of aid : the perspective of Nonprofit organizations", January 2021
[1274] MORET, Erica, "Safeguarding Humanitarian Banking Channels: How, Why and by Whom?" , NRC,January 2023 https://www.nrc.no/globalassets/pdf/reports/safeguarding-humanitarian-banking-channels/safeguarding-humanitarian-banking-channels.pdf

## § – 4 Les enjeux de protection de données des transferts monétaires et mesures de conformité bancaire dans l'humanitaire

Évoquons maintenant un peu plus précisément les conséquences des mesures de LCB/CT sur les programmes de cash transferts. Ces derniers nécessitent en effet des transferts de fonds entre ONG et bénéficiaires, et donc des interactions avec des institutions financières.

Les transferts monétaires peuvent être reçus sur un téléphone, prendre la forme d'un porte-monnaie numérique, d'une carte de retrait. Ils peuvent se faire sous la forme de coupons électroniques ou non, être restrictifs ou non. Et évidemment, les plateformes peuvent voir là une opportunité de marché : Facebook s'était notamment positionné sur les monnaies virtuelles, en ciblant également le secteur de la solidarité internationale [1275]. Selon le contexte, les prestataires de services financiers peuvent être des entreprises émettrices de coupons électroniques, des établissements financiers (des banques et des institutions de microfinance, par exemple) ou des opérateurs de réseau mobile.

C'est dans les années 2000 que ces types de projet commencent à émerger, favorisés par l'augmentation de la connectivité en téléphonie mobile. Ils connaissent une légère augmentation dans les années 2010. Dans un bilan effectué en 2014[1276], il apparaissait qu'ils étaient encore utilisés par une minorité d'ONG, mais depuis ce type de dispositif est utilisé de façon croissante, et compterait selon un rapport de décembre 2022 pour 19 % des projets humanitaires[1277]. Deux grosses ONG concentrent les opérations de transfert monétaire : le WFP, l'UNHCR, et dans une certaine mesure l'IFRC et le CICR. À titre indicatif, précisons qu'en 2020 le WFP a envoyé 2, 1 millions de dollars via des dispositifs de cash transfert, dans 67 pays, dont 25 en programme de téléphonie mobile. Et l'UNHCR a envoyé 700 millions de dollars via des programmes de transferts monétaires dans 100 pays, dont 47 en transfert électronique, et 15 qui reposent sur de la téléphonie mobile[1278].

Une des conditions des programmes de transfert monétaire est de pouvoir utiliser un compte bancaire. Et cela nécessite donc de devoir partager un certain nombre d'informations avec les banques. Ils sont donc associés à de nombreux enjeux de protection des données du fait de l'application de mesures de vigilance raisonnable[1279]. Privacy International — qui a produit un

---

[1275] KAURIN Dragana, "Why Libra Needs A Humanitarian Fig Leaf", *Medium*, 2019 https://medium.com/berkman-klein-center/why-libra-needs-a-humanitarian-fig-leaf-79ae6a463c8

[1276] HUTTON, Josephine, BOESER,Shawn, GROOTENHUIS, Floor, "A Review of Cash Transfer Programming and the CALP Network 2005–2015 and Beyond, 2014", Calp Network. https://www.calpnetwork.org/publication/a-review-of-cash-transfer-programming-and-the-cash-learning-partnership-calp-2005-2015-and-beyond/

[1277] KREIDLER Corinna, TAYLOR Glyn, "Where next? The evolving landscape of cash and voucher policies", December 2022. https://www.calpnetwork.org/publication/where-next-the-evolving-landscape-of-cash-and-voucher-policies/ D'après ce rapport l'aide humanitaire reposerait pour 19 % sur du cash transfert.

[1278] AWANIS Aramé,LOWE Christopher, ANDERSSON-MANJANG Simon K., LINDSE, Doninica, "State of the Industry Report on Mobile Money", GSMAhttps://www.gsma.com/sotir/wp-content/uploads/2022/03/GSMA_State_of_the_Industry_2022_English.pdf

[1279] "data responsibility in cash and voucher assistance, Guidance note series data responsibility in humanitarian action", the Centre for humanitarian data, OCHA, December 2020https://data.humdata.org/dataset/repository-for-pdf-files/resource/a1379937-5165-46f1-8bf0-b99ea7c0bb26/download/guidance_note_cash_voucher_assistance.pdf

rapport sur le sujet — donne l'exemple suivant : pour un programme de cash transfert, un bénéficiaire a dû partager des données personnelles du fait de mesures de type KYC. Or il se trouve que cette personne a fui son pays d'origine pour trouver refuge dans un autre État. Et la nouvelle banque peut partager des données avec l'ancienne banque. Cette dernière peut alors en déduire où se situe son ancien client. Et ce type d'information peut être échangé avec d'autres agents financiers ou policiers. Pour les ONG, il ne s'agit pas simplement d'une problématique de défense de la vie privée des bénéficiaires, mais d'une problématique de protection. On peut ainsi lire dans un rapport du CICR : « Les préoccupations en matière de protection concernent notamment l'exclusion des personnes des programmes d'assistance parce qu'elles figurent sur certaines listes ou que leur localisation les désigne comme hostiles aux autorités d'une manière ou d'une autre. »[1280]

Cela dit, le risque de se trouver sur des listes de sanctions est considéré comme minime par certaines ONG. Cela est vrai pour les listes internationales, comprenant généralement des responsables d'organisations terroristes[1281]. Le cas des listes nationales est différent, au regard de leur opacité et de leur instrumentalisation potentielle, il est plus difficile d'anticiper le risque qu'un bénéficiaire puisse s'y retrouver.

De surcroit, comme l'a montré Privacy International, les répercussions des mesures de KYC en matière d'atteinte à la vie privée sont avérées, et le Caplenetwork et le CICR ont produit différentes recommandations pratiques pour les atténuer. Les organisations énumèrent tout un ensemble de questions à se poser avant l'ouverture d'un tel programme : est-ce que le gouvernement en place mène une politique de discrimination politique et/ou ethnique et/ou religieuse envers une minorité ? Le simple fait de révéler qu'elles ont eu recours à de l'aide humanitaire peut être dans certains cas discriminant et révéler que la personne fait partie de telle ou telle minorité, potentiellement persécutée. Est-ce qu'il y a des opposants à un régime parmi les bénéficiaires ? Un bénéficiaire appartient-il à un parti politique considéré comme terroriste ? Est-ce que les services financiers sont liés aux autorités étatiques, aux services de renseignement ou aux forces de l'ordre ? Si les bénéficiaires sont des réfugiés : est-ce que le service financier a une branche dans le pays d'origine de la personne exilée où les données

---

"cash feasibility assessment", Cash working group, North West Syria, Calpnetwork, 2020 https://www.calpnetwork.org/wp-content/uploads/ninja-forms/2/IOM_CFA_external_final_compressed.pdf https://www.calpnetwork.org/wp-content/uploads/ninja-forms/2/IOM_CFA_external_final_compressed.pdf

RAVAGNANI, Martina, NEWHOUSE, Nina, COUPE, Hannah, LUCAS, Elle, MMAH, Otobong," Beneficiary screening for humanitarian cash and voucher assistance : a comparative assessment", London School of Economics and political Science", Oxfam, 2021https://www.calpnetwork.org/wp-content/uploads/ninja-forms/2/OxfamBONDLSE_2021_BeneficiaryScreeningCVA.pdf

BAILEY, Sarah, GORDON, Laura, "Humanitarian cash transfers and the private sector", background note for the high level panel on humanitarian cash transfers", may 2015 https://documents.wfp.org/stellent/groups/public/documents/op_reports/wfp278451.pdf

[1280]"Protection concerns here include people's exclusion from assistance programmes because they appear on certain lists or their location marks them out as hostile to the authorities in some way."SLIM, Hugo, BANFIELD, Rachel, SOULEYMANE ADENHOF, Thierno, BURTON, Jo, "cash transfer programming in armed conflict: The ICRC's experience", ICRC, 2018 https://resources.peopleinneed.net/documents/594-4359-002-cash-transfer-programming-upd-1-11-2018-web-1-.pdf

[1281] "The majority of the Rohingya population comprise of families and children which reduces the risk of sanctioned persons. However, like in any CDD process, sanction and criminal lists should be checked by the FSP to exclude this potential risk as required by Bangladesh law. Politically exposed persons: As Rohingyas are not recognized as citizens of Myanmar, they do not have political rights. The risk of finding politically exposed persons within the Rohingya population in Bangladesh is minimal. To minimize the risk, the name of the beneficiary should be checked in the PEP list by the FSP as required by Bangladesh law. " "Money Laundering & Terrorist Financing Risk Management Guidelines", Bangladesh Bank, Sept. 2015, p.65.

"TIP sheet, know your customer regulation, electronic cash transfer learning action network", Calpnetwork, September 2020, https://www.calpnetwork.org/wp-content/uploads/2020/09/KYC-tipsheet.pdf

pourraient être demandées par les autorités ? Est-ce que les bénéficiaires ont exprimé des craintes que leurs données soient partagées avec des autorités[1282] ?

Différentes solutions de minimisation de risque sont envisagées, elles reposent surtout sur des stratégies de contournement des mesures de KYC. Par exemple, il est possible d'utiliser un compte déjà actif du bénéficiaire, comme le conseille le CICR : « le CICR s'efforce, dans la mesure du possible, de faire appel à des prestataires de services financiers auprès desquels les personnes possèdent déjà un compte personnel, de sorte qu'elles connaissent les services et s'y sentent à l'aise, qu'elles aient déjà satisfait aux exigences KYC et qu'on ne leur demande pas de faire confiance à des systèmes qui ne leur sont pas familiers. Si le problème réside dans le fait que les personnes ne peuvent pas satisfaire aux exigences KYC, il peut s'avérer plus difficile à résoudre. » [1283] Sachant qu'ouvrir un nouveau compte est considéré comme plus risqué : « la création de nouveaux comptes par la Société nationale pour des bénéficiaires individuels, à supposer que cela soit possible, devrait être analysée plus en détail afin de déterminer les risques éventuels en matière de protection des données. » [1284] Et enfin, il peut être envisagé d'ouvrir des comptes « par procuration » : « Les comptes virtuels sont détenus et gérés par l'organisation humanitaire qui peut créer des sous-comptes pour les bénéficiaires afin de leur permettre de recevoir de l'argent. Avec de tels comptes, l'identification des clients est effectuée par l'organisation et non par les bénéficiaires individuels. »[1285] Des données de bénéficiaires peuvent toujours être partagées durant le programme, mais dans une moindre mesure : « les données relatives aux bénéficiaires peuvent encore devoir être communiquées au service financier à des fins d'identification au moment du versement de l'argent, mais la quantité de données à communiquer au service financier est généralement réduite par rapport à la création de comptes nominatifs, car il n'est pas nécessaire d'établir un système de connaissance du client avec les personnes concernées. »[1286] Cette démarche peut être compliquée à mettre en place, et les travailleurs humanitaires peuvent avoir accès aux données du bénéficiaire, ce qui est moins risqué, mais reste invasif[1287].

Les ONG peuvent tenter d'obtenir une série de garanties par les banques (dont certaines vont à l'encontre des recommandations du GAFI). Il est ainsi conseillé de négocier les exigences en matière de KYC, notamment pour les personnes n'ayant pas de documents d'identité, et chercher à réduire les échanges de données. Il est possible de faire en sorte que l'institut bancaire ne partage pas de données à d'autres acteurs sans l'approbation de l'ONG, ou du

---

[1282]« Global learning event cash transfer programming and preparedness, Hosted by the International federation of Red Cross and Red Crescent societies in partnership with the Cash learning partnership", Kuala Lumpur, 25 and 26 july 2013 https://preparecenter.org/wp-content/sites/default/files/learning-event-report-final.pdf
"Practical guidance for data protection in cash and voucher assistance, a supplement to the cash in Emergencies toolkit", January 2021 https://cash-hub.org/wp-content/uploads/sites/3/2021/01/CVA-Data-Protection-Guidance-final.pdf

[1283] « the ICRC, where possible, tries to use financial service providers that people already hold personal accounts with, so that they are familiar and comfortable with the services, have already met the KYC requirements and are not being asked to trust unfamiliar systems. If the issue is that people cannot meet the KYC requirements, this can be harder to resolve. »BURTON, Jo, ""Doing no harm" in the digital age: what the digitalization of cash means for humanitarian action", *International review of the Red Cross*, n°913, 2021https://international-review.icrc.org/articles/doing-no-harm-digitalization-of-cash-humanitarian-action-913

[1284] "The creation of new accounts by the National Society for individual beneficiaries, assuming this is feasible, should be analysed in more detail to determine possible data protection risks."ibid.

[1285] "Virtual accounts are owned and managed by the humanitarian organization where they could create sub-accounts for beneficiaries to allow them to receive cash. With such accounts, the KYC is done with the organization and not the individual beneficiaries." "Practical guidance for data protection in cash and voucher assistance, a supplement to the cash in emergencies toolkit", IFRC, January 2021https://cash-hub.org/wp-content/uploads/sites/3/2021/01/CVA-Data-Protection-Guidance-final.pdf

[1286] "Beneficiary data may still need to be shared with the FSP for identification purposes at the time of cash disbursement, but the amount of data to share with the FSP is generally reduced compared to creating named accounts because KYC is not being established with the individuals. Ibid. https://cash-hub.org/wp-content/uploads/sites/3/2021/01/CVA-Data-Protection-Guidance-final.pdf

[1287] Ibid.

moins de faire en sorte que l'ONG en soit informée avant les autorités. Il est recommandé de demander directement aux cellules de renseignement le type de profil pouvant être labélisé comme étant « suspect ». Privacy international rappelle ainsi que : « pour anticiper de tels scénarios, les organisations humanitaires devraient systématiquement demander aux cellules de renseignement financier davantage d'informations sur la manière dont les transactions sont qualifiées de "suspectes" et sur les personnes qui ont accès aux données relatives aux transactions et aux titulaires de comptes une fois qu'elles sont qualifiées de "suspectes". » [1288] Cela dit, l'applicabilité de telles recommandations pose question. En effet, certaines mesures d'atténuation de risque paraissent contredire les pratiques des banques, comme le fait de limiter les collectes de données supplémentaires[1289]. Enfin, toujours est-il que dans certains cas, la solution prônée par les ONG est tout simplement le fait de ne pas avoir recours à des programmes de transferts monétaires en raison de la sensibilité des données traitées, notamment lors de conflits[1290].

Jusqu'à quel point les ONG cherchent-elles à passer « sous les radars » ? Quel degré de minimisation d'exposition et de visibilité des bénéficiaires est-il recherché ? Les réponses à cette question varient selon l'organisation et le contexte. Par exemple l'UNHCR, met moins l'accent sur la protection des données des bénéficiaires que sur le fait de s'assurer qu'ils disposent de documents d'identité afin de favoriser leur inclusion financière. En effet, du fait d'un manque de papier d'identité, il peut être difficile pour les exilés d'ouvrir un compte et se plier aux mesures de KYC.

Cela dit, les mesures de KYC sont inégalement appliquées, d'où des situations très diverses pour les exilés.Dans certains pays, la faiblesse de l'implémentation du cadre juridique AML/CFT fait que les exigences en matière de KYC peuvent être parfois minimes. Et donc dans ce cas, il serait plus facile pour un bénéficiaire d'ouvrir un compte bancaire[1291]. Il se trouve que des institutions financières peuvent être plus ouvertes que le prévoit le cadre juridique, parfois en raison d'un manque de connaissance de ce dernier [1292]. Les réglementations peuvent être théoriquement strictes, mais peu mises en œuvre. D'où, comme en Jordanie, la possibilité pour les réfugiés d'utiliser des services de transferts de fonds même avec la carte de l'UNHCR, le système d'identification de l'organisation étant reconnu comme une preuve valide d'identité[1293]. Toutefois, dans certains cas, la faiblesse de l'implémentation du cadre LCB/FT n'a pas d'impact sur le fait de pouvoir ouvrir ou non un compte, cette opération restant alors difficile pour les bénéficiaires.

---

[1288] "To anticipate such scenarios, humanitarian organizations should systematically ask FIUs for more information on how transactions come to be labelled as "suspicious" and who gains access to transaction and account holder data once they are labelled "suspicious"The humanitarian metadata problem : "doing no harm" in the digital era", *ICRC, Privacy International*, October 2018

[1289] "Practical guidance for data protection in cash and voucher assistance, a supplement to the cash in emergencies toolkit", IFRC, January 2021 https://cash-hub.org/wp-content/uploads/sites/3/2021/01/CVA-Data-Protection-Guidance-final.pdf

[1290] SLIM, Hugo, BANFIELD, Rachel, SOULEYMANE ADENHOF, Thierno, BURTON, Jo, "cash transfer programming in armed conflict: The ICRC's experience", ICRC 2018 https://resources.peopleinneed.net/documents/594-4359-002-cash-transfer-programming-upd-1-11-2018-web-1-.pdf

[1291] "Displaced and disconnected, Country reports", UNHCR innovation service, April 2019https://www.unhcr.org/innovation/wp-content/uploads/2019/04/Country-Reports-WEB.pdf

[1292] "Cash assistance and access to formal financial services, information on assessing KYC and CCD regulation", UNHCR, 2021 https://www.unhcr.org/sites/default/files/legacy-pdf/616e8d244.pdf

[1293] ISAACS, Leon, HUGO, Sarah, ROBSON, Gemma, BUSH, Charlie, ISSACS, Poppy, MORE MARTINEZ, Inigo," Impact of the Regulatory Environment on Refugees' and Asylum Seekers' Ability to Use Formal Remittance Channels", KNOMAD Working paper 33, July 2018

Dans certains cas, l'assouplissement du cadre juridique est à l'initiative de l'État même, comme c'est le cas en Allemagne. En 2015, le ministère de la Justice et de l'Intérieur allemand s'inquiétait du risque que représenterait l'émergence d'une potentielle économie informelle portée par l'arrivée de réfugiés n'ayant pas accès à des services financiers. La cellule de renseignement financier germanique, le BAFIN, avait alors autorisé un système alternatif d'ouverture de compte, avec un système de KYC plus léger. Il suffisait de fournir une lettre des autorités compétentes en matière d'immigration, contenant des données sur le nom du réfugié, la date de naissance, sa nationalité et une photographie du bénéficiaire. On peut noter que — de manière plus générale — l'Allemagne ne fait pas figure de « bonne élève » aux yeux du GAFI [1294].

Enfin, l'assouplissement des exigences en matière de KYC est parfois le fruit de négociations de l'UNHCR auprès de gouvernements pour élargir des possibilités d'identification, comme au Bangladesh pour les Rohingyas par exemple[1295]. L'UNHCR — tout en travaillant à l'adoption de solutions d'identification pour les exilés [1296] — a négocié auprès d'acteurs gouvernementaux et les banques centrales des pays où il intervient pour essayer d'alléger les mesures de KYC et faire en sorte qu'elles soient moins gourmandes en données. Cela dit, l'organisation plaide aussi pour l'utilisation de ses propres systèmes d'identification, eux-mêmes très invasifs, reposant sur le stockage centralisé de données biométriques [1297]. D'ailleurs dans un rapport du GAFI sur les systèmes d'identification numérique, le cas de l'UNHCR est examiné, et l'usage de son système d'identification (notamment biométrique) à des fins de KYC est envisagé[1298].

Toujours est-il que d'autres ONG choisissent non plus de négocier auprès des banques, mais de recourir à des solutions de financement informelles, et de sortir des circuits « officiels », en ayant recours notamment à l'hawala. Or, il se trouve que ce type de forme de financement est considéré par les autorités comme un canal de financement du terrorisme. L'hawala est un mode de financement bien implanté dans certains pays, comme la Syrie ou l'Afghanistan, pays dans lesquels il s'agit même d'un des principaux modes de paiement utilisés par les populations locales, mais aussi par les humanitaires [1299]. Il est très commun, familier et disponible dans de nombreuses zones, parfois même les plus sensibles. Concrètement, l'hawala repose sur l'existence de deux intermédiaires, chargés de rassembler et de distribuer des fonds dans leurs zones d'action respective. Le client va effectuer un dépôt auprès d'un premier prestataire qui en contrepartie va lui fournir un code permettant aux parties prenantes d'identifier la transaction. Le courtier contacte son homologue pour lui transmettre

---

[1294] "Germany's measures to combat money laundering and terrorist financing, Mutual evaluation report", FATF August 2022, https://www.fatf-gafi.org/en/publications/Mutualevaluations/Mer-germany-2022.html

[1295] "Displaced and disconnected", Country reports, UNHCR innovation service, April 2019https://www.unhcr.org/innovation/wp-content/uploads/2019/04/Country-Reports-WEB.pdf

MARTIN, Aaron, "Displaced & disconnected,Connectivity for refugees", UNHCR Innovation, April 2019https://www.unhcr.org/innovation/wp-content/uploads/2019/04/Displaced-Disconnected-WEB.pdf

[1296] "Digital identity", FATF, March 2020https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-on-Digital-Identity.pdf.coredownload.pdf

[1297] MARTIN,Aaron, TAYLOR, Linnet, " Exclusion and inclusion in identification: regulation, displacement and data justice", *Information Technology for Development*, 27:1, 50-66, 2021 10.1080/02681102.2020.1811943

[1298] Ibid.

[1299]ZERDEN, Alex, "Establishing a humanitarian financial corridor for Afghanistan", *Lawfare, Foreign relations & international law*, 15/11/2021 https://www.lawfaremedia.org/article/establishing-humanitarian-financial-corridor-afghanistan

le code. Et de son côté, le bénéficiaire peut aller retirer ses fonds dans une autre agence — un autre hawaladar — grâce au même code d'identification, sans avoir nécessairement à communiquer d'autres données personnelles. Il n'y a pas de mouvement de fond dans l'immédiat. Le premier courtier s'acquitte seulement par la suite des dettes contractées auprès du second qui a avancé des sommes pour les destinataires de la transaction. Cette dette est acquittée à plus ou moins long terme, sous la forme d'un virement bancaire, de l'envoi d'espèce, de chèque, de marchandises, etc. Ces formes de transfert reposent donc non pas sur la traçabilité des fonds et sur la vérification de l'identité du client, mais sur la confiance, facilitée par les relations interpersonnelles tissées entre les courtiers et leur clientèle[1300].

L'hawala permet donc de contourner les méthodes de traçabilité des instituts financiers. Il est donc utilisé à la fois de façon quotidienne, mais également par des populations plus marginales comme les exilés[1301]. Et surtout, son opacité fait qu'il est considéré comme une des voies de financement du terrorisme. Le GAFI stigmatise donc l'hawala et ce dès les années 1990, d'abord de façon mesurée, puis plus tranchée à partir du 11/09. On assiste à une « sécuritisation » de ce mode de financement. Et une recommandation du GAFI lui est même consacrée. L'hawala devient suspect « per se », comme le raconte Anthony Amicelle, parce qu'il ne repose pas sur des modalités usuelles de traçabilité des fonds[1302].

Or, pour contourner les différents obstacles qu'on a évoqués, les humanitaires peuvent avoir recours à l'hawala. Dans certaines zones c'est même leur mode principal de transfert de fonds. D'autant que ce genre de réseau est aussi opérant dans des régions affectées par des conflits (contrairement aux banques)[1303]. L'hawala est apprécié par les humanitaires pour ses facilités opérationnelles, pour sa flexibilité et sa rapidité[1304]. Il peut être utilisé pour des transferts de fonds pour les programmes d'une ONG ou encore pour des projets de « cash transfert ». L'ONG reçoit alors des fonds via des hawalas pour les redistribuer aux communautés.

Mais l'hawala n'est pas pour autant exempt de tout risque en matière de protection des données. Pour tout dire, cela dépend du type d'hawala employé. Comme on l'a dit, il existe depuis plusieurs années un mouvement de régulation de ce type de canal de financement. Dans certains cas, il peut s'agir d'hawala enregistré, bénéficiant de licences. Ils sont donc

---

[1300] "The world bank and the international monetary fund, informal funds transfer systems : an analysis of the informal hawala system", World Bank, IMF, 21/03/2003 https://documents1.worldbank.org/curated/en/410351468765856277/pdf/multi0page.pdf

[1301] BOITIAUX, Charlotte, ALBOZ, Dana, LOUARN, Anne-Diandra, « La hawala, système parallèle et opaque de transfert d'argent utilisé par les migrants », *Infomigrants,* 12/04/2018 https://www.infomigrants.net/fr/post/8616/la-hawala-systeme-parallele-et-opaque-de-transfert-dargent-utilise-par-les-migrants

[1302] AMICELLE, Anthony, CHIFFELLE, Jaquet, OLIVIER, David, « La traçabilité, une technique de stigmatisation? Retour sur la problématisation de l'"hawala" dans le contexte antiterroriste », *Revue Internationale de Criminologie et de Police Technique et Scientifique*, 2015, LXVIII.p. 338-353.

[1303] "cash feasibility assessment", *Cash working group*, North West Syria, Calpnetwork, 2020 https://www.calpnetwork.org/wp-content/uploads/ninja-forms/2/IOM_CFA_external_final_compressed.pdf

"Exploring blockchain and mobile money in the northwest of syrian assessment of current and potential utility of alternative tools in minimising money transfer challenges and aid duplication", AFNS, IMMAP, 2023 https://afns.org/volumes/doc/Blockchain-and-Mobile-Money-in-Northwestern-Syria.pdf?v=1695478374

"cash feasibility assessment", Cash working group, North West Syria", *Calpnetwork*, 2020 https://www.calpnetwork.org/wp-content/uploads/ninja-forms/2/IOM_CFA_external_final_compressed.pdf

"Afghanistan Hawala casH transfers for food assistance and livelihood protection",*ACF*, 2012,https://www.actioncontrelafaim.org/wp-content/uploads/2018/01/acf_afghanistan_cash_case_study_jan_2012.pdf

[1304]"Exploring blockchain and mobile money in the northwest of syrian assessment of current and potential utility of alternative tools in minimising money transfer challenges and aid duplication", AFNS, IMMAP, 2023 https://afns.org/volumes/doc/Blockchain-and-Mobile-Money-in-Northwestern-Syria.pdf?v=1695478374

moins informels, plus d'informations peuvent être demandées comme conditions de transferts. Et ce type de canaux financiers peut même être lié à des acteurs gouvernementaux : « les données relatives aux transactions, les informations d'identification, sont susceptibles d'être accessibles aux structures de Damas, les agences devront examiner le profil de leurs bénéficiaires pour décider si cela est susceptible de les exposer à un risque accru, et si la clause de confidentialité des données est suffisante. » [1305]

Les conclusions d'un atelier organisé avec des ONG sous l'égide d'une firme de conseil, Beechwood confirme ce point. Sur les slides des présentations des participants sont listés — sous forme de notes télégraphiques — les points suivants : « Le processus d'enregistrement dans les zones contrôlées par le régime exige des hawaladars qu'ils fournissent de nombreux documents ; il existe des problèmes de protection des données avec les agents hawala enregistrés par le gouvernement syrien ; le gouvernement syrien a probablement un certain degré de contrôle sur les flux d'argent transitant par la Syrie, quelle que soit la zone. Il est probable qu'il l'autorisera tant qu'il aura une part du gâteau. »[1306]

Or, dans certains cas, les hawaladars peuvent avoir accès à minima aux noms des bénéficiaires, ce qui peut être facteur de risques selon certaines ONG : il est donc parfois recommandé de ne pas leur fournir ce type de données, ainsi les numéros de téléphone, et des documents d'identité, et d'inclure des clauses de protection de données dans leurs interactions avec des hawaladars [1307].

L'utilisation de réseaux d'hawala « non enregistrés » comprend d'autres risques. Tout d'abord, il n'y a tout simplement pas de consensus parmi les ONG sur la légitimité et la nécessité de passer totalement sous les radars du gouvernement hôte : « Pour ce qui est de transferts d'hawala non enregistré externes ou internes à la Syrie, cette solution n'est pas conseillée. Si l'avantage perçu est de dissimuler les transactions au gouvernement hôte, le projet devra peut-être être reconsidéré. » [1308]

Et les ONG plaident parfois pour une utilisation « transparente » de ce type de réseau de financement opaque. Tout d'abord, il s'agit d'une forme de transparence contrainte, pour « rassurer » les bailleurs, pouvant être méfiants à l'égard des hawalas et de leur « manque » de redevabilité[1309]. Il est évidemment difficile de conserver un historique des échanges des hawala non « enregistrés », puisqu' : « il est peu probable qu'il soit possible d'obtenir des preuves documentaires de la réception des transactions. La confirmation se fait par téléphone

---

[1305] « data about transaction, identifiant information, is likely to be available to structures in Damascus, Agencies will have to consider the profile of their beneficiaries to decide if this is likely to place them at increased risk, and if data privacy clause are suffisant".DEAN, Roger, "Remittances to syria What Works, Where and How", *Norwegian refugee council*, 2015 https://www.calpnetwork.org/wp-content/uploads/2020/01/2015-07-nrc-remittances-to-syria-report-final-1.pdf

[1306]"Registration in regime-controlled areas requires hawaladars to give lots of documentation;Data protection issues with GoS registered hawala agents; GoS likely has degree of oversight over flows of money through Syria regardless of the area. Will likely allow so long as they get a cut." BEECHWOOD international, "Hawala and humanitarian aid risks, mitigation and options in Syria", Chatham house workshop, Istanbul 14-15 December 2015.

[1307]DEAN, Roger, "remittances to Syria, What Works, Where and How", Norwegian refugee council, 2015

[1308] « from unregistered hawala outside Syria to either type of hawala inside Syria: this is not advised. If the perceived advantage is to obscure transactions from a host government, then the project may need to be reconsidered. » Ibid.

[1309] « Several aspects of the hawala system usually raise concerns among donors. These are often related to a limited understanding of the value exchange system as well as to the lack of transparent, reliable information collected and shared about the individual hawala agents that are effectively used for humanitarian transactions. Among the main concerns regarding the use of hawala networks as FSPs for humanitarian cash- based interventions are capacity and liquidity, reliability and accountability, as well as reach and costs. »
Ibid.

ou par WhatsApp. »[1310] Les ONG ne peuvent alors qu'informer les bailleurs de l'utilisation de tels financements.

Ensuite, les ONG ont elles-mêmes conscience du risque de détournement des fonds transitant par des réseaux d'hawalas. Elles tentent donc de mettre en place différentes formes de contrôle de ces derniers[1311]. Généralement, les ONG travaillent avec des partenaires de confiance et maintiennent une liste de partenaires fiables dont elles gardent la mémoire[1312] [1313] [1314]. Cela dit, il reste difficile pour les ONG de s'assurer de leur transparence et de la fiabilité des informations que les halawa transmettent aux ONG[1315]. Il existe donc une tension entre la transparence requise par les banques, par les bailleurs, voir par les ONG, qui sont partagées entre la nécessité de passer, dans une certaine mesure, sous les radars, et la volonté de conserver un certain contrôle du mode de financement utilisé.

Notons enfin que les ONG recourent parfois à d'autres méthodes pour contourner les exigences de KYC en employant des cryptomonnaies[1316]. Il se trouve que ces technologies partagent quelques points communs avec l'hawala, par exemple la confidentialité, l'absence de contrôle, la fiabilité et la décentralisation. » [1317] Les deux systèmes court-circuitent les canaux traditionnels, permettent une plus grande souplesse et un plus grand anonymat et sont tous les deux associés à l'économie criminelle. Traditionnellement, les acteurs prônant l'utilisation de cryptomonnaies défendent l'importance de l'anonymat en ligne et sont proches des milieux cypherpunks[1318].

Les cryptomonnaies sont en effet décriées ou louées pour l'anonymat (relatif) qu'elles procurent : les détenteurs de cryptomonnaies ne sont pas tenus de déclarer leur identité. Les cryptomonnaies peuvent être détenues dans un portefeuille et sont matérialisées sous forme de suite de chiffres et de lettres. Seuls les numéros et les contenus des comptes sont nécessaires pour ouvrir un compte. Comme souvent, l'anonymat n'est cependant jamais

---

[1310] « Documentary evidence of receipt of transactions is unlikely to be possible. Confirmation comes by phone or Whatsapp, Finance SOPs would have to be revised to accommodate alternative confirmation Consultation with the donor is highly recommended. From unregistered hawala outside Syria to either type of hawala inside Syria This is not advised. If the perceived advantage is to obscure transactions from a host government, then the project may need to be reconsidered DEAN, Roger, ibid.

[1311] Ibid.

[1312] The tricky part in this example is that the money physically given to the first hawala agent is thus eventually used by this agent at his discretion in his other business transactions. Similarly, the money physically provided by the end-point hawala agent to the recipient comes from his other business dealings with his other clients. In other words, humanitarian organizations have to understand where their hawala agent's money comes from (and to some extent what other clients they may have) as well as what they do with the money that they are provided with (and what type of trade they are involved with).
Ibid.

[1313] Ibid.

[1314] BEECHWOOD international," Hawala and humanitarian aid risks, mitigation and options in Syria, Chatham house workshop", Istanbul 14-15 December 2015.

[1315] Ibid.
PHILLIPS, Jason, « Counterterrorism and Humanitarian Impartiality Counterterrorism and Humanitarian Impartiality Independent review of IRC activities in Afghanistan, Somalia, and northwest Syria, International Rescue Committee, September 2021

[1316] Les « cryptomonnaies », plutôt appelées « crypto-actifs », sont des actifs numériques virtuels qui reposent sur la technologie de la blockchain (chaine de bloc) à travers un registre décentralisé et un protocole informatique crypté. Un crypto-actif n'est pas une monnaie. Sa valeur se détermine uniquement en fonction de l'offre et de la demande. Les crypto-actifs ne reposent pas sur un tiers de confiance, comme une banque centrale pour une monnaie. Il existe à ce jour plus de 1 300 crypto-actifs. Les plus connus sont le bitcoin, le ripple, l'ether, le litecoin, le nem et le dash. » « Qu'est-ce qu'une cryptomonnaie? », Autorité des marchés financiers, 11/06/2022 https://www.amf-france.org/fr/quest-ce-quune-cryptomonnaie

[1317] « Hawala and cryptocurrencies share some principles, for example, privacy, lack of oversight, reliability, and decentralization AZIZI, Hamid, "The Hawala System its operations and misuse by opiate traffickers and migrant smugglers", UNODC, 2023https://www.unodc.org/documents/data-and-analysis/AOTP/Hawala_Digital.pdf

[1318] O'DONOGHUE, Patrick, "Cryptocurrency exchanges shun EU anti-laundering directive", *The Sunday Times*, 06/04/2022 https://www.thetimes.co.uk/article/crypto-currency-exchanges-shun-eu-anti-laundering-directive-h9jmg6tqb

absolu. En effet, les transferts de cryptomonnaies d'un compte à un autre laissent des traces pouvant être analysées [1319]. Des entreprises se spécialisent d'ailleurs dans le suivi des transactions en cryptomonnaies, comme Ciphertrace. Et l'on peut donc parler de pseudonymat plutôt que d'anonymat.

Ajoutons que des institutions financières, dont le GAFI, souhaitent assurer une plus grande traçabilité de ce genre de monnaie (associée à l'économie criminelle). La future 6ème directive AML/CFT comprend un volet sur ce point, notamment en matière d'application de KYC pour des cryptomonnaies. Et actuellement, un bon nombre des sociétés de monnaies virtuelles, qu'il s'agisse de plateformes de négociation ou de fournisseurs de portefeuilles, disposent de protocoles KYC et AML, ainsi que d'outils de suivi des transactions[1320]. Un écosystème de la conformité KYC des cryptomonnaies a émergé. Des entreprises se sont spécialisées sur le sujet. Notons aussi qu'existent des recherches visant à concilier anonymat et KYC, notamment autour des protocoles de type « Zero Proof knowledge. » [1321] Mais ce mouvement de régulation ne se fait pas sans critiques au sein de l'industrie des cryptomonnaies [1322].

Il est temps de présenter les différents cas d'usage de cryptomonnaies par les humanitaires. De façon générale, elles sont présentées comme une solution d'inclusion pour des populations vulnérables financièrement ou des populations n'ayant pas accès aux circuits bancaires. Facebook a par exemple compris l'opportunité que représentent en matière de marchés les pays en développement. La firme envisageait de développer son projet, avorté, de monnaie numérique Libra en grande partie en Afrique[1323]. Mais si l'hawala est communément utilisée, l'usage de cryptomonnaies reste au sein du secteur humanitaire à l'état d'expérimentation [1324]. Un certain nombre de projets concernent les systèmes de donations d'ONG. À notre

[1319] RAMOS TUBINO, Rafael, ROBARDET, Céline, CAZABET, Rémy (2022), « Towards a better identification of Bitcoin actors by supervised learning », *Data and Knowledge Engineering*, vol. 142, 2022, p. 102094.

[1320] "What is KYC in Crypto?", *Veriff*, 06/04/2023 https://www.veriff.com/blog/what-is-kyc-in-crypto

[1321] MATSANGOU, Elizabeth,"The clash between KYC and cryptocurrencies", *World Finance*, https://www.worldfinance.com/wealth-management/the-clash-between-kyc-and-cryptocurrencies

[1322] « La demande de régulation émane paradoxalement du secteur des cryptomonnaies. Elle se présente comme un pacte faustien : se soumettre à quelques règles du gendarme de la Bourse permettrait aux acteurs des cryptomonnaies d'avoir accès à un marché financier beaucoup plus vaste, notamment aux investisseurs institutionnels et à l'argent des retraites par capitalisation. »
DURANA, Gabrielle, « Démocratiser la finance ? Les désillusions de la cryptomonnaie », *Esprit*, 2023/5 (Mai), p. 47-55. https://www.cairn.info/revue-esprit-2023-5-page-47.htm

[1323] MATHIS, Jérôme, « Avec sa cryptomonnaie, Facebook veut concurrencer les services de transfert d'argent en Afrique », *Le Monde*, 01/09/2019 https://www.lemonde.fr/afrique/article/2019/09/01/avec-sa-cryptomonnaie-facebook-veut-concurrencer-les-services-de-transfert-d-argent-en-afrique_5505189_3212.html

[1324] PARKER, Ben, "Des applications louables pour Bitcoin?", *The New humanitarian*, 13/01/2016 https://www.thenewhumanitarian.org/fr/report/102069/des-applications-louables-pour-bitcoin
OLIVEROS, Joseph, LEGHARI, Talha, "global payment solutions for humanitarian cash assistance", IFRC, December 2022https://cash-hub.org/wp-content/uploads/sites/3/2022/11/IFRC_GlobalPaymentSolutions_EN_LR.pdf
"Exploring blockchain and mobile money in the northwest of syrian assessment of current and potential utility of alternative tools in minimising money transfer challenges and aid duplication", AFNS, IMMAP, 2023 https://afns.org/volumes/doc/Blockchain-and-Mobile-Money-in-Northwestern-Syria.pdf?v=1695478374
DODGSON, Kate, GENC, Dilek, "Blockchain for humanity", ODIHPN, 29/11/2017https://odihpn.org/publication/blockchain-for-humanity/
BLAKSTAD, Sofie, "The next generation humanitarian distributed platform", Danish Red cross, Mercy Corps, Hiveonline, November 2020
WANG, Fennie, DE FILIPPI, Primavera, "Self-sovereign identity in a globalized world: credentials-based identity systems as a driver for economic inclusion", *Frontiers*, Volume 2-2019https://www.frontiersin.org/articles/10.3389/fbloc.2019.00028/full
"Exploring blockchain and mobile money in the northwest of Syrian assessment of current and potential utility of alternative tools in minimizing money transfer challenges and aid duplication", AFNS, IMMAP, 2023 https://afns.org/volumes/doc/Blockchain-and-Mobile-Money-in-Northwestern-Syria.pdf?v=1695478374
ZUCCHINI, Giulio, LOISEAU, Camille, CAPATAZ GORDILLO, Carlos, ANDUJAR PEREZ, Julian, PENALVER BLANCO, Ana, SCRUBY, Celia,"How blockchain can possibly improve humanitarian actions, community engagement, cash transfer and traceability", *Red Social innovation*, March 2023https://red-social-innovation.com/wp-content/uploads/2023/06/Blockchain_EN.pdf
KO, Vanessa, VERITY, Andrej, "Blockchain for the humanitarian sector: future opportunities", *Digital Humanitarian network*, 2016
ZHANG, Zoey, VERITY, Andrej, "Humanitarian : inventory and recommendations", *Digital humanitarian network*, August 2022,

connaissance, il existe une minorité de programme de transfert monétaire utilisant des cryptomonnaies. On peut citer le partenariat du HCR avec une firme de blockchain, Stellar ; l'expérience d'OXFAM aux îles Vanuatu et une collaboration entre l'entreprise Partisia et le CICR.

Or, encore une fois, en employant des cryptomonnaies, les humanitaires ne mettent pas nécessairement en avant la possibilité d'accorder aux bénéficiaires plus de protection en raison de leur caractère confidentiel. Oxfam comme l'UNHCR utilisent ce type de monnaie, car elles y voient une façon d'adopter une modalité opérationnelle plus souple et efficace. En outre, les humanitaires voient dans les cryptomonnaies d'autres intérêts : favoriser l'inclusion financière de personnes dépourvues de documents d'identité civile, comme le propose la firme Gravity[1325], ou le leaf program d'Unicef[1326].

Prenons l'exemple d'Unblocked cash pilot, un projet d'Oxfam mené au Vanuatu en 2019. Cet archipel — connu pour être un paradis fiscal — fut longtemps un « mauvais élève » en matière de LBC-CT. Il a été placé sur liste noire par le GAFI, qui l'a retiré de cette dernière depuis 2018 du fait d'« améliorations » concernant la mise en œuvre de ses recommandations. L'archipel est considéré comme un environnement favorable au développement des cryptomonnaies. C'est dans ce contexte qu'Oxfam Australie a donc lancé un projet de cryptomonnaies Unblocked Cash Pilot — en partenariat avec l'entreprise de blockchain australienne Sempo[1327]. Ses promoteurs y voyaient une forme de transfert monétaire plus efficace[1328]. Et une partie du rapport sur le projet se concentre sur les avantages qu'il représente en matière de gain de temps et de rentabilité.

Plus précisément, Oxfam a engagé la firme Sempo pour l'achat des DAI [1329] qui sont redistribués sur un portefeuille numérique. S'en est suivi une redistribution des DAI aux bénéficiaires, qui dépensent les cryptomonnaies auprès de vendeurs accrédités. Les dépenses sont enregistrées sur la blockchain. Puis Sempo rembourse les vendeurs en monnaie fiduciaire[1330]. Les données de transactions sont visibles sur la plateforme gérée par Sempo, ou directement sur Ethereum mainet (via un agrégateur de données, comme Etherscan).

---

[1325] "Gravity describes itself as a 'next-generation identity solution' with an ambition to give everyone access to a mobile phone by creating a digital identity infrastructure that is fundamentally inclusive. To do this, they help individuals establish a trusted identity – or « Proof of Existence » – that is independent from public infrastructures and non-dependent on official identity documents, postal addresses or banking systems.While Gravity's end-to-end solution uses back-end blockchain technology to certify a customer's KYC-related information, VOTA, Wayan, "Two blockchain use cases for self-sovereign digital identities", *ICTworks,* 31/01/2018https://www.ictworks.org/blockchain-use-cases-self-sovereign-digital-identities/

[1326] "Leaf wallet: digital financial services for refugees and under-resourced communities", Unicef venture fund, 08/06/2021 https://www.unicefventurefund.org/story/leaf-wallet-digital-financial-services-refugees-and-under-resourced-communities

[1327]JUTEL, Olivier, « Blockchain humanitarianism and crypto-colonialism », *Patterns,* Volume 3, Issue 1, 2022, https://www.sciencedirect.com/science/article/pii/S2666389921003056

[1328]CRAIG, Glen,"Going digital, what's next for Vanuatu in Blockchain innovation? Policy and regulatory recommendations for financial and economic inclusion", Pacific advisory, April 2023 https://www.calpnetwork.org/wp-content/uploads/2023/04/going-digital-whats-next-for-vanuatu.pdf

[1329]Un DAI est un « stablecoin », soit un coin adossé au dollar.

[1330] « The programme administrator or another approved party such as Sempo then reimbursed vendors for the goods and services they had exchanged with recipients for tokenised value. This cash-out process relied upon Sempo or Oxfam to exchange CCV tokens for fiat currency held within their respective bank accounts. The actual transfer of funds occurs off-chain between existing FSPs held by either Sempo or Oxfam and the vendors. This fiat currency was necessary for vendors to trade off-chain for goods. At this point, the CCVs were recorded as spent, or in possession of an approved party. Finally, the approved party was reimbursed by using the CCV to trigger a release of funds from the escrow contract. » RUST, BJORN, "Unblocked cash: piloting accelerated cash transfer delivery in Vanuatu", Oxfam, 31/10/2019
CARNABY, E., HALLWRIGHT, J. "Complexities of implementation: Oxfam Australia's experience in piloting blockchain", *Frontiers*, Volume 2 - 2019

Quant aux données personnelles, elles sont stockées « offchains » sur une base de données. Il est question du nom, de l'âge, du genre, de l'adresse, du type de participant, du vendeur ou du bénéficiaire.

Toutefois, si l'archipel a une position plutôt laxiste en matière de contrôle bancaire (pour rappel il s'agit d'un paradis fiscal), à la suite de pressions du GAFI[1331], le Vanuatu a adopté très progressivement, et ce dans une certaine mesure, un cadre normatif en accord avec les recommandations de l'organisation internationale[1332]. En tout cas, l'Etherum et les bitcoins sont théoriquement interdits au Vanuatu. Et plus généralement depuis 2021, les usagers doivent uniquement utiliser les cryptomonnaies dotées de licences enregistrées auprès des autorités. Et les usagers de cryptomonnaies — et donc d'Unblocked Cash Pilot — doivent respecter des mesures de type KYC. C'est la firme Sempo qui est chargée des démarches de conformité bancaire, et conserve les données de KYC pendant 7 ans. Oxfam n'y a théoriquement pas accès. Toujours est-il que les enjeux de protection des données que ces démarches posent n'ont pas été évoqués dans le rapport de l'ONG, qui conclut en queue de poisson : « Le suivi en temps réel des transactions dans le cadre du projet pilote UnBlocked Cash a permis une plus grande transparence que les solutions CVA traditionnelles et une réponse plus rapide aux besoins des participants. Toutefois, cela a soulevé des questions de respect de la vie privée, de pouvoir et de risque lié aux enregistrements de transactions pseudonymes disponibles en temps réel ou presque. Il convient de poursuivre les travaux afin d'identifier les risques associés à ce système et de comprendre les implications potentielles. »[1333]

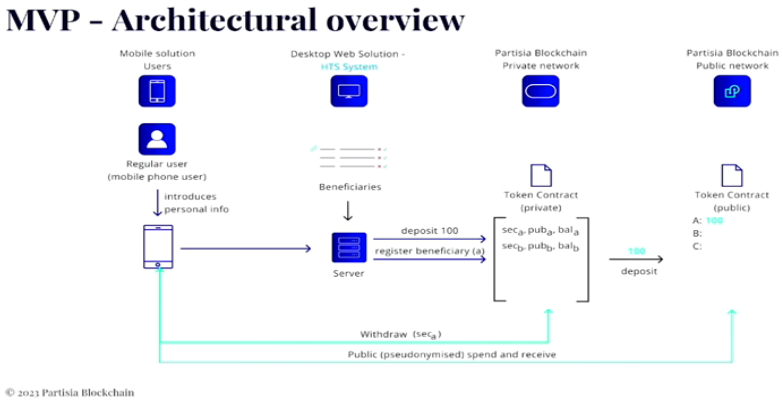
Le CICR adopte un positionnement contraire. Et la protection des données est au fondement du projet pilote mené avec la firme de Blockchain Partisia. Ce dernier repose sur un système de double blockchain. Une première blockchain privée, et accessible par les bénéficiaires, sert à tracer l'ensemble des dépenses des bénéficiaires. Une deuxième blockchain publique, destinée aux bailleurs, sert à avoir une visibilité sur l'ensemble des transactions. La clef du bénéficiaire change à chaque transaction, son historique d'achat ne peut donc pas être tracé. En revanche, l'ensemble des dépenses est visible sur la blockchain publique permettant ainsi de respecter en partie la redevabilité bailleur. Pour s'inscrire, le bénéficiaire doit créer un compte. Ce sont les sous-délégations qui connectent les personnes au système, et à chaque transaction elles doivent obtenir une autorisation à la délégation nationale, qui approuve le transfert. Les bénéficiaires peuvent ensuite dépenser les tokens dans des magasins faisant partie du projet. Une remarque cependant. Les supports de communication du projet ne précisent pas à quel type de token le CICR souhaite avoir recours ni comment seront prises en

[1331] the Vanuatu Financial Service Commission, (VFSC), the integrated regulator for non banking financial services and Fintech related activities including digital assets such as cryptocurrencies, NFTs and FeFi, wishes to inform the public that trading in digital assets (including cryptocurrencies, NFTs and DeFi) requires a class D license under the Financial Dealers Licensing Act, issued by the Vanuatu Financial Services commission. Trading without a licenses is prohibited and punishable by law." Crypto & digital assets trading, Vanuatu financial services commission, march 2022
https://www.vfsc.vu/wp-content/uploads/2022/03/VFSC-Press-Release-Crypto-Digital-Assets-Trading.pdf

[1332] Asia/Pacific Group on Money Laundering, mutual evaluation of Vanuatu, 2018

[1333] "Real-time monitoring of transactions during the UnBlocked Cash pilot provided both greater transparency than traditional CVA solutions and faster response to participant needs. However, this raised issue of privacy, power, and potential risk of pseudonymous transaction records available in real-time or near real-time. More work should be done to identify risks associated with this system and to understand the potential implications." RUST, BJORN, "Unblocked cash: piloting accelerated cash transfer delivery in Vanuatu", Oxfam, 31/10/2019

compte les exigences de KYC. En outre, on ne sait pas encore dans quel pays le projet pourrait être testé, sachant que « des questions réglementaires se posent, a-t-il noté, car certains pays interdisent les cryptomonnaies. Le calendrier de déploiement doit également tenir compte de la responsabilité du CICR en tant que fournisseur d'aide humanitaire. » [1334]




### L'ARCHITECTURE DE LA BLOCKCHAIN PARTISIA [1335]

On est revenue dans ce chapitre sur l'action d'ONG en faveur d'un statut d'exception face aux mesures de lutte contre le financement du terrorisme, les humanitaires ont plaidé le respect de l'impartialité de l'aide au sein d'institution multilatérale (ONU et son Conseil de sécurité), mais aussi auprès de bailleurs de fonds, comme l'USAID ou l'AFD. On a vu que l'accent était mis sur le respect du DIH et que l'argument de la vie privée a été mobilisé qu'à la marge. Et ce en dépit des problématiques en matière de protection des données que soulève l'ensemble des mesures contre le financement du terrorisme. On pense au corpus juridique de soft law du GAFI ou aux lois de lutte contre le blanchiment d'argent et le financement du terrorisme. Les instances européennes de protection des données s'inquiètent du manque de proportionnalité de ces mesures. Or, les humanitaires sont aux prises avec les répercussions de ces textes de loi et des mesures de compliance bancaire, notamment dans les programmes de transferts monétaires. Les ONG critiquent majoritairement ces dispositifs pour des motifs opérationnels et en raison des risques d'atteinte au DIH et au principe de neutralité et d'impartialité de l'aide. Leur priorité est donc de négocier avec les banques un allégement des mesures de conformité bancaire, quitte à contrevenir aux normes de KYC. Cela implique aussi pour certaines le fait d'adopter des solutions aux marges de la légalité. On pense à l'hawala ou à des cryptomonnaies, ce qui est facteur d'insécurité juridique pour les ONG et constitue une prise de risque, d'autant que ces solutions ne sont pas sans répercussions potentielles en matière d'atteinte à la vie privée pour les bénéficiaires.

---

[1334] "There are regulatory issues, he noted, as certain countries ban cryptocurrencies. A timeline for deployment also must take into account the ICRC's responsibility as a humanitarian aid provider", MATSUDA, Tom, "Red Cross to reveal prototype for blockchain-based aid distribution", *The Block*, 02/12/2022 https://www.theblock.co/post/191686/red-cross-unveils-prototype-for-blockchain-aid-distribution-project
https://www.youtube.com/watch?v=a28D1MNWnzM
https://www.youtube.com/watch?v=YjiD0-a3rro

[1335] « ICRC AND partisia blockchain cryptographic enforced humanitarian token system », Partisia Blockchain Foundation, 21/05/2023https://www.youtube.com/watch?v=a28D1MNWnzM&ab_channel=PartisiaBlockchainFoundation

## Chapitre 05 — La cybersécurité au-delà du régalien, cyberopérations et humanitaire : assurer la protection des bénéficiaires

### Introduction de chapitre

Dans un interview accordé à la revue du Comité international de la Croix-Rouge, le professeur de droit international Marko Milanovic déclare que « s'il y a quelques années seulement, quelqu'un avait écrit un livre (…) sur la vie privée dans les conflits armés, la plupart des juristes internationaux auraient pensé que l'auteur (ou les auteurs) était un tantinet fou[1336]. » Effectivement. Au regard des drames humains des guerres, des blessés et des morts, la vie privée parait peu de chose. Mais la guerre n'épargne pas le terrain numérique. Et l'inclusion du domaine numérique comme un espace opérationnel pour les armées fait l'objet de réflexions tout aussi bien académiques que stratégiques depuis les années 1990. La publication de l'article de John Arquilla et David Ronfeldt *Cyberwar is Coming* en 1993 a fait date. Le domaine numérique a été progressivement inclus dans les doctrines militaires, aux USA tout d'abord autour du centre de réflexion RAND, puis cette formalisation doctrinale a conduit à l'ouverture d'une unité dédiée en 2010 (le Cybercom) ; tandis qu'en France, le Commandement de la cyberdéfense a été créé en 2016. La numérisation du champ de bataille englobe un large spectre de problématique, dont les cyberopérations, qui nous intéressent présentement. Mais si une partie des débats concerne la place qu'elles occupent dans les tensions entre grandes puissances et sur leur portée dans le cadre de conflit, ce ne sont pas les atteintes à la vie privée qui préoccupent les militaires et le champ académique. L'objet des discussions concerne plutôt la façon dont les conséquences d'actes offensifs dans le cyberespace sont perçues, qualifiées et définies. Il faut alors déterminer si les cyberopérations consistent en des actes de violence, si elles peuvent avoir des conséquences matérielles (directes ou indirectes), si elles peuvent représenter un gain stratégique, s'il s'agit d'actes pouvant dépasser le seuil de la conflictualité, ou non, si les cyberopérations représentent un risque d'escalade, ou si, au contraire, elles régulent les confrontations entre puissances et représentent justement une forme d'exutoire moins violent qu'un affrontement cinétique. En bref, la discussion se concentre sur les formes de la guerre et ses évolutions, la place des cyberopérations dans les conflits, la pertinence ou non du fait de qualifier de cyberguerre l'ensemble des tensions et affrontement secouant l'espace numérique.

Tout d'abord, au cours des années 1990, dans un contexte de militarisation et de sécuritisation du cyberespace[1337], des discours catastrophistes et anxiogènes se sont multipliés. Ces derniers allaient de pair avec des scénarii de cyberattaques touchant des infrastructures dites vitales,

---

[1336] "if only a few years ago somebody wrote a book (...) about privacy in armed conflict, most international lawyers would have though the author (s) to be slightly mad" "The rights to privacy and data protection in times of armed conflict", *International review of the red cross*, n°923, 2023

[1337] DOUZET, Frédérick, GERY, Aude, "Le cyberspace, ça sert, d'abord, à faire la guerre. Prolifération, sécurité et stabilité du cyberespace, *Hérodote*, 2020/2, n° 177-178,p. 329-350

et mettant donc gravement en péril les populations civiles[1338]. Certains analystes ont pu s'inquiéter de la possibilité d'un « cyber Pearl Harbor »[1339], et de ses répercussions sur des infrastructures critiques et sur la société civile. Ce mouvement de sécuritisation s'est formalisé par l'élaboration de doctrines militaires et la création de différents organes dédiés aux volets défensifs et offensifs du cyber[1340]. Depuis, ces discours catastrophistes ont été en partie nuancés, également au sein des institutions liées aux forces de l'ordre et aux institutions militaires, quand bien même le conflit ukraino-russe ait relancé le débat sur la pertinence de ce type de récit[1341].

Car à vrai dire, il existe certes différents cas de cyber-opérations ayant eu lieu durant des conflits. Les États-Unis, l'Angleterre et l'Australie en ont mené contre l'État islamique ; la Russie contre la Géorgie et contre l'Ukraine. Mais la plupart des cyberopérations se jouent dans une zone grise, hors d'affrontements cinétiques directs, et ne représentent rarement des dommages concrets. Les modalités d'affrontement entre grandes puissances prennent de nombreuses formes : cyberattaques, opérations de cyber-espionnage, interruptions ou obfuscations de systèmes de communications ennemies, opérations d'influence et de déstabilisation, désinformation[1342], etc. Autant d'opérations qui se situent en dessous du seuil d'affrontement direct, brouillant la frontière entre guerre et paix. Qualifier ces nouvelles formes de conflictualités ne va pas de soi. Le terme « guerre hybride » ne fait pas consensus, et le fait de pouvoir parler de « cyberguerre » reste très discuté parmi les universitaires et les militaires eux-mêmes. Certains parlent alors de « cyberguerrilla ». Mais surtout, le « cyberPearl harbor » tant craint n'a pas encore eu lieu et pour un bon nombre d'analystes, seule l'opération Stuxnet en 2010 aurait eu des répercussions physiques directes en paralysant le système de production nucléaire iranien[1343].

Cela ne signifie pas pour autant que les cyber-opérations sont sans effets notables. Elles s'inscrivent notamment dans une recomposition plus générale des souverainetés étatiques. Les cyber-opérations sont potentiellement des ingérences dans d'autres territoires. Les frontières entre acteurs étatiques et acteurs privés sont brouillées (via le recours à des groupes criminels pour mener des cyber-opérations) [1344] . Mais certaines formes de cybercriminalités échappent en partie aux États. À vrai dire, cette situation n'est pas totalement inédite. Fin 1990, au sortir de la guerre froide, on parlait déjà de nouvelles formes

---

[1338] DANET Didier, « Collapsologie numérique », dans : TAILLAT, Stéphane, CATTARUZZA, Amael, DANET, Didier éd., *La Cyberdéfense. Politique de l'espace numérique.* Paris : Armand Colin, « Collection U », 2018, p. 157-166. https://www.cairn.info/cyberdefense-politique-de-l-espace-numerique--9782200621292-page-157.htm

[1339] PANETTA, L. « Defending the Nation from cyber-attack (business executives for national security) », New york, 11/10/2012,http://archive.defense.gov/speeches/ speech.aspx?speechid=1728
https://arstechnica.com/information-technology/2015/02/fear-in-the-digital-city-why-the-internet-has-never-been-more-dangerous/
MUNRO, Neil, « The Pentagon's new nightmare : an electronic Pearl Harbor », Washington Post, 16/07/1995
Lawson, S."Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats", *Journal of Information Technology & Politics*, 10(1), 2013, p. 86–103. https://doi.org/10.1080/19331681.2012.759059

[1340] COUSTILLIERE, Arnaud, LEROY, Aude, *Soldat de la cyberguerre, un pionnier raconte la cyberdéfense française*, Tallandier, 2024, 288 p.

[1341] BROOKING, Emerson, LONERGAN, Erica, "Welcome to cyber realism: parsing the 2023 departement of defense cyber strategy", *War on the rocks*, 25/09/2023 https://warontherocks.com/2023/09/welcome-to-cyber-realism-parsing-the-2023-department-of-defense-cyber-strategy/?utm_source=pocket_saves

[1342] MARANGE, Céline, QUESSARD-SALVAING, Maud, *Les guerres de l'information à l'ère numérique*, Paris : Presse Universitaire de France, 2021, 456 p.

[1343] Stuxnet est un vers informatique découvert en 2010, conçu par les américains et les israéliens pour s'attaquer aux centrifugeuses iraniennes d'enrichissement d'uranium.

[1344] EGLOFF, Florian, *Semi-sate actors in cybersecurity*, Oxford, University press, 2022, 305 p.

de conflictualité, impliquant des milices et acteurs non étatiques. Et la façon de les qualifier et de déterminer quelles en étaient les dynamiques a fait l'objet de discussion dans le secteur académique[1345].

Ajoutons que les années 1990 ont aussi été marquées par une multiplication d'attaques contre les humanitaires venant notamment de groupes armés. Il s'en est suivi la structuration et la professionnalisation au sein du secteur d'acteurs de la sécurité, ce qui est allé de pair avec la formalisation de normes régulant les conduites afin de protéger les travailleurs humanitaires. Mais si les ONG clament qu'elles ne sont pas des cibles (« not a target »), et plaident pour un arrêt des enlèvements d'humanitaires et des bombardements d'hôpitaux. Ce slogan est maintenant décliné dans une version « modernisée » : les ONG ne sont pas des cibles numériques (« not a digital target »). Il constitue un appel à stopper les cyberopérations contre les ONG, qui sont, comme on le verra, largement victimes des affrontements agitant le terrain numérique. Et cet appel est fait non seulement au nom de la vie privée des individus, mais aussi au nom de leur sécurité. Peter Maurer, ancien président du CICR, enjoint ainsi la communauté humanitaire à « unir nos forces — et trouver des partenaires — pour assurer la meilleure protection possible contre les cyber-opérations visant les opérations humanitaires et les données personnelles qui nous sont confiées »[1346]. En dépit de ce discours, les acteurs de la sécurité des ONG humanitaires habitués à gérer les accidents ayant lieu sur le plan physique (enlèvement, rançons, assassinats, etc.) prennent encore peu en compte les « nouvelles menaces ». Les cyberattaques ne sont pas encore considérées comme des « accidents de sécurité » affectant les humanitaires. Pour les bénéficiaires, la situation est différente. Leur protection face aux cyberopérations commence à être envisagée. S'il est question de cyberconflictualités, certains acteurs cherchent à vouloir attirer l'attention sur leurs répercussions sur les civils. En effet, les États sécurisent le cyberespace, le rattachent à leur stratégie de défense au nom de la préservation d'intérêts nationaux. Mais d'autres acteurs militent pour une plus grande prise en compte des individus dans les politiques de cybersécurité. Et il commence — parmi les ONG de défense des droits de l'homme ou les organes onusiens — à être question de « sécurité humaine numérique ». Cette expression fait écho aux théories de la « sécurité humaine », forgées au cours des années 1990 et qui a correspondu à un « élargissement » de la notion de sécurité des intérêts régaliens aux civils. Pour notre part, on détaillera dans un premier temps ce qui est entendu par « sécurité humaine numérique ». On essayera de comprendre quels types d'acteurs défendent cette approche et souhaitent inscrire la défense de la société civile et des individus, voire des droits de l'homme (et donc aussi du droit à la vie privée), au cœur des politiques de régulation du cyberespace. En tout cas, on verra que le CICR se distingue légèrement de ces approches et se réfère majoritairement au DIH (et non pas aux droits de l'homme) comme outil de protection

[1345] MARCHAL, Roland, MESSIANT Christine, « Les guerres civiles à l'ère de la globalisation. Nouvelles réalités et nouveaux paradigmes », *Critique internationale*, 2003/1 (n° 18), p. 91-112. https://www.cairn.info/revue-critique-internationale-2003-1-page-91.htm

[1346] "join forces – and find partners – to ensure the best possible protection against cyber operations targeting humanitarian operations and personal data entrusted to us"
MAURER, Peter, "The digitalization of armed conflicts : three humanitarian priorities", CSDS Policy Brief, The Centre for Security, diplomacy and Strategy, 13/06/2022 https://brussels-school.be/sites/default/files/CSDS%20Policy%20brief_2214.pdf

des civils dans le contexte de numérisation des guerres contemporaines[1347]. Cette approche n'est pas sans limites, notamment parce que le DIH ne couvre pas l'ensemble des cyber-opérations. Il reste à savoir si la non prise en compte des atteintes à la vie privée représente un manque en matière de protection des bénéficiaires

Mais à vrai dire, quel terme utiliser pour décrire ces différentes formes d'attaques ? On parle tour à tour de menace cyber, de cyber-risque, de cybercriminalité, de cyberopération, d'accident cyber, de cyberattaque, de piratages, etc.[1348] Elles sont en outre d'intensité et de nature très diverses. Et elles vont du simple « bug » informatique, à des « défacement » (l'écran de l'ordinateur étant remplacé par un fond uni). Il s'agit d'attaque non ciblées, opportunistes, ou encore des attaques très sophistiquées de type « advanced persistent threat » (APT). Ce terme désignant des attaques sophistiquées au long cours, ciblant un acteur précis pour des motifs stratégiques, soit un type de cyberopération nécessitant une motivation. De par leurs complexités, il s'agit d'acteurs généralement étatiques ou soutenu par un Etat. Mais des groupes non étatiques dotés de fortes compétences et ressources peuvent également mener des APT.

Les cyber-opérations peuvent en outre toucher de multiples cibles. Il peut s'agir de petite PME ou des ministères régaliens, des services publics comme les hôpitaux ou universités, ou encore des entreprises industrielles, et notamment leur système d'information, les « Supervisory Control And Data Acquisition » (SCADA). Elles peuvent frapper l'ensemble du réseau informatique, allant des objets connectés (montres, caméras), aux postes informatiques. On assisterait de plus à une rapide évolution des menaces, du fait de l'émergence de nouvelles technologies. On pense au développement de l'IA, et aussi à la course à la faille par des hackeurs, en quête des « failles zero day »[1349]. La variété de la nature des attaques et des cibles implique une très grande multiplicité définitionnelle. Pour simplifier les choses, on peut dire qu'il existe trois types d'agression cyber : espionnage, sabotage et subversion (et par conséquent de désinformation, influence, etc.) Notre étude se concentrera sur les deux premiers types d'événements, puisqu'on travaille sur des enjeux de protection des données et de vie privée.

On abordera un large panel d'actions, qui ont pour point commun de nécessiter de pénétrer un système informatique de façon non autorisée, afin d'avoir accès à des données variées (de code ou de contenu), et ce en vue d'obtenir du renseignement, de manipuler ou de détruire des données ou des infrastructures. On se concentrera majoritairement aux actions menées par des États, puisqu'on s'intéresse aux répercussions du jeu des souverainetés étatiques sur les ONG. Il sera donc a priori moins question de cybercriminalité de type « scam », escroqueries en ligne, ou de rançongiciel qu'un ensemble d'action rentrant dans le jeu d'affrontement entre puissances, ainsi que leurs répercussions sur les ONG. Mais disons d'emblée que l'écosystème de la cybercriminalité sous-traite dans certains cas les actions des

---

[1347] DORMANN, Knut, "Applicability of the Additional Protocols to Computer Network Attacks" ICRChttps://www.icrc.org/en/doc/assets/files/other/applicabilityofihltocna.pdf
DORMANN, Knut, "Computer network attack and international humanitarian law", *Cambridge Review of international affairs*, 19/05/2001

[1348] D'ailleurs l'OTAN établit une compilation des différentes définitions de cyberattaque : https://ccdcoe.org/cyber-definitions.html.

[1349] Il s'agit de vulnérabilité d'un logiciel qui ne sont pas connues par ses développeurs, et qui ne peuvent donc pas faire l'objet d'un correctif.

États[1350], ce qui complique la possibilité de tracer une frontière nette entre les deux mondes. Par exemple, des actions types rançongiciel a priori des actes purement criminels, peuvent servir de camouflage à des opérations d'exfiltration[1351] de données ou être employés dans une stratégie de « cyberguerilla »[1352] dans le cadre de conflits entre États.

Pour ce qui concerne la terminologie à employer, on recourra à l'expression de « cyberopération », traduisant donc la motivation des actions nous intéressant qui sort du motif strictement criminel. Sachant que Stéphane Taillat définit le terme de « cyberopération » comme : « la manipulation, le détournement, l'endommagement, la perturbation, l'interruption ou la destruction d'un réseau ou d'un système d'information à des fins politiques et stratégiques. » Notons d'emblée que le terme de cyberopération est à différencier de la définition d'une cyberattaque selon le CICR (qui n'inclut pas les opérations de renseignement).

Par conséquent, une des finalités de la cybersécurité est de protéger les systèmes d'information contre l'ensemble de ce type d'opération, mais il est aussi possible d'y inclure une dimension offensive, et pour en reprendre la définition de Nicolas Arpagian la cybersécurité concerne « les usages défensifs et offensifs de ces systèmes d'information qui irriguent désormais nos organisations modernes. Elle prend en compte les contenants, c'est-à- dire les moyens techniques (réseaux informatiques, téléphoniques, satellitaires…) utilisés pour l'échange de données, qui peuvent faire l'objet d'opérations d'infiltration, d'altération, de suspension voire d'interruption, comme les contenus, c'est-à-dire l'ensemble des informations qui circulent ou sont stockées sur des supports numériques (sites Internet, bases de données, messageries et communications électroniques, transactions dématérialisées…). »[1353]

## Section 1 — Descriptif des cyber-opérations touchant l'humanitaire

Il est maintenant temps de préciser la nature des cyber-opérations touchant les organisations humanitaires. Mais documenter les cyber-opérations n'est pas une tâche simple. Tout d'abord, il est évident que les accidents ne sont pas tous communiqués, du fait de la sensibilité potentielle du sujet. Cela dit, une bonne partie d'événements se situent en deçà du seuil de ce qui peut constituer un accident et relèvent plutôt du « bug ». La cybersécurité implique en effet aussi la régulation quotidienne de micro-attaques qui sont très loin d'être des « Pearl Harbour numériques ». Ainsi, on peut lire dans un rapport sur la cybersécurité à l'ONU qu' : « il est intéressant, et peut-être surprenant, de constater que dans leurs réponses, les organisations participantes ont invariablement déclaré que l'impact des incidents de

[1350] EGLOFF, Florian, *Semi-State actors in cybersecurity*, Oxford University press, 2021, 294 p.
[1351] MILENKOSKI, Aleksandar, VOGELE, Julian-Ferdinand, "Chamelgang & friends, cyberespionage groups attacking critical infrastructure with ransomware", *SentinelLABS Research Team*, June 2024
https://assets.sentinelone.com/sentinellabs/chamelgang-friends-en
" Des groupes chinois de cyberespionnage utilisent des rançongiciels pour se camoufler", Incyber, 03/07/2024 https://incyber.org/article/groupes-chinois-cyberespionnage-utilisent-rancongiciels-pour-camoufler/
[1352]COLLOMB Cléo, HERNANDEZ Nicolas, « Les attaques par *ransomwares* comme actes de cyber guérilla. Une approche écosystémique de la menace cyber dans le contexte de la guerre en Ukraine », *Études françaises de renseignement et de cyber*, 2023/1 (N° 1), p. 155-176. https://www.cairn.info/revue-etudes-francaises-de-renseignement-et-de-cyber-2023-1-page-155.htm
[1353]ARPAGIAN, Nicolas, *La cybersécurité*, PUF, Que Sais-je?2014,p.4

cybersécurité auxquels elles avaient été confrontées était mineur ou insignifiant, quel que soit le type d'impact. Dans le même temps, il est admis que le nombre et la fréquence des incidents de cybersécurité évités sont considérables, de l'ordre de milliers d'événements par mois, et qu'ils ont augmenté de manière exponentielle ces dernières années. » Elles peuvent être relativement bénignes, de prime abord, mais également invisibles[1354]. Des intrusions peuvent passer inaperçues, étant commises par des « attaquants dormants », ayant pénétré des systèmes informatiques en tentant de laisser le moins de traces possibles en vue de « repérer les lieux » et attendre le moment opportun pour mener leurs opérations. Leur tâche est facilitée par le fait que la plupart des ONG n'ont pas de capacité technique de veille suffisantes pour repérer toutes les anomalies dans le trafic de l'organisation : *« on n'a pas les équipements pour pouvoir faire ça, comment font les entreprises. Il y a des équipements qui enregistrent tout le trafic qui joue sur le réseau, les adresses IP entre autres et en fait ces données sont gardées un certain temps, et les machines analysent les flux. (…) les industriels s'en rendent compte et sortent des patchs pour les services d'exploitation, il y a une veille. (…) Qui peut faire ça ? Il n'y a pas beaucoup de monde dans l'humanitaire qui est capable de faire ça, mon exemple est calé sur WFP dont je connais le fonctionnement interne, ce n'est pas une petite agence, c'est important, même eux ne sont pas capables de le faire, parce qu'ils n'ont pas l'infrastructure pour le faire*. »[1355]

Un autre point de difficulté concerne le manque de prise en compte du secteur de la société civile par les firmes spécialisées en analyse de cybermenace. D'après les chercheurs Lennart Maschmeyer, Ronald J. Deibert et Jon R. Lindsay leurs analyses tendraient à sous-évaluer la place de la société civile et les attaques touchant les pays appartenant aux pays dits du Sud. Une partie de ces firmes ayant plus intérêt à vendre leurs produits au « mieux offrant », à savoir les entreprises[1356]. Ainsi, dans le rapport 2020 de PWC, les ONG sont placées selon les statistiques de la firme à la dernière place. Il n'est évidemment pas possible de déterminer si ce résultat est dû ou non à une sous-évaluation de ce secteur. Il serait ainsi difficile d'estimer la place des ONG au sein du paysage plus global des cyber-opérations. On peut se demander si on retrouve le même biais chez des agences gouvernementales d'analyses de menaces, des acteurs pour lesquels l'intérêt commercial pèse moins. Par exemple, dans le rapport 2023 de l'Agence nationale des systèmes de sécurité et d'information (ANSSI) on peut lire que les attaques contre les associations seraient (à l'échelle française) en augmentation et compteraient pour 9 % du total des attaques en 2023, contre 4 % en 2022[1357].

Toujours est-il que différentes organisations cherchent à remettre l'accent sur la société civile dans l'analyse des menaces cybernétiques. Il s'agit du Citizen Lab, d'Access Now, d'Amnesty International. Cependant, on n'a pas trouvé de référence dans leur documentation disponible publiquement relatives aux attaques touchant des ONG humanitaires (ou alors à des cas

[1354]« Interestingly, and perhaps surprisingly, in their responses participating organizations invariably reported the impact of cybersecurity incidents they had been confronted with as minor or insignificant, irrespective of the impact type. At the same time, it is acknowledged that the number and frequency of averted cybersecurity incidents is considerable, in the range of thousands of events per month, and has grown exponentially in recent years. »
CALLEJAS, Jorge Flores, AFIFI, Aicha, LOZINSKIY, Nikolay, "cybersecurity in the United nations system organizations",JIU/REP/2021/3
https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2021_3_english.pdf
[1355] Entretien n°26, ONG8, Ingénieur, 31/03/2020
[1356] MASCHMEYER, Lennart, DEIBERT, Ronald J., LINDSAY, Jon R. "A tale of two cybers - how threat reporting by cybersecurity firms systematically underrepresents threats to civil society", *Journal of Information Technology & Politics*, 18:1, 2021, p. 1-20.
[1357] Cyber threats overthrew, 2023, https://www.cert.ssi.gouv.fr/uploads/CERTFR-2024-CTI-002.pdf

isolés, comme celle ayant touché le CICR en 2022), bien que ce type d'organisme documente largement d'attaques contre la société civile et des « minorités », à savoir des journalistes, des militants des droits de l'homme, des diasporas, la communauté LGBT+, etc.

Le Cyberpeace Institute inclut au contraire directement dans son travail d'analyse le secteur humanitaire. L'organisation vient de publier fin novembre 2023 un rapport quantitatif concernant la perception de la cybersécurité par 27 ONG genevoises intervenant dans différents secteurs : domaine médico-social, droits humains, politiques de développement et humanitaire[1358]. On a pu l'utiliser comme source, mais ce dernier n'est pas dépourvu de limites. Tout d'abord, le rapport ne différencie pas nécessairement les attaques par type d'ONG, ce qui fait qu'on ne peut pas être assuré qu'elles concernent les humanitaires. Et surtout, ces résultats dépendent de sources publiques. Le Cyberpeace Institute réalise une veille sur les médias sociaux, les rapports des gouvernements et de la société civile. Cléo Collomb et Nicolas Hernandez pointent les limites d'une telle méthodologie : un bon nombre d'entités ayant subi une attaque ne la déclare pas. Les chercheurs proposent une autre méthodologie, par extraction automatique de données (scrapping) sur les forums de hackeurs dédiés à la publication de données. Cela dit, il semblerait que nos limites soient les mêmes que celles du Cyberpeace Institute, nous n'avons pu utiliser une pareille méthodologie dans le cadre de nos recherches. Notre tableau des cyber-opérations touchant l'humanitaire est donc une ébauche, donnant un premier aperçu du phénomène.

À côté du travail du Cyberpeace Institute, il existe un autre projet visant à combler les lacunes de documentation des cyberattaques : l'« UnderServed Project ». Son objectif est de développer une plateforme pour rapporter et analyser des menaces touchant des secteurs qui sont vulnérables aux cyberattaques, mais qui manquent encore de ressources pour y faire face[1359]. À cette heure, il n'a pas rendu de rapports disponibles publiquement.

En somme, on a dû se rabattre sur le travail des organismes spécialisés en « renseignement des menaces » (threat intelligence) comme FireEye, Mendiant, Microsoft, etc. La société civile y est peu représentée, mais par agrégation de documents nous avons pu obtenir des informations exploitables. Et pour compléter ces sources, on a collecté du matériel empirique à base de coupures de presse. Sachant qu'une part des articles citent les rapports des firmes spécialisées dans le renseignement numérique. Donc, encore une fois, notre approche est tout à fait descriptive et non pas quantitative, du fait des limites précitées. Il s'agit donc d'un premier aperçu non exhaustif du paysage du risque cyber touchant les acteurs humanitaires.

Nous avons fait le choix d'opter pour un classement thématique (et non pas chronologique), en traitant à part les cyber-opérations s'inscrivant dans le cadre de conflits armés, notamment lors du conflit ukrainien. On a pu déduire de notre travail que les humanitaires sont concernés au moins par trois types de cyber-opérations. Un premier type d'action englobe les cyber-opérations ciblant les données des donateurs, pouvant se traduire par des rançongiciels. La

---

[1358] Cyberpeace institute, "NGOs serving humanity at risk: cyber threats affecting international Geneva", November 2023. https://cyberpeaceinstitute.org/wp-content/uploads/CyberPeace_Analytical%20Report_NGO.pdf

[1359] https://underserved-project.eu/?utm_medium=email&_hsmi=278032052&_hsenc=p2ANqtz--EWt4AXs4ipqftwfeg7hR_ru3OHyWPEfJkXFzCVAswXzNCnzS7K_QZaih4vxXC3_kX8Sge6Z7fg6AxX-JfF597LLhIrdvL2aNfliLXgrU-M7ojr7E&utm_content=278032052&utm_source=hs_email

BENBOUZID, Bilel, VENTRE, Daniel, « Pour une sociologie du crime en ligne. Hackers malveillants, cybervictimations, traces du web et reconfigurations du *policing* », *Réseaux*, 2016/3-4 (n° 197-198), p. 9-30. https://www.cairn.info/revue-reseaux-2016-3-page-9.htm

finalité de ce type d'action est alors principalement financière, quand bien même elles ont un effet déstabilisateur et peuvent s'inscrire dans des stratégies de sabotage et de cyberguérilla, et se traduire par la publication de données des victimes sur le dark web[1360] . D'autres actions ont pour finalité directe la collecte de renseignement. Enfin, une catégorie de cyber-opération vise à déstabiliser les ONG dans des cadres de conflits. Ce type d'attaques constitue une forme d'instrumentalisation, de « weaponization » de l'aide, pour reprendre l'expression de Marietje Schaake, ancienne directrice du Cyberpeace institute. [1361]Dans ce dernier cas, l'objectif est bien souvent de paralyser le fonctionnement d'une organisation, par des attaques de défacement (DDoS), ou par suppression de données (par « wiper »).

Pour rentrer dans le vif du sujet, une bonne part des cyberattaques contre des ONG ont tout d'abord des motivations financières. Elles prennent la forme de rançongiciels[1362] et touchent les bases de données de donateurs. Ainsi, un sous-traitant d'ONG internationale et de bailleurs de fonds, Blackbaud (firme gérant des données de donateurs), a été attaqué par un logiciel malveillant courant 2020. [1363] D'après la presse, 200 clients de Blackbaud auraient été concernés. Parmi les victimes déclarées, on compte les ONG World Vision, Save the Children, Mercy Corps et Human Rights Watch. Dans un communiqué, Mercy Corps précise qu'ont pu être consultées les données suivantes : noms des donateurs, adresses, numéros de téléphone, adresses mail, date de naissance. Selon l'ONG, aucune donnée bancaire de type numéro de compte ou de carte de crédit n'aurait été compromise. Le début de l'attaque remonte à février 2020, et se clôt en mai 2020. Blackbaud aurait payé la rançon face à la menace de suppression de données[1364].

D'autres exemples parlants peuvent être mentionnés. Tout d'abord, l'ONG Roots of Peace, intervenant en Afghanistan, a été ciblée par une attaque de type « fraude au président », entrainant le transfert de 500 000 de dollars à un compte bancaire chinois[1365]. Une base de données de donateurs d'Oxfam Australia a été hackée en janvier 2021, ont été dérobés des

---

[1360] COLLOMB, Cléo, HERNANDEZ Nicolas, « Les attaques par *ransomwares* comme actes de cyber guérilla. Une approche écosystémique de la menace cyber dans le contexte de la guerre en Ukraine », *Études françaises de renseignement et de cyber*, 2023/1 (N° 1), p. 155-176. https://www.cairn.info/revue-etudes-francaises-de-renseignement-et-de-cyber-2023-1-page-155.htm

[1361]Nous reprenons cette expression à Marietje Schaake au sujet des cyberattaques touchant les ONG, sachant qu'elle l'a employée dans une conférence organisée par le Digitharium du CICR datant de 2021, soit avant l'invasion russe de 2022, et qu'elle est tout d'abord utilisée par l'historien Mark Galeotti, elle implique de considérer que tout entité peut être utilisée dans le cadre d'un affrontement, concernant l'humanitaire elle implique l'instrumentalisation de cette dernière dans le cadre d'une stratégie guerrière.

[1362] En rappelant encore que les effets des ransownware ne sont pas qu'économiques, mais comme le proposent Cléo Collomb et Nicolas Hernandez, elles peuvent s'inscrire dans des stratégies de déstabilisation dans des confrontations inter-étatiques. « Nous avons ici proposé de comprendre les attaques par ransomwares à l'aune du concept de cyber guérilla pour donner à voir le rôle que ces derniers sont susceptibles de jouer dans les combats numériques. Les ransomwares ont évolué depuis 2015 et leur transformation s'est précipitée depuis l'invasion de l'Ukraine par la Russie en février 2022. Ils ont changé de nature, en procédant par double (voire triple et quadruple) extorsion, impliquant la publication des données – et plus seulement leur chiffrement. Si cette publication est un moyen de faire pression sur les victimes, elle constitue également une ouverture au renseignement. » COLLOMB Cléo, HERNANDEZ Nicolas, « Les attaques par *ransomwares* comme actes de cyber guérilla. Une approche écosystémique de la menace cyber dans le contexte de la guerre en Ukraine », *Études françaises de renseignement et de cyber*, 2023/1 (N° 1), p. 155-176. https://www.cairn.info/revue-etudes-francaises-de-renseignement-et-de-cyber-2023-1-page-155.htm

« were paid an undisclosed ransom to return the data and delete any copies ».

PARKER, Ben, "Dozen of NGOs hit by hack on US fundrasing database", *The New Humanitarian*, 04/08/2020https://www.thenewhumanitarian.org/news/2020/08/04/NGO-fundraising-database-hack

[1363] MERCY CORPS,"Statement on blackbaud security incident", 26/08/2020 https://www.mercycorps.org/press-room/releases/statement-blackbaud-security-incident

[1364] MERCY CORPS,*ibid.*

[1365] Cyberpeace Institute, "Hackers trick humanitarian non-profit into big wire transfers", 14/07/2020 https://cyberpeaceinstitute.org/news/2020-07-14-hackers-trick-humanitarian-non-profit-into-big-wire-transfers/

noms, des adresses, des dates de naissance, des emails, numéro de téléphone, etc. Oxfam Australia n'a pas précisé le nombre de personnes concernées, mais d'après la presse, jusqu'à 1 million de donateurs pourraient avoir été impactés par l'attaque[1366]. Autre cas, Pareto Phone, une firme de télémarketing utilisée par des ONG pour le ciblage de donateurs, a été touché par un rançongiciel dans le courant de l'été 2023. L'attaque aurait été menée par le groupe de hackeurs Lockbit[1367]. Enfin, les actions de type « scam » sont aussi monnaie courante. Lors du tremblement de terre en Turquie ou au Maroc, de telles opérations se sont ainsi multipliées, l'objectif des attaquants était d'« arnaquer » des donateurs potentiels, via des campagnes de phishing[1368].

Les ONG subissent aussi des cyberopérations dont la finalité est la surveillance et/ou la collecte d'information et de renseignement, pouvant relever dans certains cas de cyberespionnage. Premier exemple, des acteurs opérant au sein de l'appareil étatique chinois peuvent ainsi mener des opérations de déstabilisation à l'égard d'opposants ou d'exilés[1369] et de minorités persécutées comme les Ouïghours[1370], soit des catégories de personnes auxquelles les humanitaires peuvent porter assistance. On aurait affaire a priori à des opérations ayant comme finalité la surveillance d'opposants au régime chinois afin d'exercer une forme de pression sur ces derniers. Sachant que les formes de contrôle de la diaspora recourent à une diversité de moyens dépassant le seul domaine numérique. Ceci étant dit, on peut citer les actions d'un groupe sponsorisé par le gouvernement chinois, et baptisé RedAlpha. D'après la firme d'analyse de menace The Recorded, le groupe aurait mené une campagne de « phising » à l'encontre de membres de la société civile. En ont été victimes des ONG de droits de l'homme et des ONG humanitaires, des acteurs gouvernementaux engagés auprès de minorités, dont des Ouïghours, ou des Tibétains. The Recorded affirme ainsi que : « le ciblage et l'usurpation par RedAlpha d'organisations telles qu'Amnesty International et la FIDH, liées à l'action humanitaire et aux droits de l'homme, sont particulièrement préoccupantes compte tenu des violations des droits de l'homme commises par le Parti communiste chinois à l'encontre des Ouïghours, des Tibétains et d'autres groupes minoritaires ethniques et religieux en Chine. »[1371]

L'attaque qui suit ne concerne pas directement une ONG humanitaire, mais elle illustre le type de risques encourus par ces dernières. En juillet 2024 a été signalée une fuite de données

---

[1366] "Oxfam Australia Data incident", 26/03/2021https://www.oxfam.org.au/updates-suspected-data-incident/

[1367] https://msf.org.au/article/statements-opinion/notification-privacy-act-sections-26wk-26wl

[1368] BIZGA, Alina, "Cybercriminals exploit human misery in earthquake-hit Turkey and Syria with new online disaster scam", *Bitdefender,* 07/02/2023, https://www.bitdefender.com/blog/hotforsecurity/cybercriminals-exploit-human-misery-in-earthquake-hit-turkey-and-syria-with-new-online-disaster-scam/

[1369] "110 Overseas, Chinese Transnational policing gone Wild", Safeguard Defenders, 2022 https://safeguarddefenders.com/sites/default/files/pdf/110%20Overseas%20%28v5%29.pdf

[1370] "Targeted in Türkiye : China's transnational repression against Uyghur", Safeguard Defender, 2023 https://safeguarddefenders.com/sites/default/files/pdf/TARGETED%20IN%20TURKIYE%20.pdf

BRADLEY, Jardine, "Great Wall of Steel : China's Global Campaign to suppress the Uyghurs", Wilson Center, 2022

HALL, Natalie, BRADLEY, Jardine, ""Your family will suffer": how China is Hacking, surveilling, and Intimidating Uyghurs in Liberal democracies", The Oxus Society for Central Asian Affairs, 2021 https://uhrp.org/wp-content/uploads/2021/11/UHRP-Your-Family-Will-Suffer-Report.pdf

[1371] "RedAlpha's humanitarian and human rights-linked targeting and spoofing of organizations such as Amnesty International and FIDH is particularly concerning given the CCP's reported human rights abuses in relation to Uyghurs, Tibetans, and other ethnic and religious minority groups in China"

The Record, "RedAlpha conducts multi-Year credential theft campaign targeting global humanitarian, think tank, and government organizations", 16/08/2022 https://www.recordedfuture.com/blog/redalpha-credential-theft-campaign-targeting-humanitarian-thinktank

touchant jusqu'à 3 millions d'exilés syriens. Il s'agit de passeport et de données personnelles. Les données ont été publiées sur un groupe Telegram appelant à commettre des violences contre des réfugiés syriens. La fuite a eu lieu alors que des émeutes contre la communauté syrienne ont touché la Turquie courant juillet[1372], les exilés ont aussi craints que ces informations soient réutilisées par le gouvernement d'Assad à des finalités de répression[1373]. Les médias ne donnent pas de précision sur la source (sur les acteurs gérant les serveurs stockant ces données) ni sur les modalités de l'attaque. La direction de la gestion de l'immigration — rattaché au ministère de l'Intérieur — a déclaré qu'« une enquête à grande échelle a été lancée afin de déterminer l'ancienneté de ces données, leur source et la date à laquelle elles ont été obtenues, et de fournir au public des informations fiables. » [1374] L'UNHCR aurait été contacté par des exilés craignant pour leur sécurité[1375], l'agence n'a pas fait de commentaire public, au regret Noura Aljizawi, chercheuse Citizen Lab, pour qui l'UNHCR n'aurait pas rempli son rôle de protection des réfugiés : « Ni le gouvernement ni le HCR n'ont proposé une quelconque forme de soutien aux personnes touchées, les laissant seules, vulnérables à l'exploitation et aux dommages potentiels. (…) Le silence du HCR est alarmant et reflète un modèle plus large de négligence internationale concernant les droits numériques des réfugiés. Les agences de l'ONU et les organisations internationales ont un rôle essentiel à jouer, non seulement en fournissant des fonds et en créant des programmes de soutien spécifiques, mais aussi en développant un cadre international pour la protection des données des réfugiés et en plaidant en faveur de la protection des droits numériques des personnes déplacées. » [1376]

Quant aux actes stricts de cyberespionnage, ils peuvent regrouper différentes modalités d'action et être menés par des acteurs très variés. Ce terme désigne l'accès non autorisé à des ordinateurs, à des systèmes informatiques ou à des réseaux. Et ce *afin d'obtenir des informations*, sans affecter la fonctionnalité du système auquel on accède ni effacer les données qu'il contient ou qui y transitent. Précisons que ces opérations de cyberespionnages peuvent s'inscrire dans une catégorie plus vaste d'opérations, regroupant l'ensemble des

---

[1372] BOURCIER, Nicolas, " Réfugiés syriens attaqués en Turquie : " La crise fait de nous les parfaits boucs émissaires", Le Monde, 16/07/2024 https://www.lemonde.fr/international/article/2024/07/16/refugies-syriens-attaques-en-turquie-la-crise-fait-de-nous-les-parfaits-boucs-emissaires_6250514_3210.html

[1373]SOYLU, Ragip, KEMAL, Levent, "Turkey: Passports belonging to millions of Syrians leaked", Middle East Eye, 05/07/2024 https://www.middleeasteye.net/news/turkey-passports-belonging-millions-syrians-leaked

[1374]" Bu nedenle bu verilerin hangi yıllara ait olduğunun, hangi kaynaktan, hangi tarihte alındığının belirlenebilmesi ve kamuoyuna sağlıklı bilgi verilmesi için geniş çaplı soruşturma başlatılmıştır."Ülkemizde Geçici Koruma Kapsamında Bulunan Suriyelilerin Kimlik Bilgilerinin Sızdırıldığı İddialarına İlişkin Basın Açıklaması, 05.07.2024 https://www.goc.gov.tr/ulkemizde-gecici-koruma-kapsaminda-bulunan-suriyelilerin-kimlik-bilgilerinin-sizdirildigi-iddialarina-iliskin-basin-aciklamasi

[1375] « Suite à la fuite massive de données personnelles de 3,3 millions de Syriens vivant en Turquie le 4 juillet, l'Agence des Nations Unies pour les réfugiés (UNHCR) a reçu des appels « par le biais de ses lignes de conseil nationales de la part de Syriens exprimant leurs inquiétudes quant à l'impact de la fuite de données sur leur sécurité », a déclaré Selin Unal, porte-parole de l'UNHCR en Turquie, à The Syria Report. « "Following the massive leak of personal data of 3.3 million Syrians living in Turkey on July 4, the U.N. Refugee Agency (UNHCR) has received calls "through its national counselling lines from Syrians expressing concerns that data leak may impact their safety," Selin Unal, UNHCR Turkey spokesperson told The Syria Report." Syrian Refugees in Turkey Face Fraud and Security Risks After Massive Data Leak 16/07/2024 https://syria-report.com/syrian-refugees-in-turkey-face-fraud-and-security-risks-after-massive-data-leak/

[1376] « Furthermore, neither the government nor the UNHCR have offered any form of support for affected individuals, leaving them alone, vulnerable to further exploitation and harm. »
UNHCR's silence is alarming and it reflects a broader pattern of international neglect regarding refugees' digital rights. UN agencies and international organizations have a vital role to play—not only in providing funding and creating dedicated support programs but also in developing an international framework for refugees' data protection and advocating for protecting displaced people's digital rights." ALJIZAWI, Noura, "Locked in, locked out : how data breaches shatter refuggees"safety", The Tahrir Institute for middle East Policy,21/08/2024 https://timep.org/2024/08/21/locked-in-locked-out-how-data-breaches-shatter-refugees-safety/

actes imputables à des agences de renseignement[1377]. Ajoutons que les modalités d'intrusion sont variées, et que dans certain cas, la collecte de renseignements ne se fait pas par une intrusion directe dans un système d'information. Par exemple, des données publiées sur le darknet à la suite d'opérations ayant des motivations a priori économiques comme un rançongiciel peuvent être employées dans un second temps à des finalités de renseignement[1378]. Encore une fois, il est toujours difficile d'en attribuer les motifs des attaques ainsi que leurs auteurs et leurs relations avec des gouvernements : les liens entre ces derniers et des groupes de hackeurs peuvent être très fluides[1379].

Toujours est-il qu'on peut commencer par noter qu'il est très peu probable que des opérations d'intelligence économique soient menées à l'encontre d'humanitaires. Sur ce sujet, il existe bien un exemple de cyberopération, mais qui relève plutôt des rivalités économiques entre entreprises privées qu'entre Etats. L'exemple concerne Emerson Tan, le président de Mautinoa Technologies, qui a déclaré avoir trouvé une faille de sécurité dans le logiciel RedRose, une entreprise concurrente. Cette dernière édite un logiciel de gestion de données de programmes de Cash Transfert utilisé par le Catholic Relief Services, en Afrique de l'Ouest. L'objectif n'était a priori pas de collecter de l'information sur un concurrent, mais clairement de déstabiliser un compétiteur. L'attaquant a pu en effet pénétrer le serveur cloud de l'ONG et a pu consulter des données de plus de 8 000 bénéficiaires situés en Afrique de l'Ouest, soit des noms, des photographies, des détails sur les compositions des familles, des codes PIN[1380].

Les ONG humanitaires sont plus communément victimes d'opérations de cyber-espionnage menées par des acteurs étatiques et/ou para-étatiques. D'ailleurs, Edward Snowden a révélé que des ONG humanitaires ont été surveillées par la NSA et l'agence britannique GCHQ. Il

[1377]« in the cyber domain, intelligence does not stop at espionage. Intelligence agencies conduct operations in the digital domain that clearly resemble aspects of covert action, while stopping short of the highest level of violence, i.e. there are no cyber assassinations (even if targeting is greatly enhanced). Indeed, the Internet is not just a natural environment for mass-scale espionage; it is also very well suited to intelligence-led covert operations. This includes information operations (such as disinformation campaigns and elections interference), all kinds of subversive operations (such as hack and leak operations and the political use of ransomware) and sabotage operations (such as Stuxnet and NotPetya). » »Dans le domaine cybernétique, le renseignement ne s'arrête pas à l'espionnage. Les agences de renseignement mènent des opérations dans le domaine numérique qui ressemblent clairement à des actions secrètes, tout en s'arrêtant au niveau de violence le plus élevé, c'est-à-dire qu'il n'y a pas de cyber-assassinats (même si le ciblage est grandement amélioré). En effet, l'internet n'est pas seulement un environnement naturel pour l'espionnage de masse ; il est également très bien adapté aux opérations secrètes menées par les services de renseignement. Il s'agit notamment d'opérations d'information (telles que les campagnes de désinformation et l'ingérence dans les élections), de toutes sortes d'opérations subversives (telles que les opérations de piratage et de fuite et l'utilisation politique des ransomwares) et d'opérations de sabotage (telles que Stuxnet et NotPetya). »BROEDERS, Bennis, KAVANAGH, "Shades of grey : cyber interlligence and (inter)national security", EU cyber direct October 2023 https://eucyberdirect.eu/research/shades-of-grey-cyber-intelligence-and-inter-national-security

[1378] « Les *ransomwares* ont évolué depuis 2015 et leur transformation s'est précipitée depuis l'invasion de l'Ukraine par la Russie en février 2022. Ils ont changé de nature, en procédant par double (voire triple et quadruple) extorsion, impliquant la publication des données – et plus seulement leur chiffrement. Si cette publication est un moyen de faire pression sur les victimes, elle constitue également une ouverture au renseignement. « « les *ransomwares* sont susceptibles de jouer un véritable rôle dans la géopolitique de la conflictualité. Ils fragilisent les écosystèmes d'information, ouvrent la porte au renseignement en diffusant des données sensibles et peuvent menacer par rebond les intérêts des États. « COLLOMB, Cléo, HERNANDEZ, Nicolas, « Les attaques par *ransomwares* comme actes de cyber guérilla. Une approche écosystémique de la menace cyber dans le contexte de la guerre en Ukraine », *Études françaises de renseignement et de cyber*, 2023/1 (N° 1), p. 155-176. https://www.cairn.info/revue-etudes-francaises-de-renseignement-et-de-cyber-2023-1-page-155.htm

[1379] EGLOFF, Florian*, Semi-state actors in cybersecurity*, Oxford University press, 2022, 304 p.

[1380] CORNISH, Lisa, "New security concern raised for RedRose digital payment system", *Devex*, 28/11/2017.https://www.devex.com/news/new-security-concerns-raised-for-redrose-digital-payment-systems-91619
PARKER, Ben, "Security lapses at aid agency leave beneficiary data at risk", *The New humanitarian*, 27/11/2017, https://www.thenewhumanitarian.org/investigations/2017/11/27/security-lapses-aid-agency-leave-beneficiary-data-risk

s'agissait, de l'ONU, du PNUD, d'UNICEF et Médecins du Monde[1381]. Au demeurant, le dernier rapport de Microsoft indique une recrudescence dans les derniers mois de 2023 d'opérations de ce type alors que la majorité des cyberopérations constituait auparavant la destruction d'infrastructure ou des rançongiciels, bien qu'il ne faille pas mettre de côté et sous-estimer ce type d'attaques, dont l'ampleur reste difficilement évaluable. Toujours est-il qu'on peut lire dans le rapport de Microsoft que : « près de la moitié de ces attaques ont parfois visé des États membres de l'OTAN, et plus de 40 % d'entre elles ont visé des organisations gouvernementales ou privées impliquées dans la construction et l'entretien d'infrastructures essentielles. »[1382] Les ONG sont particulièrement vulnérables à ce type d'attaque — du fait de la sensibilité des données qu'elles traitent — mais aussi de la sophistication propre à ce type de cyber-opération, pouvant être qualifiée d'« Advanced persistent threat ». S'en protéger exige de fortes compétences techniques dont les ONG ne disposent pas : « *comme il y a une dimension très technique, pour les cyberattaques de type APT, ça pointe la limite en matière de gestion par la technique. Oui tout à fait, ça se reproduira, c'est le problème, c'est difficile de prévenir, on ne fait que colmater, on a toujours un pas en arrière, souvent ils utilisent des failles qu'on ne connait pas*. »[1383]

La cyberopération de nature étatique la plus retentissante de ces dernières années concerne le CICR. Fin janvier 2022, l'organisation humanitaire s'est aperçue que le serveur d'un sous-traitant suisse hébergeant les données du service de rétablissement de liens familiaux[1384] a été touché par une opération d'infiltration. Environ 500 000 personnes seraient concernées. Les hackeurs ont pu accéder à des données personnelles variées, à des noms, des photos, des données géographiques. D'après nos entretiens avec des membres du CICR, la cyber-opération aurait été découverte lors d'une opération de scan des réseaux par une entreprise de sécurité. L'attaquant a profité de l'existence d'une faille reposant sur un correctif manquant selon la firme. La firme de cybersécurité The Record précise que : « La Croix-Rouge a déclaré que les pirates ont exploité la vulnérabilité CVE-2021-40539[1385] pour prendre pied dans leur réseau. La Croix-Rouge a affirmé que cette vulnérabilité permettait aux attaquants de contourner l'authentification, de placer des coquilles web sur ses serveurs, puis de se déplacer latéralement dans son réseau et de compromettre les informations d'identification de l'administrateur[1386] ; le CICR a confirmé cette analyse en étant sur ce point relativement transparent, et en consacrant une page web de leur site à une description de l'attaque : « une

---

[1381] BALL, James, HOPKINS, Nick, "GCHQ and NSA targeted charities, Germans, Israeli PM and EU chief", *The Guardian*, 20/12/2013 https://www.theguardian.com/uk-news/2013/dec/20/gchq-targeted-aid-agencies-german-government-eu-commissioner
Le Monde, « Médecins du monde, Total, Unicef : la surveillance tous azimuts de la NSA », 20/12/2013. https://www.lemonde.fr/technologies/article/2013/12/20/medecins-du-monde-total-unicef-la-surveillance-tous-azimuts-de-la-nsa_4338321_651865.html

[1382] "At times, nearly half of these attacks targeted NATO member states, and more than 40% were leveled against government or private sector organizations involved in building and maintaining critical infrastructure."
Microsoft Threat intelligence, "Microsoft digital defense report, Building and improving cyber resilience", October 2023.

[1383] Entretien n° 93, OI 2, DPO, ingénieur, 02/06/2023

[1384] Les activités de rétablissement de liens familiaux menées par le CICR permettent de retrouver la trace de disparus dans le cadre de conflits ou de catastrophes naturelles https://www.croix-rouge.fr/retablissement-des-liens-familiaux

[1385] Cette dernière avait été publicisée depuis septembre 2021. « APT Actors Exploiting Newly Identified Vulnerability in ManageEngine ADSelfService Plus", CISA, https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-259a

[1386] « The Red Cross said the hackers used an exploit for the CVE-2021-40539 vulnerability to gain an initial foothold inside their network.Impacting the Zoho ManageEngine ADSelfService Plus, a password management and single sign-on (SSO) solution from Indian company Zoho, the Red Cross said this vulnerability allowed attackers to bypass authentication, place web shells on its servers, and then move laterally across its network and compromise administrator credentials. »CIMPANU, Catalin, "Red Cross blames hack on Zoho vulnerability, suspect APT attack", *The Record*, 16/02/2022 https://therecord.media/red-cross-blames-hack-on-zoho-vulnerability-suspects-apt-attack

fois à l'intérieur de notre réseau, les pirates ont pu déployer des outils de sécurité offensive qui leur ont permis de se faire passer pour des utilisateurs autorisés ou des administrateurs. Ils ont pu ensuite accéder aux données, bien que celles-ci soient cryptées. »[1387]

Selon l'organisation humanitaire, les attaquants étaient « dormants » : « *on sait qu'il y avait quelqu'un depuis au moins novembre, tapis, ils captaient tout ce qui se passait. (…) On a débranché la base de données, on a tout mis « off line » pour éviter que toutes les personnes captent plus de données*. « *ils ont tenu à être discrets, s'installer dans le temps, être discrets, sans notre intervention, on ne s'en serait pas rendu compte*. »[1388]

Cette discrétion peut être interprétée au moins de deux manières : soit les attaquants en étaient à la première phase d'une attaque, ils effectuaient un repérage des lieux avant le lancement de l'opération en tant que telle ; soit leur objectif était la collecte de renseignement à des fins de surveillance et/ou de collecte d'informations. Les données n'ont pas été manipulées ou supprimées, comme nous le précise un enquêté « *Nous ne pensons pas que les données aient été altérées à ce stade, mais pour en être sûrs, nous faisons appel à une société d'audit indépendante pour le confirmer.* » [1389] Aucune revendication n'a été faite. Le CICR a affirmé que les données n'ont pas été mises en vente sur le « dark web ». Un journaliste prétend le contraire[1390], cela a été le cas pour une cyberopération ayant touché la Croix-Rouge Italienne en juin 2024[1391]. Pour le CICR, en l'absence de sources supplémentaires, nous ne tranchons pas sur ce point.

L'attaque serait de nature étatique, comme l'a communiqué le CICR. Nos enquêtés ne sont cependant pas tous formels sur ce point. Certains restent prudents lors de nos entretiens : « *on s'est rendu compte qu'il y avait une entité, c'est difficile de dire que c'est un État, un groupe d'individus* ». Et d'autres enquêtés sont plus catégoriques : « *en raison de sa sophistication, on pense qu'il a été soutenu par un État.* » [1392] En tout cas, le CICR a déclaré à la presse que le hack peut être considéré comme une opération de type Advanced Persistent Threat (APT) ou menace persistante avancée[1393]. Le CICR ne l'a cependant pas attribuée publiquement à un État précis. Or la vulnérabilité CVE-2021-40539 dont ont profité les hackeurs ayant ciblé le CICR aurait été en grande partie exploitée, selon plusieurs rapports de groupes d'analystes en menace cyber, par des acteurs chinois de type APT, et plus

---

[1387] We do not believe that the data has been tampered with at this time, but to be sure we are hiring an independent audit firm to confirm this CICR." "Cyberattaque contre le CICR : le point sur ce que nous savons », 16/02/2022. (MAJ 29/06/2022) https://www.icrc.org/fr/document/cyberattaque-cicr-ce-que-nous-savons
le terme « tampered » consiste en cybersécurité au fait de modifier de façon intentionnelle mais sans autorisation un système, un composant du système, ou ses données.

[1388] Entretien n°91, OI2, DPO, juriste, 26/05/2023

[1389] "Cyber-attack on ICRC: What we know", 21/02/2022 https://reliefweb.int/report/world/cyber-attack-icrc-what-we-know-enarrude

[1390] SEYDTAGHIA, Anouch, « Les données volées du CICR seraient désormais en vente », *Le Temps,* 22/02/2022https://www.letemps.ch/monde/donnees-volees-cicr-seraient-desormais-vente

[1391] «Actuellement, une partie des données volées à la Croix-Rouge italienne se trouvent mises à disposition sur le darknet. Sur ce réseau parallèle, des pirates livrent des échantillons de ces informations, concernant des migrants et des réfugiés - on parle de données très personnelles, comme des photos, des documents d'identité et des formulaires de la Croix-Rouge italienne. »SEYDTAGHIA, Anouch, BUSSARD, Stéphane, « La Croix-Rouge italienne touchée par une fuite massive de données, le CICR enquête *», le Temps*, 19/06/2024 https://www.letemps.ch/cyber/cybersecurite/le-cicr-a-nouveau-touche-par-une-fuite-massive-de-donnees

[1392] Entretien n° 91, OI2 DPO, juriste, 26/05/2023

[1393] L 'APT désigne un piratage ciblé. Il est conçu et dirigé contre une cible connue à l'avance. Ces opérations exigent des moyens humains et financiers. Les criminels agissent sur commande : vol de données, sabotage. DU fait des moyens requis, ils sont généralement liés à des acteurs étatiques.

précisément par le groupe Volt Typhoon[1394]. Depuis mi-2021, Volt Typhoon est surtout connu pour avoir activement ciblé des infrastructures états-uniennes (infrastructures électriques, transport, système hydriques, etc.) [1395] Les attaquants sont restés « dormants » (« living on the land » selon l'expression anglophone), toutefois d'après les déclarations de l'agence américaine de cybersécurité leur objectif ne serait pas le renseignement, mais le sabotage d'infrastructures critiques[1396]. Le CISA a averti ainsi début 2024 que « Le choix des cibles et le comportement de Volt Typhoon ne correspondent pas à des opérations traditionnelles de cyberespionnage ou de collecte de renseignements, et les organismes auteurs américains estiment avec une grande certitude que les acteurs de Volt Typhoon se prépositionnent sur les réseaux informatiques afin de pouvoir se déplacer latéralement vers les équipements de télécommunications pour en perturber le fonctionnement. »[1397]

Concernant le CICR, on ne peut pas pour autant trancher sur la nature de l'attaquant. La vulnérabilité CVE-2021-40539 peut être bien sûr exploitée par d'autres groupes de hackers. Ajoutons aussi que d'autres hypothèses ont été avancées quant à l'identité de l'attaquant du CICR. Ainsi, Brian Krebs, un journaliste spécialisé sur les sujets « cyber » et anciennement employé par le Washington Post, affirme qu'il existerait une connexion entre l'attaque du CICR et des acteurs liés à l'Iran[1398]. Il fonde son hypothèse sur le fait qu'un hackeur du nom de « sheriff » aurait déclaré vendre les données du hack du CICR sur le « dark web ». Or ce « sheriff » est enregistré sur le forum de rançongiciels sous une adresse identifiée par le FBI comme étant liée à un groupe menant des opérations d'influences et de désinformations diffusant des récits alignés sur les intérêts iraniens. Toujours est-il que cette hypothèse contredirait la communication publique de l'organisation humanitaire (puisqu'elle déclare qu'elle n'a pas fait l'objet d'un rançongiciel), et qu'à notre connaissance elle n'a pas été reprise par d'autres sources (que ce soient des revues spécialisées ou des agences d'analyse de menace), mis à part le journal en ligne Incyber news[1399].

En guise de conclusion, gardons à l'esprit qu'une bonne part des auteurs d'attaques à visées politiques ne seraient pas identifiés, avec une limite non négligeable : ces chiffres ne se basent que sur des attribution rendues publiques (ce qui n'est donc qu'un aperçu du phénomène). Du moins, c'est ce qu'avance une agence européenne de cybersécurité, l'European Repository of Cyber Incidents.

---

[1394] FALCONE, Robert, WHITE, Jeff, RENALS," Peter, targeted attack campaign against manage Engine ADselfservice plus delivers Godzilla Webshells, nglite trojan and kdcsponge stealer", 07/11/2021
https://unit42.paloaltonetworks.com/manageengine-godzilla-nglite-kdcsponge/

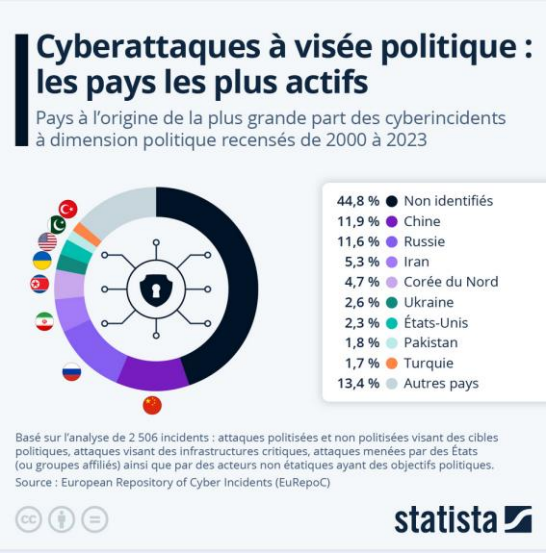
[1395] "Volt Typhoon targets US critical infrastructure with living-off-the-land techniques", Microsoft Defender XDR,24/05/2023 https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/

[1396] TEMPLE-RASTON, Dina, "Neuberger : defining espionage vs. pre-positioning for attacks is key to battling state actors", *The Record*, 15/02/2024 https://therecord.media/volt-typhoon-china-defining-espionage-pre-positioning-neuberger-munich

[1397] "Volt Typhoon's choice of targets and pattern of behavior is not consistent with traditional cyber espionage or intelligence gathering operations, and the U.S. authoring agencies assess with high confidence that Volt Typhoon actors are pre-positioning themselves on IT networks to enable lateral movement to OT assets to disrupt functions"America Cyberdefense Agency, "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure", 07/02/2024 https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

[1398] KREB, Brian, "Red Cross hack linked to iranian influence operation?", *Krebson Security*, 16/02/2022
https://krebsonsecurity.com/2022/02/red-cross-hack-linked-to-iranian-influence-operation/

[1399]"The email of the cybercriminal who sold the data stolen to the International Committee of the Red Cross (ICRC) was also allegedly used to create sites linked to cyber influence from Iran", *InCyber news*, 21/02/2022 https://incyber.org/en/article/red-cross-hack-may-be-linked-to-cybercriminals-operating-for-iran/ https://incyber.org/en/article/red-cross-hack-may-be-linked-to-cybercriminals-operating-for-iran/




L'attribution à un État est un acte politique. Or le CICR a fait le choix de communiquer publiquement sur le fait qu'il était victime d'une attaque étatique sans pointer de gouvernement précis. Ce choix était motivé par la volonté de conserver une position de neutralité tout en envoyant un message souhaité fort et dénoncer le non-respect du DIH. Comme nous l'explique un enquêté : « *mentionner que c'est un État nous permet par la suite d'utiliser cet argument en disant voilà c'était un État c'est pas important lequel… le fait que ce soit un État signifie que c'était un signataire de la Convention de Genève, donc c'est quelqu'un qui nous a pas respectés et c'est ça qu'on a envie de dire, bah voilà il nous a pas respectés (…) ça nous permet d'avoir cette discussion, ce dialogue en disant voilà ça va pas.* » [1400] Un autre enquêté ajoute qu' : « *On n'a pas attribué à un État particulier, c'est en raison de la nature du CICR. Qui reste neutre, dans le cadre d'un conflit, en cas de constat de violation de droits de l'homme, il ne va pas faire de condamnation ouverte, on est dans la diplomatie de couloir, et dans la négociation, à la différence d'Amnesty international ou MSF. Pour moi les deux approches sont complémentaires*. » [1401]

Le CICR a donc tenté de conserver une posture de neutralité, alors que d'après les DPO du CICR le motif des cyberattaquants pourrait être politique : « *Concernant nos hypothèses sur l'objectif, ce n'était pas l'argent, ce n'était pas un ransomware (…) ils auraient pu prendre des données, et les vendre sur le marché noir, c'est ce qu'ont dit les équipes IT. Là c'était plus politique que financier, ils étaient là pour la qualité des renseignements. C'est politique, mais ils n'ont pas fait de revendications, ils n'ont pas fait de coups de pression, on n'a pas établi de communication avec quelque entité, c'était pour leur propre usage.* «[1402]

S'agit-il de cyberespionnage ? On a vu que l'objectif supposé du groupe Volt Typhoon consisterait en des opérations de sabotage d'infrastructure technique ; mais il est fort probable que le CICR ne soit pas lié à cette vague d'attaque. Il existe peu d'élément permettant de trancher sur ce point. La part d'acte de cyberespionnage parmi les attaques

[1400] Entretien n°93, OI2, DPO, ingénieur, 02/06/2023
[1401] Entretien n°91, OI2 DPO, juriste, 26/05/2023
[1402] ibid

liées à des acteurs étatiques reste discutée, selon les analyses des chercheurs Ryan Maness, Brandon Valeriano et Benjamin Jensen, une bonne partie d'entre-elles relèveraient d'acte d'espionnage[1403]. Concernant nos enquêtés, l'objectif de la cyberattaque était pour eux l'exploitation des données du CICR, ce qui implique aussi le caractère ciblé de l'attaque, soit une caractéristiques des APT. Ce point reste discuté au sein de l'organisation : « *est-ce qu'on était vraiment une "target" en tant que CICR ? Moi j'ai pas la réponse. C'est super dur à savoir. Après… De toute façon c'est difficile, je pense qu'il y a des collègues qui doivent savoir d'où ça venait, mais moi je suis pas au courant, mais on sait que c'est arrivé*. »[1404] Un autre enquêté est plus assuré : « *C'étaient des outils de piratages connus, mais le code était construit en sorte de cibler nos serveurs, il a été fait spécifique pour nous, il n'a pas été lancé au hasard.* » [1405]

Concluons en rappelant que, certes, cette cyber-opération a été très médiatisée, et il s'agit d'une des attaques les plus impressionnantes à l'encontre d'une ONG humanitaire, cela dit, elle est loin d'être un cas isolé. Et comme le déclare Cordula Droege actuelle cheffe des services juridiques du CICR : « Depuis lors, nous et d'autres organisations humanitaires avons été attaqués par diverses opérations cybernétiques et d'information visant à extraire des informations, à désactiver nos services ou à saper nos opérations. »[1406]

Ainsi, quelques années plus tôt, en juillet 2019, l'ONU avait été touchée par une attaque. L'ONU l'aurait détectée un mois plus tard. Une alerte aurait été envoyée le 30 aout. Selon un rapport publié le 20 septembre, et auquel la presse a pu avoir accès, 42 serveurs auraient été compromis, 25 seraient suspectés de l'être. Les serveurs seraient liés au Conseil des droits de l'homme et départements RH de l'ONU, localisés à Genève et à Vienne [1407] . Les cyberattaquants n'auraient pas donné de signes d'activité. Encore une fois, ils seraient décrits comme « dormants », ce qui — pour le rapport — pourrait indiquer le fait qu'on ait affaire à un Advanced Persistent Threat (APT), soit des acteurs associés avec des hackeurs étatiques, et potentiellement des campagnes de cyber espionnage. Le rapport ne mentionne pas d'hypothèses sur le nom du groupe et de l'État à l'origine de l'attaque[1408].

Le groupe de hackeurs aurait exploité une vulnérabilité de type CVE-2019-0604, associé à un serveur de Microsoft SharePoint, plateforme intégrée à Microsoft Office. La vulnérabilité n'avait a priori pas fait l'objet d'un correctif par l'ONU : « Le fait que la vulnérabilité ait été divulguée depuis longtemps et que le correctif logiciel ait été déployé depuis longtemps n'est

---

[1403] VALERIANO, Brandon, JENSEN, Benjamin, MANESS, Ryan C., *Cyber strategy : the evolving character of Power and coercion*, Oxford university press, 2020, 320 p.

[1404] Entretien n°93, OI2, DPO, ingénieur, 02/06/2023

[1405] Entretien n°91, OI2, DPO,Juriste, 26/05/2023

[1406]« Since then we and other humanitarian organization actually have been attacked about various cyber and information operation aiming to extract information or disabling our services or undermining our operations. »
« Protecting civilians against digital threats during armed conflict », CICR, 19/10/2023 https://www.icrc.org/en/event/protecting-civilians-against-digital-threats-during-armed-conflict

[1407] WINDER, Davey, "United Nations confirms "serious" cyberattack with 42 core servers compromised", *Forbes*, 30/01/2020, https://www.forbes.com/sites/daveywinder/2020/01/30/united-nations-confirms-serious-cyberattack-with-42-core-servers-compromised/?sh=71e6d5b1633d
MUHLBERG, Byron, "UN Admits data breach from unpatched sharePoint vulnerability", *CPO Magazine*, 10/02/2020. https://www.cpomagazine.com/cyber-security/un-admits-data-breach-from-unpatched-sharepoint-vulnerability/

[1408] WINDER, Davey, "United Nations confirms "serious" cyberattack with 42 core servers compromised", *Forbes*, 30/01/2020 https://www.forbes.com/sites/daveywinder/2020/01/30/united-nations-confirms-serious-cyberattack-with-42-core-servers-compromised/?sh=71e6d5b1633d

pas de bon augure pour une organisation telle que l'ONU. C'est précisément le type de vulnérabilité qui peut être exploitée à distance pour contourner les identifiants, et qui est utilisée par des acteurs sophistiqués de la menace. »[1409] Un officiel onusien interviewé par le journal The New Humanitarian a estimé « qu'au moins 400 Go avaient été téléchargés pendant l'attaque et que la réaction des Nations unies avait "minimisé" le degré de gravité de la situation. » [1410] L'office des droits humains de l'ONU a botté en touche et fait la réponse suivante à un mail du New Humanitarian : « Bien que les pirates aient accédé à une partie autonome de notre système en juillet 2019, les serveurs de développement auxquels ils ont accédé ne contenaient pas de données sensibles ou d'informations confidentielles. Les pirates ont réussi à accéder à notre Active User Directory, qui contient les identifiants de notre personnel et de nos appareils. Ils n'ont toutefois pas réussi à accéder aux mots de passe. Ils n'ont pas non plus réussi à accéder à d'autres parties du système. Dès que nous avons eu connaissance de l'attaque, nous avons pris des mesures pour arrêter les serveurs de développement concernés ». Lors d'une réunion d'information donnée par Stéphane Dujarric, porte-parole du secrétaire général des Nations unies, ce dernier aurait considéré que la cyber-opération n'aurait pas été un « événement marquant ». À la question de savoir pourquoi l'ONU a couvert l'attaque, M. Dujarric a répondu que les serveurs en question « contenaient des données de test non sensibles provenant de deux serveurs de développement utilisés pour des applications web. Les personnes qui devaient être informées l'ont été. »[1411] Cette attaque a fait l'objet d'une couverture médiatique, mais il est évident que l'écosystème onusien est régulièrement la cible de cyber-opérations. Une autre opération a été menée courant 2021, un mot de passe et un identifiant vendus sur le darknet[1412]. Tout récemment, en mars 2024, l'United Nation development program a été la cible d'un rançongiciel entrainant une fuite de donnée sur le « dark web »[1413]. Comme le constate l'United Nations International Computing Centre (UNICC) dans un rapport de 2022 sur le panorama des menaces, les attaques contre l'ensemble des agences onusiennes augmentent en fréquence et gagnent en sévérité. Dans un rapport publié en 2023, l'UNICC avance que selon ses propres

[1409] « That the vulnerability was long-since disclosed, and the software patch long-since rolled out, does not look good for an organization such as the UN. It's precisely the kind of vulnerability that can be exploited remotely to bypass logins, which is employed by sophisticated threat actors. » PARKER, Ben, "EXCLUSIVE : the cyber-attack the UN tried to keep under wraps", *The New Humanitarian*, 29/01/2020, https://www.thenewhumanitarian.org/investigation/2020/01/29/united-nations-cyber-attack

[1410] "at least 400GB had been downloaded during the attack and that the UN response had "downplayed" the level of seriousness. "PARKER, Ben, ibid.

[1411] « Although hackers accessed a self-contained part of our system in July 2019, the development servers they accessed did not hold any sensitive data or confidential information. The hackers did manage to access our Active User Directory, which contains the user IDs for our staff and devices. However, they did not succeed in accessing passwords. Nor did they gain access to other parts of the system. Once we became aware of the attack, we took action to shut down the affected development servers. »
In a briefing given by Stéphane Dujarric, spokesman for the UN Secretary-General, responded to a question regarding the cyber-attack by saying that it was "not a landmark event." Asked why the UN covered up the attack, Dujarric replied that the servers in question "contained non-sensitive test data from two development servers used for web application. People who needed to be notified were notified
Parker, Ben, ibid.

[1412] « L'ONU victime d'une intrusion informatique en avril », *Le Monde*, 10/09/2021 https://www.lemonde.fr/pixels/article/2021/09/10/l-onu-victime-d-une-intrusion-informatique-en-avril_6094150_4408996.html

[1413]GREIG, Jonathan, "UN agency says data stolen in ransomware attack", *The Record*, 17/04/2024 https://therecord.media/un-agency-data-stolen-ransomware-attack
LOY, Irwin, "Inklings, cyber-attack exposes UN data", *The New Humanitarian*, 17/04/2024, https://www.thenewhumanitarian.org/newsletter/2024/04/17/inklings-cyber-attack-exposes-un-data

analyses au sein de l'ONU, les cyberattaques comporteraient 52 % d'APT, 23 % de cybercrime, 17 % d'attaques d'acteurs qualifiés d'opportunistes[1414] et 8 % d'attaques non attribuées[1415].

Autre exemple, en 2021, des hackers ont utilisé le logo de l'USAID pour lancer une campagne de phishing auprès d'ONG de développement, de défense des droits de l'homme et humanitaire[1416]. 3000 individus ont été ciblés, appartenant à 150 organisations localisées dans 24 pays. Pour chaque cible un outil dédié a été utilisé, et Microsoft rapporte que les attaquants ont pu prendre le contrôle d'un compte de contact de l'USAID, ce qui leur a permis d'envoyer des courriels à des milliers de victimes.

Concernant l'attribution, Microsoft a directement associé l'attaque au groupe russe Nobelium. L'agence de threat intelligence Volexity partage cette analyse, et bien qu'elle « ne puisse pas dire avec certitude qui est à l'origine de ces attaques, l'hypothèse peut être faite qu'il s'agit d'un acteur connu avec lequel Volexity a déjà eu affaire à plusieurs reprises. Cependant, un certain nombre de caractéristiques de l'attaque sont cohérentes avec les tactiques précédemment utilisées par APT29 »[1417] L'objectif de l'opération aurait été du cyber-espionnage : « les analystes soupçonnent que les attaques de Nobelium s'inscrivent dans le cadre d'efforts plus vastes de collecte de renseignements déployés par la Russie pour avoir accès aux politiques étrangères des gouvernements occidentaux et des acteurs de la société civile qu'ils soutiennent, en particulier ceux qui critiquent le Kremlin ou soutiennent le travail électoral en Europe, et pour mieux comprendre ces politiques. »[1418]

Les cyberopérations qu'on a décrites ont eu lieu en contexte de paix, mais elles s'inscrivent dans des dynamiques d'affrontement plus globales. Toutefois, d'autres types d'attaques s'inscrivent directement dans des conflits armés. Pour rappel la frontière entre guerre et paix reste brouillée, et l'idée de cyberopérations menées en soutien à des frappes armées reste

---

[1414] L'UNICC les décrit comme suit : « individu ou groupe qui profite des vulnérabilités pour obtenir un accès non autorisé ou mener des activités malveillantes. Ces acteurs peuvent ne pas avoir de cible spécifique à l'esprit, mais plutôt exploiter toute opportunité qu'ils rencontrent pour accéder à des informations sensibles ou perturber des systèmes. »

[1415] UNICC, "Cybersecurity threat landscape report 2022", April 2023 https://www.unicc.org/wp-content/uploads/2023/05/UNICC-Cyber-Threat-Landscape-Report-2022.pdf

[1416] The New humanitarian, "From cyber-attacks to bot farms : the top tech threats humanitarians face in Ukraine", 09/03/2022 https://www.thenewhumanitarian.org/opinion/2022/03/09/from-cyber-attacks-to-bot-farms

MICROSOFT Threat Intelligence, "New sophiscated email-based attack from Nobelium", 27/05/2021 https://www.microsoft.com/en-us/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/

SATTER, Raphael, SINGH, Kanishka, "Microsoft says group behind SolarWinds hack now targetting government agencies",*Reuters*, 28/05/2021 https://www.reuters.com/technology/microsoft-says-group-behind-solarwinds-hack-now-targetting-government-agencies-2021-05-28/

[1417] « While Volexity cannot say with certainty who is behind these attacks, it does believe it has the earmarks of a known threat actor it has dealt with on several previous occasions. However, a number of attack attributes are consistent with previous tactics used by APT2"CASH, Damien, GRUNZWEIG, Josh, MELTZER, Matthew, KOESSEL, Sean, ADAIR, Steven, LANCASTER, Thomas, "SUSPECTED APT29 operation launches election fraud themed phishing compaingns", *Volexity* 27/05/2021 https://www.volexity.com/blog/2021/05/27/suspected-apt29-operation-launches-election-fraud-themed-phishing-campaigns/

APT29 aka Nobelium, Cozy Bear, IO Sekoia, https://www.sekoia.io/en/glossary/apt29-aka-nobelium-cozy-bear/

[1418] « Analysts suspect Nobelium's attacks were part of wider intelligence-gathering efforts by Russia to gain access and deeper insights into the foreign policies of Western governments and the civil society actors they support, particularly those critical of the Kremlin or supporting elections work in Europe."

NAKASHIMA, Ellen, SHABAN, Hamza, « Russian Governement hackers target civil society groups after compromising USAID email marketing account », *Washington Post*, 28/05/2021

https://www.washingtonpost.com/national-security/russia-hack-usaid-human-rights-groups/2021/05/28/3e996c42-bfae-11eb-9c90-731aff7d9a0d_story.html

The New humanitarian, "From cyber attacks to bot farms : the top tech threats humanitarians face in Ukraine", 09/03/2022 https://www.thenewhumanitarian.org/opinion/2022/03/09/from-cyber-attacks-to-bot-farms

une gageure : ces dernières demandant un certain temps de préparation, dans l'environnement chaotique de la guerre, le déploiement d'armes numériques n'est pas toujours efficace. Les cyberopérations peuvent aussi manquer de précision, touchant ainsi par ricochet aussi des civils, un phénomène accentué par l'interconnexion du réseau. Mais des cyberopérations ayant une faible valeur stratégique peuvent toutefois être dommageables pour leurs victimes. Notre prisme d'analyse est lié au droit à la vie privée. Il ne relève pas d'une lecture géopolitique des cyberopérations, visant à évaluer leur avantage pour les parties belligérantes.

Notons également que la temporalité des conflits tend à s'étendre sur le temps long (le CICR le rappelle régulièrement), ce qui laisse un temps plus grand de préparation de cyberopérations, et que circonscrire un conflit dans l'espace numérique reste une gageure. Les armes cyber tendent à étendre le champ de bataille hors des lignes de front pouvant aussi toucher des pays non impliqués directement, mais soutenant un camp (nous pensons évidemment au conflit russo-ukrainien). Relier ces actes à un conflit en cours fait l'objet de discussions, qu'on ne tranchera pas ici, on se limitera à donner deux aperçus de cyberopérations pouvant toucher les humanitaires dans le cadre de conflits armés, au Yémen ainsi qu'en Ukraine.

Par exemple, d'après un rapport de la firme FireEye, dans le cadre du conflit syrien des ONG humanitaires ont été touchées par des cyber-opérations, entre mai 2013 et décembre 2013. L'organisation précise que les auteurs exacts de l'attaque n'ont pas été identifiés. On aurait potentiellement affaire à des forces pro-Assad, puisque, selon les analystes, « si ces données étaient acquises par les forces d'Assad ou leurs alliés, elles pourraient leur conférer un net avantage sur le champ de bataille. » [1419] Les hackers auraient récupéré les données d'évaluations de besoins, la liste du matériel nécessaire pour la construction d'un camp, des données financières, la liste des bénéficiaires, des informations personnelles sur les réfugiés, à savoir des demandes d'asile aux autorités turques, des scans de documents d'identité.

Un groupe russe aurait engagé une campagne majeure de cyberespionnage, ciblant des organisations de défense des droits de l'homme, the Syrian Observatory for Human Rights, mais aussi des ONG humanitaires. L'objectif de cette opération « semble être d'étouffer le flux sortant d'informations sur la crise humanitaire en Syrie et sur l'étendue de l'implication de la Russie dans les opérations militaires dans le pays. Les attaques auraient été bien organisées avec le soutien de l'État, utilisant des logiciels malveillants pour effacer des données, diffuser de fausses informations en utilisant des comptes officiels et donner accès à des contacts d'ONG, y compris à des cibles très sensibles ».[1420]

---

[1419] « if this data was acquired by Assad's forces or their allies it could confer a distinct battlefield advantage. »
REGALADO, Daniel, VILLENEUVEE, Nart, SCOTT RAILTON, John, « FireEye threat intelligence, Behind the Syrian conflict's digital frontlines », février 2015

[1420] "seemed to be to stifle the outgoing flow of information on Syria's humanitarian crisis, and the extent of Russia's involvement in military operations in the country. The attacks were reported to be well organized with state support, using malware to "erase data, spread false information using official accounts and give access to NGOs contacts, including highly sensitive targets", "Russia mounts major cyber-espionage campaign against Syrian organisations," *The New Arab*, Février 2016, "https://www.alaraby.co.uk/english/news/2016/2/21/russia-mounts-major-cyber-espionage-campaign- against-syrian-organisations
AMAREL, Emma, VERITY, Andrej, DU, Jiahui, "Cybersecurity vs humanitarian organization, on a collision course?", *DH, Digital humanitarian network*, August 2018.

Citons un autre exemple. Depuis mai 2022, la cellule de recherche — Insikt Group — de Recorded Future a enquêté sur une campagne de cyber-opérations menée au Yémen par OilAlpha. Ce groupe est identifié en tant qu'entité supportant un agenda pro-Houthi, bien que le rapport précise que ses allégeances politiques sont « mouvantes ». Ainsi, Insikt Group reste prudent : « Bien que l'activité d'OilAlpha soit pro-Houthi, il n'y a pas suffisamment de preuves pour suggérer que des agents yéménites sont responsables de cette activité de menace. Des acteurs extérieurs, comme le Hezbollah libanais ou irakien, ou même des opérateurs iraniens soutenant le Corps des gardiens de la révolution islamique, pourraient être à l'origine de cette activité. »[1421]

Le groupe a ciblé des personnes impliquées dans des négociations avec le gouvernement de l'Arabie Saoudite, mais aussi des ONG, des journalistes et des organisations humanitaires, dont le Croissant rouge saoudien, le Norwegian Refugee Council ou Unicef. OilAlpha a élaboré des opérations d'ingénierie sociale, mais a eu aussi recours à différents malwares : « Les acteurs de la menace OilAlpha sont très probablement impliqués dans des activités d'espionnage, car les appareils portables ont été ciblés par des outils d'accès à distance (RAT) tels que SpyNote et SpyMax. »[1422] Spynote et SpyMax sont donc deux chevaux de Troie d'accès à distance (RAT). Il s'agit d'un outil d'accès utilisé par les développeurs de logiciels malveillants pour obtenir un accès complet et à distance du système d'un utilisateur. Spynote peut par exemple enregistrer des données audio comme des appels téléphoniques, et vidéo, enregistrer chaque clic effectué, voler des mots de passe et suivre la position de l'appareil[1423].

Selon Insikt Group, la motivation d'OilApha est moins claire en ce qui concerne son choix d'une cible humanitaire et les analystes restent prudents dans leurs conclusions : « Ce dernier, le Norwegian Refugee Council, est une exception, ce qui soulève la question de savoir pourquoi un groupe de menace usurperait l'identité d'ONG ou ciblerait des personnes associées à des ONG au Yémen. Des sources publiques suggèrent que des milices houthi ont enlevé des employés d'ONG et des agents de sécurité. Les partisans de la ligne dure des Houthis se méfient des ONG, qu'ils considèrent comme des outils d'"influence occidentale" permettant l'infiltration et l'espionnage étrangers. »[1424]

La campagne d'OilAlpha a connu de nouveau développement, et en juillet 2024 Insikt Group publie des éléments d'analyses inédits relatifs à des cyberopérations visant à nouveau des humanitaires ( les ONG Norwegian Refugee Council et Care International). Cette fois ci, les ONG n'apparaissent plus comme des cibles faisant figure d'exception, mais sont

[1421] "While OilAlpha's activity is pro-Houthi, there is insufficient evidence to suggest that Yemeni operatives are responsible for this threat activity. External threat actors like Lebanese or Iraqi Hezbollah, or even Iranian operators supporting the IRGC, may have led this threat activity." INSIKT Group, "OILALPHA: a likely pro-houthi group targeting entities across the Arabian peninsula", *The Record*, 16/05/2023 https://www.recordedfuture.com/oilalpha-likely-pro-houthi-group-targeting-arabian-peninsula

[1422] « OilAlpha threat actors are highly likely to be involved in espionage activity, as handheld devices were targeted with remote access tools (RATs) like SpyNote and SpyMax. We have also observed njRAT samples communicating with C2s associated with this group, making it likely that OilAlpha has used other malware for testing or attack operations. »
INSIKT Group, "OILALPHA: a likely pro-houthi group targeting entities across the Arabian peninsula", *The Record*, 16/05/2023 https://www.recordedfuture.com/oilalpha-likely-pro-houthi-group-targeting-arabian-peninsula

[1423] WALLEN, Jack, SpyNote : sur Android, ce spyware vous écoute et vole vos données, ZDNET, 25/10/2023 https://www.zdnet.fr/actualites/spynote-sur-android-ce-spyware-vous-ecoute-et-vole-vos-donnees-39962036.htm

[1424] The latter, the Norwegian Refugee Council, is the outlier, which raises the questions of why a threat group would spoof NGOs or target NGO-associated individuals in Yemen. Public sources suggest Houthi militia groups have abducted NGO workers and security. Houthi hardliners are wary of NGOs, which are viewed as tools of "Western influence" to enable foreign infiltration and espionage Ibid.

spécifiquement visées via le même modus operandi, et ce alors le contexte sécuritaire est très dégradé pour les humanitaires [1425].

Enfin, le conflit russo-ukrainien comprend depuis 2014 une facette numérique, qui a fait l'objet de nombreuses discussions. Certains chercheurs surlignent l'importance cruciale des cyberopérations dans le déroulé des opérations, d'autres relativisent leur poids, ou du moins surlignent qu'elles sont moins efficaces[1426] et moins nombreuses qu'escompté[1427]. Enfin des chercheurs du laboratoire de recherche Geode mettent en avant des dimensions numériques du conflit moins documentées, notamment des opérations de déroutage de réseaux[1428].

On ne tranchera évidemment pas ici ce débat, on se contentera de remarquer que les cyber-opérations contre les ONG humanitaires sur ce terrain conflictuel s'inscrivent dans une stratégie plus large de déstabilisation de la société ukrainienne. Cette stratégie numérique comprend plusieurs volets. Certaines cyber-opérations sont relatives à des actions de désinformation. Certaines cyber-opérations cherchent à décrédibiliser les institutions occidentales et ukrainiennes, jouant sur le sentiment anti-migrant. D'autres attaques à l'encontre d'ONG d'aide aux exilés ont [1429]pour objectif la désorganisation de l'aide et le renforcement de la situation chaotique sur le terrain[1430]. En somme, ce type d'action pourrait être qualifiée de « sabotage numérique »[1431].

---

[1425]OilAlpha Malicious applications target humanitarian aid groups operating in Yemen, Recorded future, 09/07/2024 https://go.recordedfuture.com/hubfs/reports/cta-2024-0709.pdf
"Yemen : Houthis disappear dozens of UN, Civil Society Staff, release detainees, end arbitrary arrests and enforced disappearances", *Human RIghts Watch,* 26/06/2024 https://www.hrw.org/news/2024/06/26/yemen-houthis-disappear-dozens-un-civil-society-staff

[1426] BATEMAN, Jon, BEECROFT, Nick, WILDE, Gavin, "What the russian invasion reveals about the future of cyber warfare", 19/12/2022 https://carnegieendowment.org/posts/2022/12/what-the-russian-invasion-reveals-about-the-future-of-cyber-warfare?lang=en
LEWIS, James, "Cyber war and Ukraine", June 2022https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220616_Lewis_Cyber_War.pdf?VersionId=S.iEKeom79InugnYWlcZL4r3Ljuq.ash

[1427] MASCHMEYER, Lennart, DUNN CAVELTY, Myriam, "Goodbye cyberwar: Ukraine as reality check", Policy Perspectives, Vol.10/3, may 2022 https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/549252/2/PP10-3_2022-EN.pdf

[1428] DOUZET, Douzet, PETINIAUD, L. Pétiniaud, SALAMATIAN, K. LIMONIER, K., ALCHUS T, "Measuring the Fragmentation of the Internet: The Case of the Border Gateway Protocol (BGP) During the Ukrainian Crisis," *2020 12th International Conference on Cyber Conflict (CyCon)*, Estonia, 2020, pp. 157-182

[1429] En Février 2022 une campagne de phishing a été menée contre des organisations et des individus, notamment des responsables politiques, aidant des réfugiés ukrainiens. Le groupe a l'origine de cette campagne serait associé au gouvernement bélarusse. Son nom: UNC1151, ou Ghostwriter, ou son autre attribution TA445. Le groupe TA445 a déjà mené des actions de déstabilisation visant à raviver les sentiments anti-migrants en Europe : « .information warfare and targeted cyber-attack model https://www.proofpoint.com/us/blog/threat-insight/asylum-ambuscade-state-actor-uses-compromised-private-ukrainian-military-emails BREWSTER, Thomas, «Warning : hackers are targeting the ukraine refugee crisis », *Forbes*, 02/03/2022
https://www.forbes.com/sites/thomasbrewster/2022/03/02/warning-hackers-are-targeting-the-ukraine-refugee-crisis/
WAHLSTROM, Alden, REVELLI, Alice, RIDDELL, Sam, MAINOR, David, SERABIAN, Ryan," The IO offensive : information operations surrounding the russian invasion of Ukraine", *Mandiant*, 25/11/2022 https://www.mandiant.com/resources/blog/information-operations-surrounding-ukraine
Mandiant Threat intelligence, "Evacuation and Humanitarian Documents used to Spear Phish Ukrainian Entities", 25/11/2022 https://www.mandiant.com/resources/blog/spear-phish-ukrainian-entities
RAGGI, Michael, CASS, Zydeca, "the Proofpoint Threat Research TeamAsylum Ambuscade: State Actor Uses Lua-based Sunseed Malware to Target European Governments and Refugee Movement", *Proofpoint*, 01/03/2022https://www.proofpoint.com/us/blog/threat-insight/asylum-ambuscade-state-actor-uses-compromised-private-ukrainian-military-emails

[1430] https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us
GROSSMAN, Taylor, KAMINSKA, Monica, SHIRES, James, SMEETS, Max, "The Cyber dimension of the russia-ukraine war", *European cyberconflict research initiative*, April 2023
https://eccri.eu/wp-content/uploads/2023/04/ECCRI_REPORT_The-Cyber-Dimensions-of-the-Russia-Ukraine-War-19042023.pdf
LEWIS ANDREW, James, "Cyber War and Ukraine", *Center for strategic & international studies* , 16/06/2022,
https://www.csis.org/analysis/cyber-war-and-ukraine

[1431] ROVNER Joshua, « Théorie du sabotage », *Études françaises de renseignement et de cyber*, 2023/1 (N° 1), p. 139-153. https://www.cairn.info/revue-etudes-francaises-de-renseignement-et-de-cyber-2023-1-page-139.htm

Ainsi, une attaque de type « data-wiping » (qui conduit à l'effacement de données) a frappé une station de contrôle frontalier qui venait au secours des Ukrainiens fuyant vers la Roumanie. L'attaque a d'abord été rapportée par le Washington Post ainsi que par Amazon, qui déclare que : « Nous avons constaté à plusieurs reprises que des logiciels malveillants ciblaient spécifiquement des organisations caritatives, des ONG et d'autres organismes d'aide afin de semer la confusion et de provoquer des perturbations. Dans ces cas particulièrement flagrants, les logiciels malveillants visaient à perturber les fournitures médicales, la nourriture et l'habillement. »[1432] Amazon ne donne pas plus de détails sur leur identité ou mode opératoire. Plus généralement, ce type d'objectif peut être atteint avec des moyens relativement peu couteux, comme des attaques de type « défacement », ou encore « Distributed Denial Of Service » en anglais (Ddos). D'ailleurs à ce sujet, le Cyberpeace institute a documenté des cas de DDoS ciblant des ONG ukrainiennes, des sites d'associations anticorruption, des fondations caritatives. Le Cyberpeace Institute rapporte aussi que des ONG humanitaires prêtant assistance à des réfugiés ont été victimes du groupe pro-russe People's CyberArmy[1433].

D'autres attaques sont considérées comme des opérations de renseignement. Ainsi, un groupe affilié à l'État russe — Blue Calisto (ou Seaborgium, ou Star Blizzard) a attaqué « une société ukrainienne de logistique et de messagerie qui, en plus de ses activités commerciales, livrait de l'aide humanitaire à l'Ukraine. Blue Calisto a aussi mené des campagnes de collecte d'informations au sein d'organisations en Europe et aux États-Unis, soulignant le portefeuille opérationnel dynamique de l'acteur de la menace, probablement à la demande du gouvernement russe. » [1434]

En décembre 2022, la firme d'audit PWC indique que le groupe aurait également piraté d'autres organisations aidant l'Ukraine, « allant de la fourniture d'aide humanitaire à l'Ukraine à l'enquête sur les actions de la Russie en Ukraine.»[1435] Le gouvernement ukrainien rapproche Blue Calisto d'un autre groupe de hackeur proche des services de renseignements russe, Gamaredon. Cette filiation est contestée par plusieurs firmes d'analyse de renseignement cyber[1436].

Les liens entre des groupes de hackers et les acteurs étatiques ne sont pas toujours clairement établis, mais pour ce qui concerne Gamaredon (ou Aqua Blizzard ou Actinium) il semble plus

---

[1432] « We have seen several situations where malware has been specifically targeted at charities, NGOs, and other aid organizations in order to spread confusion and cause disruption. In these particularly egregious cases, malware has been targeted at disrupting medical supplies, food, and clothing relief. »
« Amazon's cybersecurity assistance for Ukraine », 08/03/2022,
https://www.aboutamazon.com/news/community/amazons-cybersecurity-assistance-for-ukraine

[1433] Cyberpeace Institute, "Cyber dimension on the armed conflict in Ukraine", September 2023, https://cyberpeaceinstitute.org/wp-content/uploads/2023/09/Ukraine-Report-Q2_4.09.pdf

[1434] « a Ukrainian logistics and courier company, which had been delivering humanitarian aid to Ukraine in addition to its commercial operations. Blue Callisto also conducted credential harvesting campaigns against organizations in Europe and the United States, underscoring the threat actor's dynamic operational portfolio likely at the behest of the Russian government. »
« Blue Callisto (a. k. a SEABORGIUM, Callisto Group) is likely a Russia-based threat actor which primarily conducts phishing attacks for espionage purposes since at least 2017 »
https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/blue-callisto-orbits-around-us.html#footnotes

[1435] "ranging from providing humanitarian aid to Ukraine to investigating Russia's actions in Ukraine. " Cyber threats 2022 : a year in retrospect, PWChttps://www.pwc.at/de/dienstleistungen/Cyber/2022-year-in-retrospect-report.pdf

[1436] AIME, Felix, A Maxime, "Calisto show interests into entities involved in Ukraine war support", https://blog.sekoia.io/calisto-show-interests-into-entities-involved-in-ukraine-war-support/

certains qu'ils soient affiliés aux services de renseignement russes, et plus particulièrement au Federal Security service ( le FSB)[1437]. Ce groupe a déjà ciblé des organisations humanitaires opérant en Ukraine dès 2021. Il aurait mené des campagnes de phishing en utilisant des appâts mimant des sources légitimes, comme l'OMS.


World Health Organization

COVID-19 Weekly Epidemiological Update

Edition 50, published 27 July 2021

In this edition:

- Global overview
- Special focus: Evaluations of the effectiveness of COVID-19 vaccines in real-world settings
- Special focus: Update on SARS-CoV-2 Variants of Interest and Variants of Concern
- WHO regional overviews
- Key weekly updates

Global overview

Data as of 25 July 2021

The global number of new cases reported last week (19-25 July 2021) was over 3.8 million, an 8% increase as compared to the previous week (Figure 1), an average of around 540 000 cases were reported each day over the past week as compared to 490 000 cases reported daily the week before. This trend is largely attributed to substantial increases in the Americas and Western Pacific Regions. The number of deaths reported this week increased sharply with over 69 000 deaths, a 21% increase when compared to the

*This URL and the related lure .dot document from ACTINIUM is responsible for loading the malicious remote template. This document uses text from a legitimate who.int situational COVID-19 update report published on July 27, 2021.*

### FAUX RAPPORT DE L'OMS SERVANT D'HAMEÇON A UNE CAMPAGNE DE PHISHING D'ACTINIUM[1438]

Les cibles ne sont pas simplement des entités opérant directement en Ukraine : un groupe de hackeur – affilié à des intérêts pro-russe – a utilisé Romcom un logiciel malveillant de type « remote access trojan » (RAT) pour attaquer un hôpital américain soutenant un programme humanitaire pour des réfugiés ukrainiens. Selon BlackBerry « Si des dossiers médicaux stockés électroniquement sont volés, il serait facile pour l'acteur de la menace (et ceux qui lui sont affiliés) d'établir le profil du patient et d'utiliser ces données dans de futurs scénarios de guerre et dans la géopolitique en général. Même l'extraction d'informations partielles, telles que le nom, le sexe, la date de naissance et d'autres données connexes, représente un risque pour la personne concernée et pour ceux qui lui fournissent une aide quelconque à l'avenir. »[1439]

Les attaquants motivés par des gains financiers peuvent également mener des campagnes alignés avec les intérêts russes et cibler majoritairement des organisations liées à l'Ukraine. Ainsi Google threat analysis group a aussi suivi un groupe baptisé par le CERT-UA « UAC-0098 », composé en partie d'anciens membres du groupe CONTI. Ce dernier a mené des

---

[1437] SECURITY Service of Ukraine, GAMAREDON, "Armageddon Group, FSB RF cyber-attacks against Ukraine", 2021 https://ssu.gov.ua/uploads/files/DKIB/Technical%20report%20Armagedon.pdf
Nation State Actor Aqua Blizzard
https://www.microsoft.com/en-us/security/security-insider/aqua-blizzard

[1438] « the primary outcome of activities by ACTINIUM is persistent access to networks of perceived value for the purpose of intelligence collection. Despite seemingly wide deployment of malicious capabilities in the region, follow-on activities by the group occur in areas of discrete interest, indicating a possible review of targeting. MICROSOFT Digital security Unity, "ACTINIUM targets Ukrainian organizations",04/02/2022 https://www.microsoft.com/en-us/security/blog/2022/02/04/actinium-targets-ukrainian-organizations/

[1439] "If medical records stored electronically are stolen, it would be easy for the threat actor (and those they are affiliated with) to profile the patient and use that data in future war scenarios and in geopolitics in general. Even the extraction of partial information, such as name, sex, date of birth, and related data, poses a potential risk to that person and those who provide them with any type of aid in future." The blackberry Research & intelligence Team, "RomCom Resurfaces: Targeting Politicians in Ukraine and U.S.-Based Healthcare Providing Aid to Refugees from Ukraine", 06/07/2023https://blogs.blackberry.com/en/2023/06/romcom-resurfaces-targeting-ukraine

attaques de type rançongiciel au cours de 2022 en ciblant entre autre des ONG humanitaires européennes opérant en Ukraine. D'après Google : « Les activités de l'UAC-0098 sont des exemples représentatifs de l'effacement des frontières entre les groupes à motivation financière et les groupes soutenus par le gouvernement en Europe de l'Est, illustrant une tendance des acteurs de la menace à modifier leur ciblage pour s'aligner sur les intérêts géopolitiques régionaux. »[1440]

Pour conclure, on dispose moins d'information sur des cas d'attaques contre des organisations humanitaires russes par des hackeurs « pro-ukrainiens », pouvant opérer en zones occupées, ou depuis 2024 sur le territoire russe. À ce sujet, le paysage de l'aide humanitaire russe reste extrêmement peu documenté. Plusieurs points rapides : il faut savoir que la Russie a pu jouer un rôle de bailleurs de fonds depuis le milieu des années 2000, son action de financement passerait alors via des canaux multilatéraux - également auprès d'organisations du Nord comme le WFP – plutôt que via des canaux de financements bilatéraux[1441]. Depuis le conflit russo-ukrainien et l'opposition grandissante à l'égard de l'occident, le rôle de bailleurs de fonds de la Russie est nettement plus réduit. Cela dit, il semblerait, si l'on se fonde sur le rapport de financement de l'organisation humanitaire, que la Russie ait contribué aux programmes du WFP à hauteur de 71 490 000 dollars en 2023[1442]. Pour ce qui est des organisations humanitaires à proprement parler, il existe une antenne russe de la Croix-Rouge, son rattachement au mouvement de la Croix rouge s'est distendu au fil du conflit, d'autant que son président soutiendrait clairement l'invasion de l'Ukraine. Mais Genève n'a pas pour le moment décidé de suspendre l'antenne[1443]. Par ailleurs, l'accès à des zones occupées par des forces russes par des ONG occidentales sont confronté à de multiples dilemmes éthiques[1444], et le principe de neutralité du CICR est mis à l'épreuve[1445]. Quant à l'action

---

[1440] "UAC-0098 activities are representative examples of blurring lines between financially motivated and government backed groups in Eastern Europe, illustrating a trend of threat actors changing their targeting to align with regional geopolitical interests." BUREAU, Pierre-Marc, "Initial access broker repurposing techniques in targeted attacks against Ukraine, Google, Threat Analysis Group, 07/09/2022 https://blog.google/threat-analysis-group/initial-access-broker-repurposing-techniques-in-targeted-attacks-against-ukraine/

[1441] BREZHNEVA, Anna, UKHOVA, Daria, Russia as a humanitarian aid Donor, Oxfam, 2013, https://policy-practice.oxfam.org/resources/russia-as-a-humanitarian-aid-donor-295654/

[1442] https://www.wfp.org/funding/2023

[1443] Mise à jour sur les allégations contre la Croix-Rouge russe, IFRC, 25/04/2024 https://www.ifrc.org/fr/article/update-allegations-against-russian-red-cross

« Cette situation place l'IFRC, basée à Genève, face à «un dilemme quasiment insoluble», écrit le *Tages-Anzeiger*. Le quotidien rappelle que la faîtière n'a aucune influence directe sur les sociétés nationales. Elle peut tout au plus les suspendre, comme elle l'a fait pour celle de Biélorussie. Mais dans le cas de la Russie, l'affaire est plus délicate: elle agirait contre une partie à un conflit. Une telle mesure pourrait par ricochet mettre en difficulté le CICR, qui apporte une aide importante à la population dans les zones de combat en Ukraine. A l'inverse, laisser faire la Croix-Rouge russe semble difficilement tenable. Au moment de l'éviction de la Croix-Rouge biélorusse, la Fédération internationale avait indiqué qu'elle ne pouvait «accepter aucune politisation ou manipulation de ses activités humanitaires»

« Comment les liens troubles de Croix-Rouge russe sèment l'embarras à Genève », *Le Temps*, 27/02/2024 https://www.letemps.ch/monde/comment-les-liens-troubles-la-croix-rouge-russe-sement-l-embarras-a-geneve

SCHOBER, Timo, HALBE, Jonas, HUPPERTZ, Carina,OBERMAIER,Frederik,ZIHLMANN, Oliver, " La Croix-Rouge russe met la centrale suisse en difficulté", La Tribune de Genève, 27/02/2024

https://www.tdg.ch/la-croix-rouge-russe-met-la-centrale-suisse-en-difficulte-897718158323

[1444] SAEZ, Patrick, "Navigating humanitarian dilemmas in the Ukraine crisis", HPG emerging analysis, May 2022 https://media.odi.org/documents/Navigating_Ukrainian_dilemmas_in_the_Ukraine_crisis.pdf

[1445] JOLI, Frédéric, " Conflit en Ukraine : comprendre le rôle du CICR " intermédiaire neutre dans les conflits armés", 25/03/2022, https://blogs.icrc.org/hdtse/2022/03/25/conflit-en-ukraine-comprendre-le-role-du-cicr-intermediaire-neutre-dans-les-conflits-armes/

GRYNSZPAN, Emmanuel, "Dmytro Lubinets, commissaire aux droits humains ukrainien : « Le Comité international de la Croix-Rouge doit publiquement condamner la Russie », Le Monde, 10/02/2023 https://www.lemonde.fr/international/article/2023/02/10/dmytro-lubinets-commissaire-aux-droits-humains-ukrainien-le-comite-international-de-la-croix-rouge-doit-publiquement-condamner-la-russie_6161241_3210.html

humanitaire à proprement parler russe, elle est peu documentée, même au-delà du conflit russo-ukrainien[1446]. Notons simplement que l'action humanitaire russe est partagée entre des organisations rattachées à l'État (au Ministère des situations d'urgence), ou/et à l'Église Orthodoxe[1447].

Pour ce qui concerne les cyberopérations en elles-mêmes, mentionnons le fait qu'en guise de protestation à la publication par le CICR d'un message à destination des cybercombattants enjoignant au respect du DIH, un hacker pro-ukrainien aurait « défacé » la page web de la branche russe de la Croix-Rouge[1448]. Cette action aurait d'après le média The Record été soutenue par d'autres hackeurs ukrainiens, partageant leur rejet frontal des règles de DIH[1449]. La position de Sean Townsend, porte-parole d'un collectif de hackeurs, l'*Ukrainian Cyber Alliance*, est, dans une certaine mesure, plus pondérée. Toutefois, ce dernier déclare ne respecter que deux règles du DIH sur les 8 édictées par le CICR[1450]. Et les règles retenues par Sean Townsend n'enjoignent pas les hackers à ne pas cibler les ONG humanitaires.

---

Ikhtiyar Aslanov, ex-responsable de la Croix-Rouge en Russie : «La diplomatie humanitaire est une question de patience», Liberation, 30/06/2023 https://www.liberation.fr/international/europe/ikhtiyar-aslanov-ex-responsable-de-la-croix-rouge-en-russie-la-diplomatie-humanitaire-est-une-question-de-patience-20230630_INUI4Q4YANDTVLYLB2VLJ3HKZM/
MABILLARD, Boris, "Pourquoi le gouvernement ukrainien déteste le CICR", Le Temps, 20/12/2023 https://www.letemps.ch/monde/pourquoi-le-gouvernement-ukrainien-deteste-le-cicr

[1446] GOUSSEFF, Catherine, REGAMEY, Amandine (Dir.), « L'URSS et la Russie contemporaine face à l'humanitaire », *Connexe, les espaces postcommunisme en question (s*), 2015, vol.1, ⟨halshs-01250153⟩

[1447] ROBINSON, Jonathan, Russian aid in Syria: an underestimated instrument of soft power, Atlantic council, 14/12/2020 https://www.atlanticcouncil.org/blogs/menasource/russian-aid-in-syria-an-underestimated-instrument-of-soft-power/

[1448] Mise à jour sur les allégations contre la Croix-Rouge russe, IFRC, 25/04/2024 https://www.ifrc.org/fr/article/update-allegations-against-russian-red-cross
« Comment les liens troubles de Croix-Rouge russe sèment l'embarras à Genève », *Le Temps*, 27/02/2024 https://www.letemps.ch/monde/comment-les-liens-troubles-la-croix-rouge-russe-sement-l-embarras-a-geneve
WALKER, Shaun, « Red Cross decides against suspending Russian branch despite links to Kremlin war machine », *The Guardian*, 29/04/2024 https://www.theguardian.com/world/2024/apr/29/red-cross-decides-against-suspending-russian-branch-despite-links-to-kremlin-war-machine

[1449]« Red Cross? I don't care about their demands and I won't even think about them," the pro-Ukrainian hacker group Cyber Anarchy Squad wrote on Telegram. "If I want to fuck up critical infrastructure, I will do everything to fuck it up." « La Croix-Rouge ? Je me moque de leurs demandes et je n'y penserai même pas », a écrit sur Telegram le groupe de pirates informatiques pro-ukrainien Cyber Anarchy Squad. « Si je veux bousiller des infrastructures critiques, je ferai tout pour les bousiller. » ANTONIUK, Daryna, "War has no rules ": hacktivists scorn Red Cross" new guidelines", *The Record*, 05/10/2023https://therecord.media/hacktivists-respond-to-red-cross-rules-with-ridicule

[1450]« Так что из их восьми правил можно оставить два - не убивать гражданских в больших количествах, даже если враг состоит из людоедов и убийц. На этом всё. Естественно, что больницы, железные дороги, электростанции, коммуникации и прочая "цивильная" и " критическая" инфраструктура - первейшая и законная цель для хакеров, как гражданских так и военных. Её нужно разрушить. И кибер - один из самых гуманных способов это сделать. » « Sur les huit règles, nous pouvons donc en garder deux : ne pas tuer de civils en grand nombre, même si l'ennemi est composé de cannibales et d'assassins. C'est tout. Naturellement, les hôpitaux, les chemins de fer, les centrales électriques, les communications et autres infrastructures "civiles" et "critiques" sont les premières cibles légitimes des pirates informatiques, qu'ils soient civils ou militaires. Elles doivent être détruites. Et la cybernétique est l'un des moyens les plus humains d'y parvenir. » https://t.me/s/ruheight/1492 Message de Sean Townsend publié sur sa chaine Telegram. 1.Ne pas conduire de cyberattaques contre des objets civils. 2.Ne pas utiliser de programmes malveillants ou autres outils et techniques qui se propagent de manière automatique et portent atteinte à des objectifs militaires et des objets civils de façon indiscriminée.3.Faire en sorte d'éviter ou de minimiser les effets qu'une opération pourrait avoir sur les civils au moment de la planification d'une cyberattaque contre un objectif militaire. 4. Ne conduire aucune opération cyber contre des bâtiments médicaux et humanitaires. 5. Ne conduire aucune cyberattaque contre des objets indispensables à la survie de la population ou pouvant libérer des « forces dangereuses ». Suivant le DIH, ces objets comprennent les « barrages, digues et centrales nucléaires ». Les auteurs ajoutent à cette liste les usines industrielles et chimiques qui peuvent contenir et libérer de telles « forces dangereuses ». 6. Ne pas diffuser de menaces de violence ou répandre la terreur parmi les populations civiles. 7. Ne pas inciter à des violations du DIH. 8 Respecter ces règles même si l'ennemi ne le fait pas. RODENHAUSER, Tilman, VIGNATI, Mauro," 8 rules for "civilian hackers" during war, and 4 obligations for states to restrain them", *Humanitarian law&policy*, 04/10/2023 https://blogs.icrc.org/law-and-policy/wp-content/uploads/sites/102/2023/10/8-rules-for-civilian-hackers-during-war-and-4-obligations-for-states-to-restrain-them-Humanitarian-Law-Policy-Blog.pdf
BERTRAN, Marie-Gabrielle, GERY, Aude,"La protection des civils dans un contexte de numérisation et de « civilianisation » des conflits armés : un continuum d'obligations internationales *», Le Rubicon*, 09/11/2023 https://lerubicon.org/la-protection-des-civils-dans-un-contexte-de-numerisation-et-de-civilianisation-des-conflits-armes-un-continuum-dobligations-internationales/

## Section 2 — Les cyberopérations comme accident de sécurité pour les ONG

Les paragraphes précédents nous ont permis d'avoir un premier aperçu des accidents cyber touchant le secteur de la solidarité internationale. Mais à vrai dire, le fait d'être pris pour cible d'attaques n'est pas une nouveauté pour les ONG. Les humanitaires sont en effet depuis une trentaine d'années font face à d'autres types d'agressions, à savoir des enlèvements et des assassinats des personnels des ONG.

Pour rappel, les années 90 sont marquées par une multiplication d'accidents de sécurité, en lien avec le rétrécissement graduel de l'espace humanitaire. Tout d'abord, il s'agit de victimes au sein de conflits, d'escarmouches armées. Mais si dans les années 1980, ces morts sont encore perçus comme étant des cas isolés, dans les années 1990, ces derniers commencent à être estimés comme des problèmes de sécurité de fond. Et surtout, au début des années 2000, les humanitaires sont progressivement pris comme cibles en tant que tels. Restent dans les mémoires les attentats contre le siège des Nations unies et celui du CICR à Bagdad en 2003. L'expansion de groupes radicaux djihadistes dans le Sahel et au Moyen-Orient va de pair avec une augmentation du nombre d'enlèvements. Cela dit, un chercheur comme Mark Duffield a pu montrer que d'autres facteurs expliquent la hausse de ces accidents de sécurité : une instrumentalisation de l'aide et sa sécuritisation dans des opérations de prévention de zones perçues comme « instables » ; le floutage des frontières entre acteurs de l'aide et objectifs sécuritaires est un autre facteur d'insécurité pour les ONG[1451].

En conclure à une augmentation effective des morts sur le terrain ne fait pas consensus, et les statistiques sur ce sujet sont discutées (notamment au sein de MSF). En règle générale, cette augmentation est associée à l'extension du champ d'opération des humanitaires. En effet, dans un contexte post-guerre froide, on aurait assisté à un accroissement du nombre d'opérations en raison du boom de l'aide internationale, et l'évolution de la nature des guerres. L'affrontement bipolaire propre à la guerre froide ferait place à de nouveaux types de guerres moins facilement lisibles, touchant plus directement les civils (et également les humanitaires). Leurs qualifications font l'objet de débats académiques. Pour certains chercheurs ces nouveaux conflits ne seraient plus des conflits étatiques, mais seraient nourris par des logiques ethniques, religieuses ou économiques[1452], des milices et groupes armés y joueraient un plus grand rôle, complexifiant ainsi leur nature[1453].

Toujours est-il que dans les années 1990, un nouveau type d'acteurs émerge à la suite de la multiplication de kidnapping et d'assassinats d'humanitaires : les responsables de sécurité, les « security risk manager ». Et une série de normes et de guides régulant les pratiques des

---

[1451] FAST, Larissa, « Securitization ». In *Humanitarianism*. Leiden, The Netherlands: Brill, 2020. https://doi.org/10.1163/9789004431140_089
VAUGHN, JOCELYN. "The Unlikely Securitizer: Humanitarian Organizations and the Securitization of Indistinctiveness." *Security Dialogue*, vol. 40, no. 3, 2009, pp. 263–85. *JSTOR*, http://www.jstor.org/stable/26299791
DUFFIELD, Mark, WADDELL, Nicholas, "Securing Humans in a dangerous world", *International Politics*, 43 (1-23),2006

[1452] COLLIER, P. « Greed and grievance », dans BERDAL, MALONE, D. (eds.), *Greed and Grievance : Economic Agendas of Civil Wars*, Boulder, Lynne Rienner, 2000.

[1453] KALDOR, Mary, *New and Old Wars. Organized Violence in a Global Era*, Cambridge: Polity Press, 1999,256 p.
MARCHAL Roland, MESSIANT Christine, « Les guerres civiles à l'ère de la globalisation. Nouvelles réalités et nouveaux paradigmes », *Critique internationale*, 2003/1 (n° 18), p. 91-112.

humanitaires sont publiés est publiée , visant à minimiser les « accidents de sécurité »[1454]. Les dangers inhérents au déploiement d'opérations de secours dans les conflits et les catastrophes naturelles ont progressivement été traités comme le montrent Michel Neuman et Fabrice Weissman, en tant que risques susceptibles d'être maitrisés et gérés[1455]. D'autant que le label « accident de sécu » tend à désigner un nombre croissant de risques. De fait le chercheur Arnaud Dandoy, dans son rapport sur les enjeux sécuritaires à Haïti, fait un retour critique sur cette catégorie, qui engloberait des accidents très divers[1456].

D'ailleurs, les cyber-opérations sont-elles labélisées comme « accident de sécurité » ? Comment s'articulent les risques numériques et la gestion des accidents de sécurité au sein des ONG ? Quelles sont les différences façon de catégoriser ces opérations selon qu'il soit question d'un DPO ou d'un responsable de la sécurité d'une ONG ? Commençons par remarquer que dans de nombreux manuels rédigés par des acteurs gérant les accidents de sécurité au sein des ONG les outils numériques sont considérés comme une façon d'assurer la sérûté des humanitaires[1457]. En tout cas, les NTIC permettraient de continuer de mener une action à distance[1458], même en cas de situation sécuritaire dégradée, comme ont pu le montrer Mark Duffield ou Larissa Fast[1459]. Le contact avec le terrain est ainsi maintenu grâce au recours à des logiciels de management d'équipes (souvent locales) restées sur place, d'agent conversationnels servant à échanger avec les bénéficiaires. L'utilisation d'images

---

[1454] BEERLI, Monique, WEISSMAN, Fabrice, Suivez le guide! Les manuels de sécurité et la mise en ordre autoritaire des organisations humanitaires ». In, WEISSMAN, Fabrice, NEUMAN, Michael, (ed.), *Secourir sans périr : La sécurité humanitaire à l'ère de la gestion des risques*. Paris : CNRS Editions, 2016. p. 137–154

[1455] TAITHE, Bertrand, » Danger, Risk, Security and Protection: Concepts at the Heart of the History of Humanitarian Aid", in :NEUMAN, Michael, Weissman, Fabrice, (ed.), *Saving Lives and Staying Alive: the professionalization of humanitarian security*, London: Hurst Publishers. 2016. p. 37- 53

BEERLI, Monique, « Saving the Saviors: An International Political Sociology of the Professionalization of Humanitarian Security », Thèse de doctorat, sciences politiques, Université Genève, 2017

[1456] Il note ainsi la propension des acteurs humanitaires à subsumer sous le même vocable d'« incident sécu » l'ensemble des actes susceptibles d'affecter leur personnel ou leur matériel, qu'il s'agisse de la petite délinquance, des manifestations, de la violence des bandes, des enlèvements, ou des menaces et agressions délibérées envers les humanitaires. Cette catégorie « incident sécu » recèle une certaine ambiguïté au niveau de son utilisation, qui lui confère justement sa puissance symbolique et performative. » Arnaud Dandoy, « Insécurité et aide humanitaire : l'impossible dialogue ? », URD, 2005.

[1457] DETTE, Rahel, STEETS, Julia, "Innovating for access : the technology in monitoring higly insecure environment", *Humanitarian practice network*, 20/04/2016https://odihpn.org/publication/innovating-for-access-the-role-of-technology-in-monitoring-aid-in-highly-insecure-environments/

SANDVIK, Kristin Bergtora Sandvik, "The humanitarian cyberspace: shrinking space or an expanding frontier?", *Third World Quarterly*, 2015 *37*(1), p.17–32 DOI: 10.1080/01436597.2015.1043992

[1458] "the term 'remote management' has been widely used to describe situations in which humanitarian agencies implement programmes with limited or non-existent direct access to populations in need. For some agencies, remote management is simply the decentralisation of management, a practice that might be used in situations where the agency did have access but chose to work through partners on the ground. Several organisations have linked the notion of remote management to the absence of international staff performing some key functions associated with assessments, programme design and/or monitoring. To other agencies, remote management implies a lack of physical presence due to political limitations or security risks. It is notable that organisations also employ diverse definitions of 'access', ranging from occasional short visits to a given area by senior staff with the constant presence of local staff, to working only through local partners without any direct contact between the agency and the affected population."" Le terme « gestion à distance » a été largement utilisé pour décrire les situations dans lesquelles les agences humanitaires mettent en œuvre des programmes avec un accès direct limité ou inexistant aux populations dans le besoin. Pour certaines agences, la gestion à distance est simplement la décentralisation de la gestion, une pratique qui pourrait être utilisée dans des situations où l'agence a un accès mais choisit de travailler par l'intermédiaire de partenaires sur le terrain. Plusieurs organisations ont lié la notion de gestion à distance à l'absence de personnel international chargé de certaines fonctions clés liées aux évaluations, à la conception des programmes et/ou au suivi. Pour d'autres agences, la gestion à distance implique une absence de présence physique en raison de contraintes politiques ou de risques pour la sécurité. Il est à noter que les organisations emploient également diverses définitions de l'« accès », allant de courtes visites occasionnelles dans une zone donnée par des cadres supérieurs avec la présence constante de personnel local, au travail uniquement par l'intermédiaire de partenaires locaux sans aucun contact direct entre l'agence et la population touchée ». DONINI, Antonio, MAXWELL, Daniel, » from face to face to screen to screen : remote management, effectiveness and accountability of humanitarian action in insecure environments", International Review of the red cross, 2013, 95 (890), 383-413, Violence against healthcare https://international-review.icrc.org/sites/default/files/irrc-890-donini-maxwell.pdf

[1459] PAVANELLO, Sara, FAST, Larissa, SVOBODA, Eva, « Fostering local parnerships in remote management and high-threat setting », HPG Commissioned Report, 2018https://media.odi.org/documents/12302.pdf

satellitaires permet aussi de produire des analyses surplombantes de situations de crise. Mais a contrario, le numérique peut aussi assurer la sécurité des humanitaires intervenant sur le terrain. Ainsi, un guide de sécurité mentionne que « l'envoi de SMS, d'appels par téléphone satellite ou de vérifications par radio avec des bureaux éloignés et les personnes en déplacement a lieu régulièrement, en fonction des besoins. »[1460] Et de fait, les travailleurs humanitaires doivent être joignables et visibles pour les acteurs chargés d'assurer leur protection. On peut lire ainsi que : « pour que les signalements puissent être effectués tout au long du déplacement, tous les téléphones portables devront être entièrement chargés et fonctionner dans la région de la mission. Dans le cas contraire, des équipements et protocoles de communications alternatifs devront être envisagés. »[1461]

Le fait d'assurer la visibilité du personnel des ONG précède la numérisation du secteur, comme nous le raconte un enquêté, décrivant une mission effectuée en 1999 au sein d'une ONG qu'il décrit comme accordant une forte importance à la sécurité de son personnel *: « toute la semaine, on devait dire où on allait au responsable sécurité, qui avait un grand board dans son bureau et sur lequel il y avait noté chaque humanitaire où il se trouvait chaque jour, et puis pour nous donner des talkies-walkies, pour pouvoir communiquer avec des noms de code pour les villes où on allait. »*[1462]

Ces formes de surveillance sont depuis devenue plus invasives encore avec la numérisation du secteur : certaines ONG peuvent même utiliser des dispositifs de géolocalisation permettant de suivre la progression des voitures des personnels et pouvoir ainsi s'assurer de leur sécurité. On peut noter d'emblée l'ambiguïté de ce type de dispositif, assurant la sécurité du personnel, mais étant facteur de risque d'un point de vue de la cybersécurité, comme nous le pointe un enquêté : « *On utilise l'intérêt légitime pour les données de "car tracking"… Là il y a un intérêt légitime, pour identifier les véhicules en cas d'arrestation, de kidnapping, ou de fraude de la part du chauffeur. Mais en termes de cybersécurité cela constitue clairement une vulnérabilité : il ne fait aucun doute que les GPS des voitures peuvent être hackés pour cibler les humanitaires. »*[1463]

Par voie de conséquence, le fait de ne plus être visible représenterait un risque et doit être notifié, comme on peut le lire dans un guide relatif à la sécurité des humanitaires : « Il existe des règles pour les cas où un membre du personnel ou une équipe ne se signalerait pas ou ne serait pas joignable. Tout le personnel a connaissance de ces règles, qui sont appliquées de manière systématique. »[1464] D'ailleurs, les services de sécurité doivent également avoir une visibilité du terrain lui-même, comprendre la nature des acteurs en présence afin de mieux cerner les menaces pouvant toucher les humanitaires. Plus largement, les parties du conflit doivent assurer le libre mouvement du personnel humanitaire tout en prenant toutes les précautions nécessaires pour éviter des pertes humaines, d'où la mise en place de systèmes

[1460] RedR UK, "Insecurity Insight, European Interagency Security Forum", Manuel de gestion de l'information issue des incidents de sécurité, 2017 https://insecurityinsight.org/wp-content/uploads/2020/02/1-GIIS-Manuel-Jan2018_FR.pdf
[1461] ibid
[1462] Entretien n° 96, ONG 5, responsable de programme de santé, 05/08/2024
[1463] https://mobility.groupcls.com/metiers/humanav/
[1464] RedR UK,"Insecurity Insight, European Interagency Security Forum, "Manuel de gestion de l'information issue des incidents de sécurité", 2017

de notifications humanitaires. Il s'agit de dispositifs de communications entre humanitaires et militaires, afin de se signaler en tant que membre d'ONG et éviter d'être pris pour cible. Ce type de communication tend aussi à passer par des médiums numériques[1465]. D'après le chercheur Rob Grace, ces systèmes de notification humanitaire iraient de pair avec une série de risques en matière de protection des données qui ne seraient pas suffisamment pris en compte. Il déclare ainsi espérer qu' : « à l'avenir, ces deux sous-domaines de la réflexion sur les politiques humanitaires soient intégrés de manière très profonde. De sorte que les questions d'éthique numérique soient au cœur du système de notification humanitaire de la manière dont nous y réfléchissons et dont nous le mettons en œuvre. »[1466] Le protocole WhiteFlag vise justement à assurer un équilibre entre visibilité et confidentialité notamment via la blockchain[1467], dont les apports restent cependant discutés[1468]. En bref, l'ensemble de ces informations est sensible. Il s'agit de renseignement à valeur stratégique, pouvant dans le cadre de conflits être précieux pour des parties prenantes : « *La menace peut venir aussi bien du gouvernement que d'acteurs privés ou d'autres groupes, euh, et ensuite sur les réseaux sociaux et les apps il y a un aspect de communication. Comment s'assurer que les plans de sécurité ne soient pas, que leur confidentialité ne soit pas compromise. Il y a eu des problèmes sur les analyses de contexte et d'acteur (…) ces plans et cartes d'acteurs ont déjà fuité ou ont été hackés, et ça a pu compromettre un programme entier parce qu'une organisation a pu être accusée de faire de l'espionnage ou de récolter de l'intelligence, etc.* » [1469]

Cet équilibre entre visibilité et confidentialité peut reposer pour certaines ONG sur des techniques de dissimulation beaucoup plus symboliques, et pourraient même relever pour un de nos enquêtés d'une mise en scène des mesures de protection des données :
« *c'était complétement bidon. Le truc c'était que… les codes c'était les deux premières lettres de la ville, et on était dans une région grande comme l'ile de France, ou comme la Corse, et assez pas du tout sururbanisée, avec peu de villes, de chefs- lieux, de préfectures. Quand on disait OC, quand on disait au PC de la mission au talkie-walkie OC, qu'on était arrivé à OC, bah il y avait qu'une seule ville qui commençait par OC (…) en l'occurrence la ville c'était Ochamchire. C'est un peu bidon, c'est pas très élaboré franchement comme code, c'était un peu symbolique, ça pouvait peut être dissuasif, si des personnes entendaient qu'on parlait avec des codes peut être, des personnes malveillantes, elles pouvaient se dire, ohlala, ça c'est une grosse mission ils ont des talkies, ils utilisent des codes, ils sont sérieux, on va pas peut être agir là-dessus. Et ça peut peut être retarder, en cas d'action malveillante, ça peut peut être*

[1465]GRACE, Rob, "When security risk management and technology collide: getting humanitarian notification systems right", *GISF*, 10/01/2023 https://www.gisf.ngo/blogs/when-security-risk-management-and-technology-collide-getting-humanitarian-notification-systems-right/

[1466] « What organizations get in what organizations do not get in is a crucial question, what are the obligations of managing that data? What possible harms can result are questions that require a great deal of critical reflection. So, one thing I would like to see in the future for or HNS is for these two subfields of humanitarian policy thinking to be integrated in a very, very deep way. So that questions about digital ethics are living at the heart of HNS and how we think about it and how we implement it."
GRACE, Rob, "evolving NGO Security risk management humanitarian notification systems : unpacking the complexties and possibilities", *GISF,* 27/04/2023
https://www.gisf.ngo/resource/evolving-ngo-security-risk-management-ep3-humanitarian-notification-systems-unpacking-the-complexities-and-possibilities-gisf-podcast/

[1467] https://www.whiteflagprotocol.org/

[1468]PARK, Daniel, "Exploring distributed ledger application in OCHA's humanitarian system of deconfliction (HNS4D) active in Syria", University of British Columbia, 2021.
https://storage.googleapis.com/jnl-lse-j-tpsjpp-files/journals/1/articles/116/submission/proof/116-1-283-1-10-20220428.pdf

[1469] Ibid.

*retarder les opérations de ceux qui préparent un attentat, ou quelque chose comme ça. Tiens il a dit OC ? Qu'est-ce que ça veut dire, on va à OC… Nous, on le respectait en tout cas, sinon on se faisait rappeler à l'ordre, ce qui était justifié, parce qu'on ne savait pas ce qui pouvait se passer.* »[1470]

On a donc évoqué une tension entre sécurité, visibilité et confidentialité. Ajoutons que la manière dont les humanitaires peuvent être perçus par les autres acteurs (bénéficiaires, parties prenantes d'un conflit) est cruciale en matière de gestion de sécurité. Et cela est aussi le cas au sujet des NTIC. La confiance est un élément central de la sécurité des humanitaires afin d'éviter d'être la cible d'attaques. Pour le CICR, une des façons de garantir la confiance des populations est de rester proche de ces dernières et conserver une certaine neutralité au sein d'un conflit. L'organisation peut donc faire à dessein le choix d'être vulnérable. Pour rester neutre, il peut être en effet nécessaire de refuser certaines mesures de protection, notamment offerte par des militaires.

Et justement, le fait d'utiliser certains dispositifs visant à sécuriser les ONG peut ne pas être accepté par les populations locales et devenir un facteur d'insécurité selon un enquêté : « *on avait un contact talkie-walkie, il y avait d'autres personnes d'autres organisations qui partaient sans talkies, on le savait. Nous ça nous semblait imprudent. Mais il y a aussi des personnes qui étaient très intégrées dans la société abkhaze, nous on avait quelqu'un, d'une autre ONG, qui s'est marié avec une Abkhaze, lui il était breton et il s'est marié avec une abkhaze en Abkhazie. Donc, peut-être qu'il ne voyait pas la nécessité d'avoir un talkie lui, parce qu'il était au courant des choses qui allait se passer, etc. Et ça mettait peut être un frein symbolique entre les autochtones et les gens qui viennent là. Parce que faut se mettre à la place des autochtones, quand ils voient des gens avec des gros quatre-quatre avec des talkies walkies, sécurisés, ça montre que ces personnes expatriées craignent les locaux, ça ne prédispose pas nécessairement à la relation, l'autochtone, faut se mettre à la place de l'autochtone qui va se dire, le postulat c'est que nous on peut être dangereux. Nous les autochtones, on peut être dangereux*.»[1471]

Certains humanitaires défendent donc l'idée se fondre dans la population locale, la frontière entre humanitaire et population locale s'estompe, et il n'est alors pas nécessaire de se rendre visible aux yeux du siège. D'autres ONG prônent au contraire des modalités de traçage des personnels, qui sont alors beaucoup plus visibles pour les populations, comme on l'a vu dans l'extrait d'entretien précédent. Ces deux conceptions de la sécurité peuvent coexister dans une certaine mesure au sein d'une même organisation : « *il pouvait avoir des consignes contradictoires, le chef de sécurité qui était un jeune chef de sécurité à [Nom de l'organisation], était très prudent, nous donnait des consignes de sécurité assez strictes, sans pour autant être dans un délire, mais oui, on devait partir avec un talkie et ça c'est normal, parce qu'en cas d'enlèvement, si on ne sait pas où est la personne, il faut pouvoir la joindre. Lui il nous disait ça, mais moi avant de partir en mission, lors de ma formation à [Nom de l'organisation], le formateur qui était un chef de programme argentin, qui était un médecin, qui nous… nous*

[1470] Entretien n°96, ONG5, responsable de programme de santé, 05/08/2024
[1471] Entretien n°96, ONG5, responsable de programme de santé, 05/08/2024

*avait dit que la meilleure façon de se sécuriser dans une mission, c'était de faire des barbecues et jouer au foot avec des locaux quoi, parce que ça permet de discuter avec des gens, de savoir ce qui est en train de se tramer, de montrer qu'on est là en tant que personne pacifique… Mais il y avait l'autre courant à [Nom de l'organisation] qui était beaucoup plus dur, et qui disait qu'il fallait pas sortir* »[1472]

En tout cas, le DPO du CICR Massimo Marelli remarque que sur le terrain numérique, il n'est pas possible de transposer cette méthode. La vulnérabilité n'est plus une force, mais une faiblesse. Un piratage serait dévastateur et remettrait en cause la confiance accordée à une ONG et donc sa sécurité[1473]. Ajoutons que la confiance dans une organisation peut être entamée à cause de récits ou de récits diffusés sur les réseaux sociaux décrédibilisant l'organisation. Ainsi le CICR a été victime de Team Jorge, firme spécialisée en opération d'influence, ayant monté en exergue le lien supposé entre l'organisation et des groupes terroristes afin de la déstabiliser[1474].

En outre, les bénéficiaires peuvent ne pas avoir confiance dans les NTIC, et faire preuve d'une méfiance parfois jugée disproportionnée par les ONG et pouvant handicaper les humanitaires : « *Des communautés peuvent ne pas accepter que des staffs utilisent des téléphones. Ils ont peur de se faire espionner, etc., certaines technologies sont compliquées à utiliser… des technologies, on a un exemple en Colombie… des groupes armés ne laissaient pas passer des humanitaires si elles avaient des téléphones, elles ne les laissaient pas accéder aux populations si elles avaient des téléphones, et là ça complique les mesures de sécurité, qui sont de rester en contact… via téléphone. »*[1475]

Sécuriser ses informations peut être perçu comme mettant potentiellement en danger une ONG, comme on peut le lire dans un manuel de sécurité : « *De même, le cryptage de l'information peut donner une impression erronée de votre travail. Surtout si votre ONG fait valoir ses qualités d'ouverture et de redevabilité, on risque de vous interroger sur les raisons qui vous poussent à crypter des documents*. » [1476] Ainsi, adopter des moyens de communication moins sécurisés d'un point de vue numérique peut être plus sûr si l'on prend en compte la perception des bénéficiaires.

---

[1472] Entretien n° 96, ONG5, responsable de programme de santé, 05/08/2024

[1473] MARELLI, Massimo, "Hacking humanitarians: Defining the cyber perimeter and developing a cyber security strategy for international humanitarian organizations in digital transformation", *International Review of the Red Cross, 102*(913), 2020, p. 367-387
« the fact that the organization and its staff expose themselves and are so vulnerable vis-à-vis any
possible ill-intentioned third parties leads interlocutors to trust that the organization stands for what it says and does not have ulterior motives. In the digital world, however, vulnerability is not a strength but a weakness.
The idea that the systems of the organization could easily be breached if anyone wanted to attack them would, alone, destroy any trust in the organization and discourage stakeholders from engaging with it. »
AL ACHKAR, Ziad, "Digital risk: how new technologies impact acceptance and raise new challenges for NGOs", in GISF, Achieving Safe Operations through Acceptance: challenges and opportunities for security risk management, 2021https://www.gisf.ngo/wp-content/uploads/2021/12/Achieving_Safe_Operations_through_Acceptance_challenges_and_opportunities_for_security_risk_management.pdf

[1474] LELOUP, Damien, REYNAUD, Florian, « Quand la Croix-Rouge était victime d'une campagne sophistiquée de déstabilisation », *Le Monde*, 16/02/2023 https://www.lemonde.fr/pixels/article/2023/02/16/quand-la-croix-rouge-etait-victime-d-une-campagne-sophistiquee-de-destabilisation_6161999_4408996.html

[1475] Entretien n°34, 0NG12, 06/05/2020

[1476] GISF, La sécurité en pratique : boite à outil de gestion des risques à l'attention des agences humanitaires,2020,https://gisf.ngo/wp-content/uploads/2020/02/EISF-Security-to-Go-Online-Version-French.pdf

Néanmoins, pour certains DPO, leur méfiance dans le numérique serait le signe d'une sensibilité plus grande à la protection des données, et le fait de ne pas utiliser certaines technologies n'est pas nécessairement perçu par un DPO comme un handicap, mais comme une plus grande connaissance du risque : « *ça va être des zones où on collabore avec certains groupes qui sont recherchés, classifiés comme dangereux par les autorités, et ces groupes refusent qu'on travaille dans leurs zones avec des outils électroniques, là on est papier, c'est paradoxal et marrant que certains groupes soient beaucoup plus informés sur les risques digitaux que certains collègues à Paris ou à Genève, parce que ce sont des groupes qui sont chassés, traqués par des moyens électroniques, eux ils sont bien plus au courant, c'est pas pour rien que ben Laden faisait passer ces messages en papier, parce qu'eux se méfient de la technologie depuis bien plus longtemps que nous. Là où nous, on utilise tous des smartphones, certains groupes armés, très intelligemment, continuent à fonctionner à l'ancienne parce que c'est la façon la plus sécurisée pour continuer à fonctionner*. »[1477]

On a donc vu qu'il existe un véritable sujet sur les liens entre sécurité et numérique. Or les acteurs chargés d'assurer la protection des humanitaires ne prendraient pas assez en compte ce dernier. Et le dialogue entre service de sécurité et service informatique est pour le moment jugé insuffisant. Une responsable d'une ONG spécialisée sur la gestion des accidents de sécurité des humanitaires nous confie qu'*« il y a pas mal de nos membres qui s'en plaignent et ils sont pas forcément informés s'il y a des fuites d'information, s'il y a du hacking, le service informatique ne va pas forcément les contacter, ne le considère pas forcément comme un risque de sécurité, et ne les informe pas là-dessus. Il n'y a pas de collaboration entre les deux*. »[1478] Il n'existe d'ailleurs pas encore de dialogue sur ce sujet à l'échelle sectorielle, d'où un déficit de perspective et de vision globale de ces enjeux[1479]. Ceci a, pour autre conséquence, qu'un cadre de protection clair sur les données de sécurité manquerait. Un enquêté déplore ce point : « *on a eu on pas mal d'histoire, il y a eu des viols, des violences sexuelles, le rapport a fuité, au niveau de la confidentialité, les règles ne sont pas claires, les personnes ne savent pas avec qui elles peuvent partager les informations, quelles informations sont vraiment confidentielles (…), ils n'ont pas de guidelines claires sur la façon de protéger les déclarations d'accidents, sur la façon de les protéger au niveau digital. »* [1480] De surcroit, il n'existerait pas systématiquement de plan de gestion de crise numérique. En tout cas, les ONG seraient démunies lorsqu'il s'agit d'envisager de négocier avec les hackeurs alors que cela reste une procédure plus formalisée concernant les auteurs d'attaques physiques. Un DPO reconnait qu' : « *Au-delà de ces questions, lorsqu'un de nos bureaux est attaqué, dans un pays, quel qu'il soit, on a des moyens, des procédures, des modus operandi, pour contacter les auteurs, on sait comment faire pour ce genre de chose, c'est un peu… "business as usual", avoir des événements de sécurité à gérer là où on a des déploiements, maintenant dans le cas de ce hack.... euh… on avait rien en place*. »[1481]

[1477] Entretien n°44, OI2 DPO, juriste, 07/03/2021
[1478] Entretien n°34, 0NG12, 06/05/2020
[1479] Ibid
[1480] Ibid
[1481] Entretien n°93, OI2, DPO, 02/06/2023

Plusieurs facteurs expliquent cette absence apparente de sécuritisation des cyberaccidents au parmi les acteurs chargés d'assurer la sécurité des ONG[1482]. Tout d'abord, les dommages des accidents de sécurité ont des répercussions beaucoup plus tangibles. Les menaces numériques peuvent encore sembler plus abstraites comparativement à des risques d'enlèvement et d'assassinat. Une enquêtée spécialisée dans la gestion des accidents de sécurité, nous confie qu'une stratégie pour sensibiliser les responsables de sécurité serait alors d'appuyer sur la dimension potentiellement physique des accidents numériques : « *Déterminer les limites du domaine de la sécurité et de l'IT c'est une vraie question. L'angle de mon organisation a pris, je ne sais pas si c'est le meilleur, c'est se centrer sur les impacts du digital sur la sécurité physique, donc la limite c'est ça, à partir du moment où les risques digitaux s'éloignent des conséquences physiques, on ne peut pas avoir un impact direct, la sécurité ne sera pas intéressée à creuser le suje*t. » [1483] Il existe effectivement un lien potentiel entre ces deux types de risques : on a évoqué précédemment l'exemple d'opérations touchant les humanitaires au Yémen dans un contexte sécuritaire très dégradé, marqué par des enlèvements de membres d'ONG (dont des personnels onusiens)[1484]. Ce point reste à creuser, mais il semblerait que concernant les DPO ne pointent toutefois pas les répercussions d'opérations, non pas sur les travailleurs humanitaires, mais les bénéficiaires.

Deuxième point, pour objectiver les risques associés aux cyberattaques, il serait nécessaire de les quantifier, à l'instar des attaques physiques contre les humanitaires, qui font en effet l'objet d'une comptabilité[1485]. Or, il reste difficile de mener un exercice similaire pour les attaques numériques[1486]. En outre, les acteurs dotés de ce type de compétence / et pouvant produire ce type de savoir ne serait pas assez présent au sein d'ONG ( cf.chapitre 2). Et ce pour de multiples raisons qu'on a déjà évoquées plus haut. Les ONG souhaitent préserver leur image, elles ne disposent pas nécessairement d'outils d'analyse pour monitorer l'ensemble des attaques. Et enfin, déclarer les cyberopérations peut aussi être potentiellement dangereux pour les bénéficiaires : « *Les data breach, c'est pas évident, dans la mesure où on travaille dans des pays très intenses niveau sécurité, il faut qu'on mette en balance, le rapport d'une faille avec la confidentialité des patients, c'est le "do no harm" qui prévaut largement en la matière, dans certains cas ça va être précis, si les données fuitent, si les données fuitent*

---

[1482] Le terme de « sécuritisation » est employé par des chercheurs rattachés aux études critiques de sécurité. Thierry Balzaq le définit comme étant « un assemblage articulé de pratiques à travers lesquelles des artéfacts heuristiques (métaphores, instruments politiques, répertoires d'images, analogies, stéréotypes, émotions, etc.) sont contextuellement mobilisés par un acteur sécuritisateur qui incite l'audience à construire un réseau cohérent d'implications (sensations, pensées et intuitions), à propos de la vulnérabilité critique d'un objet de référence, lequel s'ajuste aux raisons de choix et d'actions de l'acteur sécurisateur, en investissant le sujet de référence d'une aura menaçante, à un point tel qu'une politique ciblée va immédiatement être adoptée pour le bloquer. »
BALZACQ, THierry, "A theory of securitization : origins, core assumptions, and variants", in : BALZACQ, Thierry (ed.), Securitization theory: how security problems emerge and dissolve, Routledge, 2010, p.3

[1483] Ibid

[1484] OilAlpha Malicious applications target humanitarian aid groups operating in Yemen, Recorded future, 09/07/2024 https://go.recordedfuture.com/hubfs/reports/cta-2024-0709.pdf
Yemen : Houthis disappear dozens of UN, Civil Society Staff, release detainees, end arbitrary arrests and enforced disappearances", *Human RIghts Watch,* 26/06/2024 https://www.hrw.org/news/2024/06/26/yemen-houthis-disappear-dozens-un-civil-society-staff

[1485]« Humanitaire : les chiffre de l'insécurité », *Alternatives humanitaires*, 2020, https://defishumanitaires.com/2020/09/25/humanitaire-les-chiffres-de-linsecurite/
PARADA, V., FAST, L., BRIODY, C. et al. "Underestimating attacks: comparing two sources of publicly-available data about attacks on health care in 2017", *Confl Health* 17, 3, 2023. https://doi.org/10.1186/s13031-023-00498-w
WEISSMAN, Fabrice, "Quantification et occultation des incidents de sécurité à Médecins Sans frontières", in, NEUMAN, Michael, WEISSMAN, Fabrice, *Secourir sans périr, la sécurité humanitaire à l'ère de la gestion des risques*, Paris: CNRS éditions, 2016,p.127-135

[1486] COTE, Anne-Marie, BERUBE, Maxime, DUPONT Benoit, « Statistiques et menaces numériques. Comment les organisations de sécurité quantifient la cybercriminalité », *Réseaux*, 2016/3-4 (n° 197-198), p. 203-224, https://www.cairn.info/revue-reseaux-2016-3-page-203.htm

*aux autorités, ça pourrait mettre les patients en danger. On va devoir peser les risques, voir quelles sont les données, voir quelles sont les personnes, si elles viennent d'Europe ou non. Voir ce qui pourrait être fait des données rapportées aux autorités (…). Pour le reporting de "data breach" on va voir quelle est la loi nationale qui s'applique. Si dans un pays il y a un risque énorme pour les patients, on va plutôt ne pas tout reporter aux autorités.* »[1487]

## Section 3 — Au-delà du régalien : approches humanitaires de la cybersécurité

Autant le lien entre la sécurité des humanitaires et les cyberopérations reste à construire, autant il existe un discours fort au sein de l'humanitaire (et plus spécifiquement au sein du CICR) sur la nécessité d'assurer la protection des bénéficiaires dans l'espace numérique. Ce discours s'inscrit en partie dans une remise en perspective des récits régaliens sur les menaces agitant le cyberespace par des organisations comme le Cyberpeace Institute ou IT4Peace. Elle se traduit par une injonction à remettre la personne au cœur de la cybersécurité. Un bon nombre d'ONG et d'acteurs impliqués dans la défense des droits humains en ligne revendiquent la défense d'une « cybersécurité centrée sur l'humain » (« human-centric cybersecurity »), mais aussi de « sécurité humaine numérique » (« digital human security »). Ces ONG s'opposent frontalement à ce qui constituent pour eux une prégnance de récits régaliens dans les politiques de cybersécurité, quitte peut être à minimiser les propres difficultés des Etats à sécuriser l'espace numérique. Les sections qui suivent vont détailler la position de ces ONG en nous demandant pour notre part comment le CICR se situe par rapport à leurs discours, et si elles prennent en compte la défense de la vie privée des personnes concernées ou non.

### § 1 — Sécurité humaine numérique

La défense d'une « cybersécurité centrée sur l'humain » s'inscrit plus largement dans un mouvement de décentrement d'une conception strictement régalienne de la sécurité, restreinte à la capacité d'un État de mener une riposte armée en cas d'attaque de sa souveraineté par d'autres États. Cette définition de la sécurité, pouvant être rattachée au paradigme réaliste en relations internationales, a été longuement remise en perspective, depuis au moins les années 1980. Le chercheur Barry Buzan est considéré comme un des précurseurs de la déconstruction de cette approche, ayant élargi le champ de compréhension de la sécurité à des dimensions sociétales. Toutefois, la protection de la sécurité sociétale serait d'abord, pour Barry Buzan, rattachée à la survie de l'État et non pas à la société en soi[1488]. Ce concept de « sécurité sociétale » va cependant être retravaillé, progressivement ce n'est plus l'Etat qui est menacé, mais la société. Ainsi Ole Waever parle de « sécurité identitaire ». Il entend par là la défense de l'identité d'un groupe social, culturel, voire religieux

[1487] Entretien n°17, ONG 6, DPO, 31/01/2020
[1488] BUZAN,Barry, People, States and Fear : the National Security Problem in International Relations, Brighton, Harvester, 1991

ou ethnique. À ce titre, la « sécurité identitaire » est parfois critiquée puisque pouvant être interprétée comme conduisant au repli de groupes identitaires face à des menaces « externes » [1489] .Parallèlement, d'autres chercheurs adoptent une approche plus constructiviste, voire sociologique, de l'étude de la notion de sécurité. Jeff Huysmans par exemple a interrogé la construction d'un phénomène en tant que problème de sécurité via la production de discours. De surcroit, la capacité de faire d'un sujet un problème de sécurité nécessite un certain nombre de ressources. La force de ces discours dépendant aussi, pour des analyses plus sociologique, de jeux de domination. Il s'agit d'analyser les acteurs qui énoncent la sécurisation de problématique, en analysant les jeux de pouvoir et les luttes entre agents pour imposer une définition légitime de la menace.

La notion de sécurité acquiert ainsi une certaine souplesse, et dépasse aussi le cadre du champ militaire et les violences armées, pour inclure de nouvelles menaces, qu'elles soient migratoires, environnementales, voire sanitaires (et actuellement numériques). Au risque que l'inclusion de ces menaces à l'agenda d'acteurs régaliens puisse légitimer l'élargissement de leur spectre d'action. D'autant que conjointement à cette extension du spectre d'action potentiel des acteurs de la sécurité, leur champ de projection s'élargit, et l'échelle internationale est également investie par des acteurs considérés comme régaliens, à savoir les forces de l'ordre, ou des services de renseignement[1490], qui perdent toutefois le monopole de l'exercice de la sécurité, cette dernière étant assurée aussi par des acteurs privés ( cela est flagrant concernant la cybersécurité)[1491].

En somme, réfléchir sur la notion de sécurité signifie s'interroger sur le rôle des différents acteurs impliqué dans la construction et la gestion de la sécurité d'une entité. S'agit-t-il d'assurer la sécurité de l'Etat ou d'un groupe social, d'individus ? Qui apparait comme légitime dans cette tâche ? Comment son rôle est justifié, par des discours, par différentes ressources et capitaux ? ?

En tout cas, c'est dans ce contexte théorique que, dans les années 1990, s'est formalisée la notion de sécurité humaine – en partie hors du champ académique et au sein des instances onusiennes[1492]. C'est cet ensemble doctrinaire qu'on va détailler, puisqu'il va inspirer, une trentaine d'année plus tard une version numérique de la sécurité humaine.

---

[1489] Ole Waever définit la sécurité sociétale comme « la capacité d'une société à persister dans ses caractéristiques essentielles face aux conditions changeantes et face à des menaces probables ou réelles » WAEVER, Ole « Societal security. The Concept », *in* : WAEVER, O., BUZAN, B., KELSTRUP, M., LEMAITRE, P. (eds), *Identity, Migration and the New Security Agenda in Europe*, Londres, Pinter, 1993.
WAEVER, O. « Insécurité, identité : une dialectique sans fin », in Anne-Marie Le Gloannec (dir.), Entre union et nations. L'État en Europe, Paris, Presses de sciences po, 1998.

[1490] BIGO, Didier, « La mondialisation de l'(in)sécurité ? Réflexions sur le champ des professionnels de la gestion des inquiétudes et analytique de la transnationalisation des processus d'(in)sécurisation »

[1491] BIGO, Didier, « L'Europe de la sécurité intérieure : penser autrement la sécurité », in Anne-Marie Le Gloannec, Entre Union et nation. L'État en Europe, Paris, Presses de sciences po, 1998, p. 68.
HUYSMANS, Jeff« Dire et écrire la sécurité : le dilemme normatif des études de sécurité », Cultures & Conflits, 31-32 | printemps-été 1998

[1492] AXWORTHY, Lloyd, "La Sécurité Humaine : La Sécurité Des Individus Dans Un Monde En Mutation." *Politique Étrangère*, vol. 64, no. 2, 1999, pp. 333–42. http://www.jstor.org/stable/42677205. Accessed 12 May 2024.
BASTY, Florence, « La sécurité humaine : Un renversement conceptuel pour les relations internationales », *Raisons politiques*, 2008/4 (n° 32), p. 35-57. https://www.cairn.info/revue-raisons-politiques-2008-4-page-35.htm
KALDOR Mary, « La sécurité humaine : un concept pertinent ? », *Politique étrangère*, 2006/4 (Hiver), p. 901-914. https://www.cairn.info/revue-politique-etrangere-2006-4-page-901.htm

Pour revenir aux origine de cette notion, rappelons que c'est au sein du PNUD, qu'est publié en 1994 un rapport considéré comme une des premières théorisations de la sécurité humaine. Cette approche entend envisager la sécurité de façon multidimensionnelle. La sécurité humaine engloberait la sécurité économique, la sécurité alimentaire, la santé, la sécurité environnementale, la sécurité individuelle, la sécurité sociétale (communautaire), la sécurité politique. De fait, il s'agit d'une notion large, embrassant un large spectre de sujets. Un promoteur de ce type d'approche, Lloyd Axworthy déclare ainsi dans un rapport de la Commission sur la « sécurité humaine », qu' : « essentiellement, la sécurité humaine signifie la protection des individus contre les *menaces*, qu'elles s'accompagnent ou non de violence. »[1493] À l'ONU, c'est, entre autres, Kofi Annan qui cherche à mettre à l'agenda de l'organisation la sécurité humaine. Un rapport sur le sujet est publié en 2009, Human security Handbook. Différents groupes de travail sont ensuite créés, notamment le Board for Human security. Le Japon et la Norvège y participent. Ce dernier formule comme suit de la définition de la sécurité humaine : « une approche visant à aider les États membres à identifier et à relever les défis généralisés et transversaux pour la survie, les moyens de subsistance et la dignité de leur population, qui couvre le droit des personnes à vivre dans la liberté et la dignité, à l'abri de la pauvreté et du désespoir, des réponses centrées sur les personnes, globales, spécifiques au contexte et axées sur la prévention, qui renforcent la protection et l'autonomisation de toutes les personnes et de toutes les communautés, en reconnaissant les liens entre la paix, le développement et les droits de l'homme. »[1494]

Au Japon, deux figures ont contribué à conceptualiser la notion de sécurité humaine : Sadako Ogata et Amartya Sen. Pour Amartya Sen, la sécurité humaine consiste dans la protection du : « noyau vital de toutes les vies humaines, d'une façon qui améliore l'exercice des libertés et facilite l'épanouissement humain. » [1495] On a affaire à une interprétation libérale de la sécurité humaine, établissant un lien entre les droits humains, le développement et la sécurité[1496]. Les droits de l'homme seraient même au fondement de la sécurité humaine, ou bien en seraient complémentaires. Du moins, la sécurité humaine contribuerait à garantir ces derniers, en les « sécurisant ». Mais pour les plus critiques, la sécurité humaine serait redondante, et n'apporterait rien de plus que les approches fondées sur la protection des droits de l'homme,

GROS Frédéric, « Désastre humanitaire et sécurité humaine. Le troisième âge de la sécurité », *Esprit*, 2008/3-4 (Mars/avril), p. 51-66. https://www-cairn-info.ezproxy.utc.fr/revue-esprit-2008-3-page-51.htm
TADJBAKHSH, Shahrbanou, "human security: concepts and implication, with an application to post-intervention challenges in Afghanistan", Les études du CERI, N° 117-118, September 2005
https://www.sciencespo.fr/ceri/sites/sciencespo.fr.ceri/files/etude117_118.pdf
GROS Frédéric, CASTILLO Monique, GARAPON Antoine, « De la sécurité nationale à la sécurité humaine », *Raisons politiques*, 2008/4 (n° 32), p. 5-7. https://www.cairn.info/revue-raisons-politiques-2008-4-page-5.htm

[1493] AXWORTHY, Llyod, « La sécurité humaine : la sécurité des individus dans un monde en mutation », *Politique étrangère*,64-2, 1999, p. 333-342

[1494] an approach to assist member states in identifying and addressing widespread and cross cutting challenges to the survival, livelihood and dignity of their people which covers the right of people to live in freedom and dignity, free from poverty and despair, people centred comprehensive, context specific and prevention oriented responses that strengthen the protection and empowerment of all people and all communities recognizing the interlinkages between peace, development and human rights" Human Security in theory and practice, United Nations Trust fund for human security, 2009

[1495] *La sécurité humaine maintenant*, Rapport de la Commission sur la sécurité humaine, Paris, Presses de Sciences Po, 2003.

[1496] OBERLELTNER, GERB (ed.), *Research Handbook on international law and human security*, New York: Edward Ekgar publishing, 2022.
OBERLEITNER, Gerd, "Human Security and human rights", European training-and-research centre for human rights and democracy, issue n° 8, June 2002 https://www.files.ethz.ch/isn/31301/08.pdf

ou bien elle en donnerait une vision restrictive et tendrait à dépolitiser les droits de l'homme en se limitant à la protection du droit à la sécurité et à la vie[1497].

Ajoutons que les présupposés de la doctrine de la sécurité humaine contribuerait à remettre en cause les principes westphaliens de la souveraineté. L'État souverain n'est plus le seul acteur définissant les enjeux sécuritaires. Le champ de la sécurité dépasse le domaine régalien. Des mécanismes de protection peuvent être mis en œuvre par des gouvernements régionaux, des États, des membres de la communauté internationale (comme des ONG). Dans le même temps[1498], la fonction de protection des États est en partie disqualifiée. Au contraire. Les États seraient potentiellement porteurs de menaces contre leurs propres populations. Leur fragilisation irait de pair avec l'émergence de menaces hybrides, d'insécurité latente. Il s'agit ainsi de sécuriser l'État et mettre en place des politiques de « state building » et de « peace building » afin de contribuer à restaurer la souveraineté d'États faillis et donc dangereux pour la communauté internationale. L'approche systémique de la sécurité humaine appliquée aux conflits mettrait au cœur de son action la protection des civils et « sécurise » les droits de l'homme[1499]. D'où une instrumentalisation de la notion de « sécurité humaines » qui alimente alors le nœud entre sécurité, politiques de développement et « peace building »[1500].

Or les menaces agitant le cyberespace entrainent l'émergence de nouveaux récits, dont des approches que certains acteurs désignent eux-mêmes par la formule de « sécurité humaine numérique ». La cybersécurité constituerait alors un nouveau pilier de l'approche de type sécurité humaine, à côté de l'économie, de l'environnement, de l'alimentation, de la santé. En tout cas, il est clair qu'existe une volonté de dépasser l'analyse « régalienne » de la cybersécurité, qui tendrait à mettre l'accent sur les intérêts de la nation (sécuritaires, économique)[1501]. L'analyse des dommages des cyberattaques doit alors prendre en compte d'autres répercussions, et élargir le concept de violence, en prenant en compte les dommages portant sur les infrastructures vitales, comme l'électricité, le réseau d'approvisionnement en eau[1502], infrastructures dépendant de façon croissante à Internet[1503].

Cela dit, il ne faut pas oublier que s'il a pu exister un mouvement de sécuritisation du cyberespace, si les récits souverainistes et régaliens prévalent, les gouvernements peuvent prendre en compte la nécessité d'assurer la protection des infrastructures vitales pour assurer le bon fonctionnement des sociétés. En France, la loi de programmation militaire de 2013, les

---

[1497] HOWARD-HASSMANN, Rhoda, "Human security : undermnining human rights? " *Human rights Quarterly* , 34, 2012, p.88-112

[1498] JOURDAIN, Edouard, « État d'exception et souveraineté. Genèse et mutations », *Réfractions*, 2013, hal-02106707

[1499] Comme la sécurité humaine appréhende les conflits de manière multi-sectorielle sans limiter son analyse à une cause unique, la réponse qu'elle apporte pour protéger la population dans un conflit est nécessairement systémique et intégrée. Envisager un conflit à travers le prisme de la sécurité humaine revient à se préoccuper des groupes vulnérables lors de ce conflit et amplifier la protection des droits de l'homme. BASTY Florence, « La sécurité humaine : Un renversement conceptuel pour les relations internationales », *Raisons politiques*, 2008/4 (n° 32), p. 35-57. DOI : 10.3917/rai.032.0035. URL : https://www.cairn.info/revue-raisons-politiques-2008-4-page-35.htm

[1500] DUFFIELD, Mark, "Human Security: Linking Development and Security in an Age of Terror", GDI panel "New interfaces between Security and development", 11 General conference of the EADI, 21-24 September 2005

[1501] DUNN, CAVELTY, Myriam, "Breaking the cybersecurity dilemma : aligning security needs and removing vulnerabilities", *Sci Eng Ethics* 20, 2014, p.701–715 https://doi.org/10.1007/s11948-014-9551-y

[1502] Written Evidence submitted by the Human Security Centre
https://committees.parliament.uk/writtenevidence/121729/pdf/

[1503] SINOZIC-MARTINEZ, Tanja, JAHNEL, Jutta, " TA for human security : aligning security cultures with human security in AI innovation", Journal for technology assessment in theory and practice, 24/06/2024

systèmes d'information des infrastructures d'importance vitale doivent prendre des mesures de protection spécifiques et doivent être signalés à l'ANSSI[1504]. Par exemple les systèmes d'information des hôpitaux ne sont considérés comme tels que depuis 2023[1505]. Toutefois, à l'échelle internationale, il n'existerait pas de protection unifiée, d'où la nécessité pour certains juristes comme Patryk Pawlak et Aude Géry de dépasser l'échelle nationale et d'établir un cadre normatif commun[1506], qui devrait, pour le Cyberpeace Institute, inclure les hôpitaux et les ONG humanitaires[1507].

Mais surtout, ces différentes initiatives suivent un mouvement plus général de sécuritisation des infrastructures, qui découle lui-même du contexte de la guerre froide, de la peur des destructions que le feu nucléaire pourrait porter sur les infrastructures essentielles, un récit réactualisé lors de la lutte contre le terrorisme. Stephen Collier inscrit donc la protection des infrastructures critiques dans un agenda régalien et en tant que problème de sécurité nationale[1508], bien qu'il précise ce point : pour lui, la gestion par les gouvernements des infrastructures vitales ne relèverait plus strictement du registre du régalien du fait de la mise à l'agenda de nouvelles « menaces » (comme les catastrophes climatiques ou les pandémies), et équivaudrait selon lui d'une gouvernementalité des populations. Il revendique ainsi une ce qui constitue, pour lui, une lecture foucaldienne fondée sur la notion de biopolitique de la gestion des infrastructures critiques par les États[1509].

Quant à la gestion des infrastructures critiques face aux cyberopérations, elle a pu être revendiquée par une série d'acteurs à un enjeu de sécurité nationale[1510], un fait illustré par l'alerte récente par la « Cybersecurity and infrastructure security agency » CISA, la NSA et le FBI concernant la présence de hackers chinois dans le réseau américain d'infrastructures critiques (réseaux de transports, électricité, réseau hydraulique, etc.), le tout dans un contexte de tension entre la Chine et les États-Unis[1511]. Cela reste à creuser, mais la protection d'infrastructures critiques pourrait relever de l'inclusion d'une cybersécurité sociétale au sein d'acteurs étatiques, au nom de la continuité du fonctionnement d'un Etat. Sachant qu'une chercheuse comme Myriam Dunn Cavalty a pu analyser les frictions et tension dans l'implication d'acteurs privés dans la défense des infrastructures critiques, dont le monopole de la part d'acteurs régaliens est questionnée, puisque leur sécurité est, dans une certaine mesure, nécessairement en partie déléguée du fait de la nature transversale du numérique,

---

[1504] https://cyber.gouv.fr/le-dispositif-saiv

[1505] Arrêté du 17 avril 2023 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au sous-secteur d'activités d'importance vitale « Etablissements de santé » et pris en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du code de la défense https://affairesjuridiques.aphp.fr/textes/arrete-du-17-avril-2023-fixant-les-regles-de-securite-et-les-modalites-de-declaration-des-systemes-dinformation-dimportance-vitale-et-des-incidents-de-securite-relatives-au-sous-secteur-dactivites/

[1506] PAWLAK, Patryk, GERY, Aude, "Why the world needs a new cyber treaty for critical infrastructure", *Carnegie*, 28/03/2024 https://carnegieendowment.org/research/2024/03/why-the-world-needs-a-new-cyber-treaty-for-critical-infrastructure?lang=en

[1507] "Protecting critical infrastructure through the implementation of cyber norms", *Cyberpeace Institute*, 26/04/2023 https://cyberpeaceinstitute.org/protecting-critical-infrastructure-through-cyber-norms/

[1508] GALLAND Jean-Pierre, « Critique de la notion d'infrastructure critique », *Flux*, 2010/3 (n° 81), p. 6-18. DOI : 10.3917/flux.081.0006. URL : https://www.cairn.info/revue-flux1-2010-3-page-6.htm

[1509] COLLIER, Stephen, LAKOFF, Andrew, The governement of emergency, Vital systems, expertise, and the politics of security, Princeton University Press, 2021

[1510] BARAM, Gil, MENASHRI, Harel," Critical Infrastructures and their interdependence in a cyber-attack- the case of the US", Military and strategic affairs,vol 7, n°1, March 2015

[1511] PRC State-sponsored actors compromise and maintain persistent access to US critical infrastructure, American Cyber Defense agency, 07/02/2024 https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

de l'inclusion d'acteurs privés et d'entreprise dans la gestion de la cybersécurité au jour le jour[1512], et du lien entre acteurs privés d'analyse de la menace et les services étatiques liés aux organes de cyberdéfense et cyberoffensifs de l'Etat[1513], les individus étant également invité à participer à la stabilité du cyberespace, par l'adoption de gestes d'hygiène numérique.

Toujours est-il qu'au-delà des dommages matériels, pour certains acteurs, certaines approches de la « sécurité humaine » prennent aussi la possibilité d'épanouissement des personnes, et donc comprend aussi une dimension subjectives, et émotionnelles, et pourrait inclure la nécessité non pas simplement de défendre les infrastructures mais aussi la vie privée des personnes. Ainsi pour Kristin Sandvik et Raymond Nathaniel la protection de l'identité individuelle des constitue une composante centrale de la sécurité humaine numérique : « Nous suggérons qu'étant donné que l'identité sociale est de plus en plus constituée par les technologies de l'information, les menaces pesant sur la protection des données et la vie privée peuvent être utilement considérées comme des menaces fondamentales pour la sécurité humaine. »[1514] Bien que le prisme de la sécurité humaine ait pu être interprété comme étant de l'ordre d'un bio-pouvoir (dans le sens qu'en donne Agemben)[1515], ce type d'interprétation va de pair avec la défense des droits des individus.

Et de fait, les différents acteurs reprennent ce discours, en y apportant des variations selon qu'il s'agit d'organisations impliquées dans la « pacification » du cyberespace comme ICT4Peace, Cyberpeace institute etc. , ou engagés dans actions de « consolidation de la paix » (« peacebuilding »), ou de la défense des droits de l'homme ou faisant partie des cercles onusiens , des acteurs engagés dans des organisations de défense des droits de l'homme.

Au sein des Institutions onusiennes, on ne retrouve pas ces thématiques dans les organes ayant poussé l'agenda de la sécurité humaine. Le conseil de sécurité adopte une lecture régalienne du risque cyber, à la frontière de la thématique de la criminalité cyber, tout comme l'assemblée générale de l'ONU et le comité désarment et sécurité internationale[1516]. Notons

---

[1512] « La cybersécurité est et restera une responsabilité partagée responsabilité partagée entre les acteurs publics et privés. Les gouvernements doivent continuer à jouer leur rôle en protéger les infrastructures critiques lorsque cela est nécessaire, tout en déterminant la meilleure façon d'encourager les forces du marché à améliorer la sécurité et la résilience des réseaux appartenant aux entreprises. »"Cyber security is and will remain a shared responsibility between public and private actors. Governments should maintain their role in protecting critical infrastructure where necessary, while determining how to best encourage market forces to improve the security and resilience of company owned networks."
DUNN CAVELTY, Myriam, " The militarization of cyberspace: why less may be better", 2012, *4th international conference on cyber conflict*
DUNN CAVELTY, Myriam, "Critical information infrastructure: vulnerabilities, threats and response", *Disarmament forum, ICTs and international security*, 2007
DUNN CAVELTY, Myriam, EGLOFF, Florian J., "The Politics of Cybersecurity: Balancing Different Roles of the State." St Antony's International Review 15 no.1, 2019, :37-57.

[1513]BANNELIER, Karine, CHRISTAKIS, Theodore, Cyberattaques - Prévention-Réactions : Rôles des Etats et des acteurs privés (Cyber-Attacks. Prevention-reactions: The Role of States and Private Actors) (February 25, 2017). Les Cahiers de la Revue Défense Nationale, Paris, 2017, https://ssrn.com/abstract=2957795

[1514] « We suggest that as social identity is increasingly constituted through information technology, threats to data protection and privacy can usefully be understood to now exist as core threats to human security
SANDVIK, Kristin, RAYMOND, Nathaniel, "Beyond the Protective Effect: Towards a Theory of Harm for Information Communication Technologies in Mass Atrocity Response," *Genocide Studies and Prevention: An International Journal*: Vol. 11 : Iss. 1, 2017 p.9-24

[1515] DE LARRINAGA, MIGUEL, and MARC G. DOUCET. "Sovereign Power and the Biopolitics of Human Security." *Security Dialogue*, vol. 39, no. 5, 2008, p. 517–37

[1516] PYTLAK, Allison, "Exploring human -centric cyber security", *Humanitarian Disarmament*, 06/02/2023, https://humanitariandisarmament.org/2023/02/06/exploring-human-centric-cyber-security/ "Forums like the IGF were somewhat more predisposed to consideration of a human rights or human-centric dimensions of cyber and digital security, in contrast to more traditional disarmament bodies like the UN General Assembly (UNGA) First Committee on Disarmament and International Security, where the framing centers around state use of information and communications technology (ICT) and "cyber war."

au passage qu'au-delà de l'ONU, un acteur défendant a priori des intérêts régaliens, l'OTAN a récemment inscrit à son agenda le thème de la sécurité humaine[1517], dans la continuité de l'élargissement de son mandat, hors du domaine strictement régalien, mais ne le relie pas aux menaces numériques, mentionnées dans son document stratégique de 2022. Les deux agendas ne sont pas encore fusionnés[1518].

Enfin, à l'UN Open Ended Working Group (OEWG), la thématique peinerait à se frayer un chemin parmi les États membres comme a pu le montrer Sheetal Kumar, malgré le travail de plaidoyer d'ONG et la prise en compte grandissante des acteurs de la société civile dans ces cercles de la « diplomatie numérique »[1519]. Différentes initiatives visent à pousser cette agenda au sein de l'ONU et parmi les Etats, notamment en 2021 la signature du « Joint civil society statement on cyber peace and human security » à l'assemblée onusienne du comité sur le désarmement et la sécurité internationale[1520].

On retrouve quelques traces de la notion de sécurité humaine numérique au sein de sous-forum, comme celui intitulé « human security for all ». Il défend une vision « enchantée » de la technologie, permettant de résoudre les problématiques de sécurité humaine traditionnelle, et au sein de ce forum de discussion le cyberespace ne semble pas perçu comme un espace de menace[1521].

---

[1517] HEARD, Kaleigh,THUE, Kristin, "A new aera? Nato's prioritization : human security in an insecure world", RAND, 10/08/2022 https://www.rand.org/pubs/commentary/2022/08/a-new-era-natos-prioritisation-of-human-security-in.html
"The Guiding Principles highlight five key areas where the alliance intends to be most effective in attending to the considerations for the security of civilians in its operations: (a) protection of civilians, (b) preventing and responding to conflict-related sexual violence, (c) combating trafficking in human beings, (d) children and armed conflict, and (e) protection of cultural property. "
SOLARI, Dominic, SWEENEY, Hannah, "Human security and changing threats: Nato's Policies for 2022 and Beyond", *Lawfare Media*, 05/12/2022 https://www.lawfaremedia.org/article/human-security-and-changing-threats-natos-policies-2022-and-beyond
NATO, "Human Security approach and guiding principles", 14/10/2022, https://www.nato.int/cps/en/natohq/official_texts_208515.htm?selectedLocale=en

[1518] "NATO's new policies were released at a critical time for international peace and security. The Strategic Concept reaffirms existing commitments to rules-based international order and democratic order. However, it also acknowledges the changing threats posed by Russia's war of aggression, terrorism, hybrid tactics, space and cyberwarfare, and climate change. Despite the need to aggressively deter and defend the alliance, NATO seems committed to adopting a human security approach that considers the civilian impact of all military action." Human Security approach and guiding principles, NATO,14/10/2022https://www.nato.int/cps/en/natohq/official_texts_208515.htm?selectedLocale=en

[1519] KLEINWACHTER, Wolfgang, "Cybersecurity, Internet Governance, and the Multistakeholder approach, the role of non-state actors in Internet Policy Making", Cyberstability Paper series, Global Commissions on the stability of Cyberspace, *The Hague Centre for strategic Studies,* December 2021 https://hcss.nl/wp-content/uploads/2021/12/Kleinwaechter.pdf
Civil society perspectives on the "Initial pre-draft of the OEWG on developments in the field of information and telecommunications in the context of international security",2020
https://ceipfiles.s3.amazonaws.com/pdf/CyberNorms/UNGGE/Civil+Society+Perspectives+on+the+%E2%80%9CInitial+Pre-Draft+of+the+OEWG+on+Developments+in+the+Field+of+Information+and+Telecommunications+in+the+Context+of+International+Security%E2%80%9D.pdf
ICT4PEACE, "Submission by ICT4Peace to the Open-Ended Working Group (OEWG) on security of and in the use of information and communications technologies 2021-2025", 2022,
https://ict4peace.org/wp-content/uploads/2022/01/ICT4PeaceSubOEWGIIJan2022ds-1.pdf
FERRARI, Veronica, KUMAR, Sheetal, "A human-centric approach to international cybernorms: Civil society feedback on the UN Open-Ended Working Group on ICTs proposals", Association for progressive communication, 01/12/2020
https://www.apc.org/en/news/human-centric-approach-international-cybernorms-civil-society-feedback-un-open-ended-working
Cyberpeace institute, "The OEWG "Zero Draft": The Need For A Stronger Human-centric Approach",26/02/2021
https://cyberpeaceinstitute.org/news/the-oewg-zero-draft-the-need-for-a-stronger-human-centric-approach/
KUMAR, Sheetal, " The missing piece in human-centric approaches to cybernorms implementation: the role of civil society", *Journal of Cyber Policy*, 6:3, 2021, p. 375-393.

[1520] PITLAK, Allison, "Joint civil society statement on cyber peace and human security UN General Assembly First Committee on Disarmament and International Security", 8/10/ 2021 https://reachingcriticalwill.org/images/documents/Disarmament-fora/1com/1com21/statements/8Oct_cyberpeace.pdf

[1521] https://humansecurity.world/

Au sein du PNUD, organe ayant porté la notion de sécurité humaine, la greffe numérique a du mal à prendre. Seul un rapport de 2022, intitulé les « Nouvelles menaces pour la sécurité humaine à l'âge de l'Anthropocène », évoque cette dimension. Mais le numérique est certes envisagé comme une menace, mais ce dernier pourrait aussi contribuer au développement social et individuel, au bien-être et à l'épanouissement de la société — de l'économie, du libre marché, et de l'individu dont l'épanouissement passe par la consommation d'informations. La défense de la sécurité humaine dans un contexte numérique a pour objectif final le renforcement des capabilités humaines, en écho avec un terme au centre des réflexions d'Amartia Sen qui a mis au cœur de sa pensée cette notion : « Si les implications en matière de sécurité humaine ne sont pas prises en compte, les nouvelles technologies pourraient ne pas tenir leur promesse d'accroître les capacités humaines. » [1522]

De surcroit, les ONG proches de la défense des droits en ligne mettent évidemment la personne au cœur de la cybersécurité, sans systématiquement reprendre le concept de "sécurité humaine". Une version la plus représentative de cette approche est celle donnée par Ron Deibert, le directeur du Citizen Lab[1523]. Dans un article où il précise sa pensée sur cette notion, on retrouve l'opposition entre les États comme vecteur de menace et la société civile garante de la défense des droits humains, dont la sauvegarde devient alors un enjeu de sécurité, en lien avec les formes de violence d'État et les actes de répression contre les militants des droits de l'homme. La protection des droits de l'homme permettrait alors de garantir la sécurité des personnes[1524].

Enfin, d'autres ONG se rattachent aussi à des actions de type «consolidation de la paix » (« peacebuilding ») et la défense des droits humains en ligne s'inscrit dans une démarche plus globale de « pacification » de l'espace numérique, justifiant la nécessité de sécuriser l'Internet pour assurer la protection des individus, en mettant « l'humain au centre » des politiques de cybersécurité [1525]. Ce type de positionnement est celui d'ONG comme Cyberpeace Institute ou encore ICT4PEACE dont on cite ici un extrait d'un de leurs communiqués : « Comment pouvons-nous garantir les droits, les données et la vie privée des individus en ligne, en utilisant les approches traditionnelles de la sécurité nationale, alors que les défis auxquels nous sommes confrontés sont intrinsèquement à la fois locaux, citoyens et

---

POSNER, Carolyn, "CTA announces technology as new human security pillar, *Consumer Technology association*, 18/09/2023 https://www.cta.tech/Resources/Newsroom/Media-Releases/2023/September/CTA-Announces-Technology-as-New-Human-Security-Pil
DUCQ, Alice, "UN adds tech as human security pillar in lead-up to CES 2024", *Consumer technology association*, 25/09/2023 https://www.ces.tech/articles/2023/september/un-adds-tech-as-human-security-pillar-ces-2024.aspx

[1522] "If the human security implications remain unaddressed, new technologies could fall short in their promise to expand human capabilities" PNUD, New threats to human security in the Anthropocene, 2022

[1523] Il s'agit d'un institut de recherche canadien rattaché à l'Université de Toronto étudiant les différentes menaces aux droits de l'homme en ligne (censure d'internet, surveillance et vie privée). Il a participé à l'enquête sur le logiciel espion Pegasus.

[1524] « Securing privacy requires a comprehensive approach in which individuals are empowered to control what happens to their data no matter where it is located, and governments and companies should have legal obligations to treat data in ways that protect the privacy of all users and citizens—thus promoting human security » DEIBERT, Ron, « Toward a Human-Centric Approach to Cybersecurity », *Ethics & International Affairs, 32*(4), 2018

[1525] "cyber peacebuilding adopts a human-centered approach and promotes an emancipatory normative stance on the provision of cybersecurity (Collins, Reference Collins, Salminen, Zojer and Hossain2020). Within this context, cyber peacebuilding is a reformulation and an extension of the definition of peacebuilding adapted to the digital age. Drawing upon the definition of peacebuilding proposed by the Alliance for Peacebuilding (2012), we define cyber peacebuilding as an active concept that captures those activities that delegitimize online violence, build capacity within society to peacefully manage online communication, and reduce vulnerability to triggers that may spark online violence" SHACKELFORD SJ, DOUZET F, ANKERSEN C, « Modalities: How Might Cyber Peace Be Achieved? What Practices and Processes Might Need to Be Followed in Order to Make It a Reality? » In: SHACKELFORD SJ, DOUZET F, ANKERSEN C *(ed.), Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace*, Cambridge University Press, 2022,p.37-128.

internationaux ? Une solution pourrait consister à élaborer des politiques qui considèrent l'individu comme l'épicentre du défi de la sécurité au lieu de la souveraineté territoriale traditionnelle ; les êtres humains doivent être au cœur de l'agenda des technologies de l'information et de la sécurité à l'avenir. » [1526]

Quant au Cyberpeace Institute, son approche est largement fondée sur la notion de sécurité humaine. Cela est flagrant si on se réfère à sa définition de la « paix numérique » (« cyberpeace »), qui repose largement sur cette notion. Elle est entendue comme le fait d'assurer le droit à la vie, à la sécurité et le droit à la liberté des individus. Cela implique la protection des biens nécessaires à la préservation de la vie des individus, ainsi que des infrastructures critiques. On pourrait y voir une approche restrictive, presque biopolitique de la sécurité humaine, mais l'organisation ajoute que la « paix numérique » doit aussi inclure, au-delà de la sécurité, la protection de la dignité des citoyens, ainsi que leurs droits humains (et donc leur vie privée)[1527].

## § 2 — Protection des civils dans l'espace numérique, l'approche du CICR

Comment les ONG humanitaires se situent-elles par rapport à ces discours ? Si l'on prend le cas du CICR, on peut dire que l'organisation plaide également pour mettre le bénéficiaire au cœur de la cybersécurité, mais en se référant plutôt au principe de protection. Car les liens entre humanitaire, sécurité humaine et droits de l'homme sont complexes. Assurer la stabilisation d'une zone géographique selon une approche systémique propre aux doctrines de sécurité humaine implique l'intervention d'urgence, mais également le fait de prendre en compte le développement économique sur le long terme, ainsi que garantir la protection des droits de l'homme[1528]. Les doctrines de sécurités humaines peuvent recouper l'approche humanitaire, et notamment leur action de protection. Mais elles se distinguent de celle des ONG humanitaires, notamment lorsqu'elles sont attachées au principe de neutralité, comme

[1526]« how can we secure individuals' rights, data and privacy online, using traditional national security approaches when the challenges we face are inherently both local citizen-based, and international? One way forward could be to develop policies that consider the individual as the epicenter of the security challenge instead of only traditional territorial sovereignty; human beings need to be the core focus of the IT and security agenda going forward."
"Human security in the age of AI: securing and empowering individuals", ICT for Peace foundation, 2018
https://ict4peace.org/wp-content/uploads/2018/12/Digital-Human-Security-Final-DSmlogos.pdf

[1527]"La dignité humaine est propre à l'expérience de toute personne et s'inscrit dans le cadre de ses conditions de vie quotidiennes". Les droits liés à cette définition comprennent, sans s'y limiter, les droits civils et politiques, la liberté d'expression et de réunion, ainsi que les droits culturels et autochtones. "Human dignity is unique to the individual's experience and context-specific to their everyday realities. Rights relating to this definition include, but are not limited to, civil and political rights, along with freedom of expression and assembly, as well as cultural and indigenous rights. "SHACKELFORD SJ, DOUZET F, ANKERSEN C, (eds.), " Reflections and Research Notes", In: SHACKELFORD SJ, DOUZET F, ANKERSEN C *Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace*, Cambridge University Press, 2022, p. 193-242.

[1528] « Afin de préserver les populations, la sécurité humaine recommande alors de renforcer l'action humanitaire qui est un moyen de protéger assez rapidement les individus dans les situations d'urgence en répondant aux besoins essentiels d'eau, d'assainissement, de soin et de logements. Or, comme on le sait, l'action humanitaire est parfois utilisée par certains responsables pour réduire au minimum l'impact sur les civils et faire taire les critiques internationales. La relation entre l'action humanitaire et l'action de développement est elle aussi complexe, en particulier si l'aide, par son efficacité, affaiblit l'incitation à chercher des solutions politiques. La protection des droits de l'homme et le respect du droit humanitaire sont des conditions essentielles de la sécurité humaine dans les situations de conflits. Comme la plupart des règles du droit international, celles qui régissent la protection des droits de l'homme ont été conçues dans une perspective centrée sur l'État. » BASTY, Florence, « La sécurité humaine : Un renversement conceptuel pour les relations internationales », *Raisons politiques*, 2008/4 (n° 32), p. 35-57. https://www.cairn.info/revue-raisons-politiques-2008-4-page-35.htm

le CICR[1529]. Les doctrines de sécurité humaine n'ont pas été directement à son agenda et l'organisation humanitaire met plutôt en avant les impératifs de protection, garantis par le DIH. Ce terme désigne initialement l'action que mène une organisation responsable de l'application de textes de droit international ; par exemple, l'UNHCR est garant de l'application de la Convention de 1951 relative au statut de réfugié. Elle est donc chargée d'assurer la « protection » des exilés en leur accordant (ou non) ce statut. Quant au CICR, il est garant de l'application des Conventions de Genève, dont un des objectifs est la protection des civils lors d'affrontements armés. Les Conventions obligent les parties prenantes d'un conflit à assurer la sécurité des civils et des individus qui ne participent pas aux hostilités directement. Plus largement, ce cadre juridique est mis en place à partir de la Seconde Guerre mondiale.

Les années 1990 constituent un second moment clef concernant la protection des non-combattants, du fait de leur poids grandissant parmi les victimes et de la multiplication des guerres civiles. Progressivement, le terme de protection évolue et s'élargit. Il adopte un second sens et englobe à la fois responsabilité de protéger et devoir d'ingérence humanitaire, soit la légitimation de l'intervention d'États afin de porter secours à des populations victimes de conflits en dépit des souverainetés étatiques.

Au fil du temps, il prend un troisième sens et désigne des « activités de protection » mises en place par des ONG spécifiques. Dans ce dernier cas, la notion de protection a alors une double dimension Elle signifie premièrement l'obligation pour les humanitaires de ne pas atteindre eux-mêmes à la sécurité, à la dignité et aux droits des personnes auxquelles elles apportent de l'aide ; et deuxièmement le fait de faire en sorte que les gouvernements respectent leurs obligations de protection et les droits des personnes[1530]. Les activités de protection ont donc comme finalité de « prévenir et alléger en toutes circonstances les souffrances des hommes ; de protéger la vie et la santé et de faire respecter la personne humaine de façon impartiale. » Par conséquent, les activités de protection cherchent à assurer que les personnes bénéficient du respect intégral de leurs droits, comme le prévoient la lettre et l'esprit des textes de droit (à savoir droits de l'homme, droit humanitaire, droit des réfugiés). »[1531]

Pour le CICR, la protection implique que les autorités respectent leurs obligations et les droits des individus de manière à préserver la vie, la sécurité physique et l'intégrité morale ainsi que la dignité. L'objectif est ainsi de prévenir ou de mettre fin à de potentielles violations du DIH, en renforçant la sécurité des individus et réduisant leur exposition à des risques[1532].

Trois principes régissent le travail de protection :
— Respecter les principes d'humanité, d'impartialité et de non-discrimination

[1529] SHUCKSMITH, Christy," Building human security through humanitarian protection and assistance : the potential of international Committee of the Red Cross", *Journal of Conflict transformation & security*, Vol.6/n°1, April 2017 https://cesran.org/wp-content/uploads/2010/11/JCTS_Vol6_No1_A3.pdf

[1530] ARJUN, Claire, « Evolution de la protection humanitaire : Perspective critique », *URD, revue HEM,* 09/05/2016

[1531] "Protection of Internally Displaced Persons", Inter Agency Standing Committee Policy Paper, December 1999, p.4https://interagencystandingcommittee.org/system/files/legacy_files/FINALIDPPolicy.pd
Politique du comité permanent interinstitutions sur la protection dans le cadre de l'action humanitaire, IASC, 2018 https://interagencystandingcommittee.org/sites/default/files/migrated/2018-10/iasc_protection_policy_french_logo_final.pdf

[1532] ICRC, "enhancing protection - for civilians in armed conflict and other situations of violence", https://www.icrc.org/en/doc/assets/files/other/icrc-002-0956.pdf

— Éviter les effets néfastes, c'est-à-dire respecter le principe de non-nuisance (« do no harm »)
— Placer les populations, communautés et personnes touchées au cœur de l'action déployée et se montrer ainsi responsable envers elles.

Il s'agit d'une définition générale qui peut connaitre des variations en fonction des ONG, selon que l'accent est mis soit sur la protection de telle ou telle catégorie de personnes, soit sur les atteintes aux droits de l'homme et/ou au DIH. On peut aussi parler de « protection autonome » (stand alone), soit un programme qui a un objectif inhérent de protection. Il existerait ainsi quatre activités de protection à proprement parler : protection de l'enfance, protection contre les violences basées sur le genre, les actions anti-mine, et action de protection relative à la propriété foncière. On parle aussi de « protection intégrée », ce qui désigne l'intégration d'activités de protection dans d'autres programmes humanitaires (santé, nutrition, éducation, gestion des camps, etc.). On parle enfin de protection en tant qu'approche (« mainstreaming protection »), qui intègre la protection comme fondement d'un programme en respectant le principe « ne pas nuire » (« do no harm »)[1533].

Si on prend le cas du CICR, l'organisation s'est impliquée spécifiquement dans la protection des civils dans les conflits armés. La chercheuse Miriam Bradley, dans son ouvrage *Protecting Civilian in War* la définit comme suit : « en mettant l'accent sur la sécurité physique des civils, en partant du principe que la protection est fondamentalement liée à la violence et que les objectifs de toute activité de protection doivent consister à protéger les personnes contre la violence. »[1534]

Au cœur de la protection des civils, il y a donc la volonté de préserver les individus de toute forme de violence. Et d'ailleurs, Miriam Bradley rappelle que la protection des civils s'est développée concomitamment à celle de sécurité humaine, dans le cours des années 1990 et des différents conflits comme en Yougoslavie ou lors du génocide du Rwanda. La nécessité de protéger les civils au cœur des conflits remonte au milieu du XXème siècle. L'objet de la première convention de Genève n'est pas les civils, mais les combattants hors de combat. C'est après la Seconde Guerre mondiale et ses drames que la Quatrième convention de Genève, adoptée en 1949, commence à prendre en compte la situation des civils. Cela dit, Miriam Bradley relativise cette première mise à l'agenda : ne sont en effet concernés que les civils dans des territoires occupés. Et c'est seulement en 1977 que deux protocoles additionnels à la 4e convention de Genève incluent leur protection. Cela dit, il manque encore la définition de ce qu'est un civil dans le cadre de conflits non étatiques et par conséquent ce qui constitue le principe de non-discrimination.

[1533]BONINO, Francesca, "Evaluating protection in humanitarian action: Issues and challenges", *AlnapWorking paper*, 2014
[1534] « with a focus on the physical safety and security of civilians, on the basis that protection is fundamentally about violence, and the objectives of any protection activity must be about protecting people from violence. »
BRADLEY, Miriam, *Protecting civilians in war, the ICRC, UNHCR, and their limitations in internal armed conflicts*, Oxford University Press, 2016, 232 p.
BRADLEY, Miriam. "Chapter 6: Human security in armed conflict: norms, agendas and actors for protecting civilians", in OBERLEITNER, Gerd, *Research Handbook on International Law and Human Security*", Cheltenham, UK: Edward Elgar Publishing, 2022,p. 126-145

Et donc le CICR mène des activités de protection, d'abord auprès des soldats blessés, puis au fil de l'extension de son mandat, auprès de prisonniers et de civils. Autre caractéristique de l'organisation, le DIH joue un rôle central dans les activités de protection du CICR : « l'essentiel du travail de protection du CICR consiste à présenter des allégations de violations du droit international humanitaire aux auteurs présumés dans l'espoir de mettre un terme à la violation en cours. »[1535] Et ajoutons aussi que le CICR joue un rôle de plaidoyer dans la régulation de certaines armes comme des mines antipersonnel, des armes numériques comme des cyberattaques, ou des armes automatiques à base d'intelligence artificielle[1536].

Le CICR a inscrit à son agenda la protection des civils à l'encontre de violences spécifiques : les mines, les violences touchant les femmes dans les conflits, et donc le cas des violences sexuelles, etc., et plus récemment les menaces numériques concernant les civils. Le titre d'un récent colloque organisé par le CICR est parlant : « protecting civilians against digital threats during armed conflict ». Ce dernier est le fruit du travail d'une équipe transdisciplinaire ayant documenté les différents impacts des cyber-opérations sur les non-combattants dans le cadre de conflits armés[1537]. Ces derniers ont dû prendre en compte la variété des impacts existants, des victimes, la variété des répercussions, également émotionnelles et donc difficilement quantifiables. On a évoqué dans une section précédente l'ensemble d'opération pouvant avoir lieu lors de conflits, cela va d'identification de cibles, d'opérations informationnelles pour affecter le moral du camp ennemi, l'interruption et la perturbation du système de communication ennemi pour perturber la coordination de ses forces, à l'organisation de cyber-opération en soutien de frappes cinétiques.

On est revenue sur la cristallisation du concept de protection au sein de l'écosystème humanitaire afin de mieux comprendre ce que le CICR souhaite signifier lorsqu'il évoque la nécessité de protéger les civils face aux menaces numériques. En premier lieu, tout comme les États établissent un processus de sécuritisation des menaces cybers, en formulant ces dernières en tant que menaces « existentielles » pour leur sécurité, le CICR a construit au fil du temps une véritable doctrine sur le type de cyberopération relevant d'une problématique de protection et étant par conséquent couverte par le DIH. On s'est donc appuyé dans les lignes qui suivent sur les analyses produites par les juristes travaillant pour le CICR afin de préciser la façon dont l'organisation formule les menaces numériques.

Le droit humanitaire ne s'applique en effet pas à toute cyberopération. Il semblerait tout d'abord que le CICR mette l'accent sur les répercussions physiques des attaques touchant l'espace numérique. Les cyberopérations peuvent impacter le fonctionnement d'infrastructures essentielles, comme les réseaux électriques ou les structures hospitalières. Elles peuvent paralyser les opérations humanitaires, via des attaques rendant inaccessibles leurs données, ou les ralentir, du fait de mesures de gestion de risque (notamment le retour

[1535] «the core of ICRC protection work consists in presenting allegations of IHL violations to the alleged perpetrators in the hop of stopping ongoing violation. » Ibid.

[1536] FORSYTHE, David P, "The ICRC: a unique humanitarian protagonist", *International review of the Red Cross*, Vol 89, number 865, March 2007, p.65-96

[1537] "Protecting civilians against digital threats during armed conflict, recommendations to states, belligerent, tech companies, and humanitarian organization, final report of the ICRC global advisory board on digital threats during armed conflicts", ICRC, October 2023 https://www.icrc.org/en/document/protecting-civilians-against-digital-threats-during-armed-conflict

au papier/crayon). Une cyber-opération peut paralyser totalement une organisation. Mais sans que cela résulte nécessairement d'un dommage physique affectant son système d'information. Enfin, des effets peuvent être immédiats, ou se révéler sur le long terme : « Par exemple, la suppression d'ensembles de données civiles essentielles peut entraîner des dommages civils persistants à long terme qui dépassent largement le moment où l'opération en question a été lancée, alors que les bombes peuvent causer des handicaps à vie. »[1538]

Comment alors le CICR envisage-t-il de mener ses activités de protection sur le terrain numérique ? En règle générale, c'est le DIH qui sert de cadre de référence aux activités de protection. Effectivement, le DIH stipule qu'un certain nombre d'entités (dont des civils, des hôpitaux, des ONG) ne peuvent être directement attaquées par les parties prenantes d'un conflit. Les cyber-opérations visant les civils lors de conflits sont donc en toute logique des atteintes au DIH et au nom de leur protection, le CICR plaide pour un plus grand respect de ses principes dans l'espace numérique. Or, le DIH a été conçu initialement pour les affrontements sur un champ de bataille physique et non virtuel. L'appliquer au cyberespace ne va pas de soi. Cela dit, l'organisation s'est penchée sur le sujet depuis déjà une bonne vingtaine d'années. Déjà en 2001, Knut Dörmann — ancien chef de la division juridique de l'organisation — avait alerté des possibles dommages causés par des cyber-opérations[1539]. Et il avait alors mis en avant la nécessité de réfléchir à la protection des non combattants dans le milieu numérique. Depuis, l'organisation n'a eu de cesse de réfléchir sur l'application du DIH à ce nouveau contexte. Elle a produit du droit souple (des manuels, des recommandations, etc.), tenté de peser sur le cadre normatif existant au sein des instances internationales régulant le cyberespace, comme l'Open-ended working group (OEWG)[1540]. Et elle a pris part à des discussions avec des experts ayant participé à la rédaction du manuel de Tallinn[1541]. Notre objectif n'est pas de rentrer dans le détail de ces échanges. Nous suivrons notre propre fil rouge, nous souhaitons simplement comprendre si cette vision de la protection des bénéficiaires et des civils dans le numérique inclut ou non la préservation de leur vie privée face aux cyberopérations.

---

[1538]« for example, the deletion of essential civilian datasets may bring about lingering long-term civilian harm that will vastly exceed the moment when the operation in question was launched, while bombs can cause lifelong disabilities. » Ibid.

[1539] https://www.icrc.org/en/doc/resources/documents/article/other/5p2alj.htm

DÖRMANN, Knut, "Applicability of the Additional Protocols to Computer Network Attacks, International Experts Conference on Computer Network Attack and the Applicability of International Humanitarian Law", ICRC, 2005, https://www.icrc.org/en/doc/assets/files/other/applicabilityofihltocna.pdf

DORMANN, Knut, "Computer network attack and international humanitarian law", *Cambridge Review of international affairs*, 19/05/2001

[1540] « Par sa résolution 73/27, l'Assemblée générale a créé un groupe de travail à composition non limitée (GTCNL), auquel tous les États membres de l'ONU sont invités à participer. Le groupe se réunira pour la première fois en 2019 et fera rapport à l'Assemblée générale en 2020. Le processus du GTCNL offre également la possibilité d'organiser des réunions consultatives intersessions avec l'industrie, les organisations non gouvernementales et le monde universitaire. » PYTLAK,Alison, « Joint civil society statement on cyber peace and human security UN General Assembly First Committee on Disarmament and International Security »08/10/2021 https://disarmament.unoda.org/open-ended-working-group/

[1541] En 2009, le centre d'excellence de cyberdéfense coopérative de l'Otan a mandaté un groupe d'expert internationaux pour mettre au point un corpus normatif applicable aux cyberconflits. Une première monture est publié en 2013, très vite critiqué pour son focus sur des cyber-opération les plus grave et donc son manque de réalisme; un deuxième manuel est publié en 2017, le Manuel de Tallinn 2.0. Comme le note François Delerue : « Cette première édition du Manuel de Tallinn se concentrait sur le droit applicable aux cyber opérations les plus graves, à savoir celles qui constituaient un recours à la force, une agression armée ou qui prenaient part à un conflit armé. Par conséquent, le Manuel de Tallinn 1.0 analysait principalement le droit international du recours à la force, aussi connu sur le nom de jus ad bellum ou de jus contra bellum, et le droit des conflits armés, aussi connu sous le nom de jus in bello. »
Un deuxième manuel est publié en 2017, le Manuel de Tallinn 2.0. qui prend aussi en compte les cyber-opérations menées par temps de paix. DELERUE, François, « Analyse du manuel de Tallinn 2.0 sur le droit international applicable aux cyber-opérations, étude prospective et stratégique », *CEIS*, novembre 2017 http://francoisdelerue.eu/wp-content/uploads/2020/01/20171129_NP_F-Delerue_Analyse-Manuel-Tallinn-2-0.pdf

Pour ce faire, on doit donc revenir sur la façon dont les juristes réfléchissent à l'application du DIH au cyberespace. Il semblerait qu'ils se soient heurtés à plusieurs difficultés. Tout d'abord, une partie des cyber-opérations ont lieu durant des périodes de paix, a priori hors du champ d'application du DIH (dont l'application est circonscrite aux conflits). Mais, une des caractéristiques des affrontements contemporains serait le brouillage de la frontière entre guerre et paix. Le témoignage de DPO du CICR reflète cette incertitude : « *Est-ce que l'attaque du CICR fait partie d'un cyberconflit ? C'est une possibilité, je ne suis même pas sûr que quelqu'un a une réponse, je pense que le CICR a été ciblé en raison du fait que ce soit un acteur à sa manière, je pense que c'est la position du CICR qui a été ciblée à sa manière. C'est un acteur neutre avec beaucoup de données intéressantes. Après le conflit entre la Russie et l'Ukraine n'a pas eu d'impact en matière d'augmentation de la cybermenace, mais l'a rendue plus tangible*. »[1542] Et la notion de « guerre hybride », caractérisée par des actions en-deçà du seuil de conflictualité, déborde le cadre du droit humanitaire[1543]. Le CICR ne reprend pas cette terminologie et s'en tient à définition des conflits cadrée par le DIH. Un bon nombre de commentateurs débattent sur la pertinence et le contexte de l'usage du terme de guerre hybride, mais d'un autre côté, les États dans leur majorité ne reconnaissent pas le fait qu'une cyberattaque isolée de haute intensité peut en elle-même être qualifiée d'agression armée[1544], et relever du DIH. Pour ce qui concerne les juristes du CICR comme Laurent Gisel, Tilman Rodenhauser, Knut Dormann, ils excluent l'usage du terme de guerre hybride, mais ils défendent le fait qu'une cyberopération isolée pourrait relever d'un conflit. Il n'y aurait simplement pas encore d'accord sur le degré d'intensité déclenchant l'ouverture d'hostilité via ce type d'arme numérique[1545].

Il est aussi nécessaire de préciser la façon dont le DIH protège les civils contre les différents actes de violence propre aux conflits armés sur le plan numérique. En d'autres termes, il s'agit de réfléchir à la façon dont le DIH envisage la protection des civils contre des attaques des parties prenantes. Cela suppose le fait de préciser la façon dont est défini une attaque sur le plan cinétique, puis cyber. Or, le DIH ne s'applique pas à l'ensemble des cyber-opérations

---

[1542] Entretien n° 93, OI2, DPO, ingénieur, 02/06/2023

[1543] « The international legal definition of armed conflict requires the exchange of armed fighting with the potential to inflict death or destruction. Some scholars take the alternative view that war or armed conflict are possible as a legal matter without kinetic impact. They argue that the use of malware against an opponent that creates injurious cyber effects alone is "cyberwar," "hybrid warfare," or just plain war. The argument fails to meet the definition of armed conflict under international law. »
O'CONNELL, Mary Ellen, "Data privacy rights: the same in war and peace", in :LUBIN, Asaf, BUCHAN, Russell (eds.),The rights to privacy and data protection in times of armed conflict, CCDOCOE, 2022, p.12-28

1544 Notons que la France est un des rares pays qui reconnait qu'une cyberopération peut en elle-même constituer un acte d'agression armé dans certains cas dans le cadre du Droit international : « La France réaffirme qu'une cyberattaque peut constituer une agression armée au sens de l'article 51 de la Charte des Nations unies, dès lors que ses effets et son ampleur atteignent une certaine gravité et sont comparables à ceux d'un emploi de la force physique. » Droit International appliqué aux opérations dans le cyberespace, Délégation à l'information et à la communication de la défense, ministère des Armées, 2019https://www.defense.gouv.fr/sites/default/files/ministere-armees/Droit%20international%20appliqu%C3%A9%20aux%20op%C3%A9rations%20dans%20le%20cyberespace.pdf

[1545]"Experts generally agree that cyber operations, on their own, have the potential to cross the threshold of an international armed conflict under IHL. The ICRC shares this view. The question of exactly where this threshold lies remains unsettled. In the ICRC's view, there is no reason to treat one or more cyber operations resulting in the destruction of civilian or military assets, or in the death or injury of soldiers or civilians, differently from equivalent attacks conducted through more traditional means and methods of warfare. "Les experts s'accordent généralement à dire que les cyber-opérations peuvent, à elles seules, franchir le seuil d'un conflit armé international au sens du droit international humanitaire. Le CICR partage ce point de vue. Selon le CICR, il n'y a aucune raison de traiter une ou plusieurs cyber-opérations entraînant la destruction de biens civils ou militaires, ou la mort ou la blessure de soldats ou de civils, différemment d'attaques équivalentes menées avec des moyens et des méthodes de guerre plus traditionnels. »
GISEL, Laurent, RODENHAUSER, Tilman, DORMANN, Knut, " Twenty years on : international humanitarian law and the protection of civilians against the effect of cyber operations during armed conflicts", *International Review of the red cross,* n°913, 2021

ayant lieu durant un conflit, mais seulement aux « cyberattaques ». Précisons ce point. Dans l'espace physique, le DIH couvre les attaques, qui sont définies comme suit dans l'article 49 du Protocole additionnel I aux Conventions de Genève (PA I) : « des actes de violence contre l'adversaire, que ces actes soient offensifs ou défensifs »[1546]. Cette définition semble très large, mais tout dépend de ce qui est entendu par le terme de « violence ». Il s'agit aussi de caractériser les dommages résultant d'une attaque. Ces derniers englobent selon le DIH : « non seulement le fait d'infliger la mort, des blessures ou la destruction de personnel et d'objets militaires, mais aussi, essentiellement, toute conséquence portant atteinte aux opérations militaires ou à la capacité militaire d'une partie à un conflit », tel que les actes de « sabotage et autres activités armées ou non armées restreignant ou perturbant les déploiements, la logistique et les communications », et « les actes de terrorisme. »[1547]

Comment appliquer cette définition d'une attaque au domaine numérique ? Tout d'abord, pour les experts du manuel de Tallinn, une cyber-attaque est une cyberopération dont on peut attendre raisonnablement qu'elle cause la mort de personnes ou les blesse, ou encore détruise ou endommage des objets (Règle 30 du Manuel de Tallinn 2.0). Il existe effectivement des cyber-opérations pouvant avoir des effets physiques : une attaque contre un » système de contrôle et d'acquisition de données en temps réel**»** (SCADA)[1548] contrôlant un réseau électrique peut entrainer un incendie. Une cyberattaque pourrait théoriquement tuer. L'exemple du « hacking » d'un stimulateur cardiaque est bien connu. Mais il est clair qu'une quantité négligeable de cyberopérations peuvent être qualifiées d'attaques si l'on se fonde sur cette définition. Cela en dit long sur la difficulté de maintenir une analogie entre les attaques cinétiques et numériques. Est-il possible d'élargir cette première définition ? Et si oui, comment ? Comment caractériser des opérations qui n'ont pas d'équivalents cinétiques ? Certains juristes considèrent qu'une opération rendant inopérant un ordinateur ou un réseau informatique peut être qualifiée de cyberattaque. Et dans ce cas, à partir de quel degré de dommage peut-on parler de cyberattaque ? Est-ce qu'une cyber-opération rendant inopérant un système informatique sans l'endommager physiquement est une cyber-attaque ? Une simple interruption temporaire due à une attaque par défacement est-elle une cyber-attaque ? Un désagrément ne peut être considéré comme une violence et être un signe d'attaque. Tout d'abord, comme l'a déclaré le CICR, le terme de désagrément « n'est pas utilisé dans le droit international humanitaire. » ;« Il semble donc gênant d'utiliser une terminologie inexistante pour déterminer la portée d'une obligation juridique. »[1549] D'ailleurs, l'effet d'une cyber-attaque sur la victime et sa perception subjective de la violence sont-ils pris en compte ? Ou bien la définition d'une cyber-attaque se concentre sur les répercussions d'une opération sur un système d'information ?

---

[1546] Article 49, Protocole Additionnel (I) à la Convention (IV) de Genève, 1977 https://ihl-databases.icrc.org/fr/ihl-treaties/api-1977/article-49

[1547] "should be interpreted as encompassing not only the infliction of death, injury, or destruction o[f] military personnel and objects, but essentially any consequence adversely affecting the military operations or military capacity of a party to a conflict", such as acts of ''sabotage and other armed or unarmed activities restricting or disturbing deployments, logistics and communications."
MELZER, Nils, "Interpretive guidance on the notion of Direct participation in hostilities Under international humanitarian law", ICRC, 2009https://casebook.icrc.org/case-study/icrc-interpretive-guidance-notion-direct-participation-hostilities

[1548] Il s'agit de l'ensemble des systèmes de télégestion qui permet de gérer et surveiller le fonctionnement de machines au sein d'industries.

[1549] First, it should be underlined that, as the ICRC stated, 'there is no definition of "inconvenience" and "this terminology is not used in IHL".It therefore seems troublesome to use non-existent terminology to determine the scope of a legal obligation"
"32nd international conference of the red cross and red crescent, International humanitarian law and the challenges of contemporary armed conflicts Report", October 2015

Pour les experts de Tallinn en faveur d'un élargissement de la définition d'une cyberattaque (soit une minorité), le fait de rendre inopérant un système d'information signifie qu'il faut remplacer physiquement un composant de ce dernier. Dans ce cas, une attaque par dénis de service n'est pas considérée comme une attaque. Selon d'autres interprétations, il faut simplement réinstaller l'OS (operating system) ou des données. Une attaque implique d'effectuer une action (au-delà du remplacement d'une composante physique) visant à restaurer un ordinateur ou un réseau informatique. Le CICR est en faveur de cette dernière définition. Pour l'organisation, on parle de cyber-attaque à partir du moment où un système informatique est rendu inopérant, qu'il soit rendu inutilisable du fait de sa destruction ou en raison d'autres facteurs. L'atteinte à la fonctionnalité d'un système informatique est un des critères principaux de sa définition. Le CICR motive sa position par deux arguments. Premièrement, selon la règle 8 du DIH coutumier, un objectif militaire peut être certes détruit, mais aussi capturé et neutralisé, sans être détruit ou endommagé physiquement [1550]. Deuxièmement, une cyber-opération sans impacts physiques directs sur le terrain peut avoir des répercussions indirectes lourdes pour les civils en raison d'une perte de fonctionnalité du système informatique (on peut penser aux conséquences de la paralysie complète d'un système de SI contrôlant un système d'irrigation, un hôpital, un réseau électrique, etc.) Et pour rappel, l'article 54 du DIH protège les objets indispensables à la survie de la population civile, comme les infrastructures agricoles, les réseaux électriques ou de distribution de l'eau[1551]. Et le CICR rappelle que « l'effacement ou l'altération de ces données pourrait rapidement paralyser les services gouvernementaux et les entreprises privées, et pourrait causer plus de dommages aux civils que la destruction d'objets physiques. »[1552] Notons qu'Internet n'est pas considéré comme bien essentiel selon le DIH et que si le sujet a fait l'objet de discussion, l'accès au réseau ne constitue pas un droit humain[1553].

Ajoutons que rentre en jeu un second critère de définition : le fait de considérer les données ou non comme des objets selon le DIH. Si on fait un rapide parallèle, l'objectif du RGPD est la protection de données personnelles. Quant au DIH, son objectif se formule également en matière de protection, toutefois s'il s'agit de protéger des données, les juristes cherchent à trouver comment recourir au DIH pour protéger non pas des données personnelles, mais des données de civils. Et considérer des données comme des « objets » permet de protéger des cibles même dans les cas où il n'y aurait pas de répercussions tangibles dans l'immédiat, comme des morts et des blessés (qui est un des critères de définition d'une attaque selon les experts du manuel de Tallinn).

---

[1550] DIH coutumier, chapitre 2. Règle 8. La définition des objectifs militaires https://ihl-databases.icrc.org/fr/customary-ihl/v1/rule8

[1551] il est ainsi interdit : « d'attaquer, de détruire, d'enlever ou de mettre hors d'usage des biens indispensables à la survie de la population civile, telle que les denrées alimentaires, les zones agricoles destinées à la production de denrées alimentaires, les récoltes, le bétail, les installations et réserves d'eau potable et les ouvrages d'irrigation, dans le but précis de les priver de leur valeur de subsistance pour la population civile ou pour la partie adverse, quel que soit le motif, qu'il s'agisse d'affamer les civils, de les faire fuir ou de les priver de tout autre motif » PI 1977 art 54 https://ihl-databases.icrc.org/fr/ihl-treaties/api-1977/article-54

[1552]"deleting or tampering with such data could quickly bring government services and private businesses to a complete standstill, and could cause more harm to civilians than the destruction of physical objects. The conclusion that this type of operation would not be prohibited by IHL in today's ever more cyber-reliant world – either because deleting or tampering with such data would not constitute an attack in the sense of IHL or because such data would not be seen as an object that would bring into operation the prohibition of attacks on civilian objects – seems difficult to reconcile with the object and purpose of this body of norms" 32nd international conference of the red cross and red crescent International humanitarian law and the challenges of contemporary armed conflicts, ICRC, December 2015

[1553] BASTIAN, Marie**,** «La fragmentation d'un droit préexistant ou la fondamentalité par analogie : le cas du droit d'accès à Internet», *La Revue des droits de l'homme* 15 | 2019, http://journals.openedition.org/revdh/5094

HUTCHINS, Todd, « Safeguarding civilian internet access during armed conflict : protecting humanity's most important resource in war », The Columbia science& technology law review, Vol XXII fall 2020

En effet, le statut d'objet conditionne la protection accordée à une cible et permet d'y appliquer les principes de précautions et de distinction (entre un objectif militaire et civil par exemple). Le terme d'objet est clarifié dans les protocoles additionnels des conventions de Genève et notamment son article 52, qui restreint la nature des objectifs militaires. Ces objectifs sont limités aux cibles contribuant à l'acquisition d'un avantage effectif lors d'une action militaire. L'article 47 explicite la définition d'un objet civil. Dans tous les cas, ces objets doivent être visibles, tangibles et physiques puisqu'ils correspondent à : « quelque chose placé devant les yeux, ou présenté à la vue ou à un autre sens, une chose individuelle vue ou perçue, une chose matérielle. »[1554] On peut donc considérer en tant que tels une maison, des écoles, des monuments historiques, des fermes, des systèmes d'irrigations, des barrages, des centrales nucléaires (destinées à l'électricité civile). Il faudrait alors de considérer des données en tant qu'objet civil, voire pour certaines interprétations, de bien civils essentiels. Mais un signal électronique est-il tangible et visible ?

Il n'existe pas de consensus sur ce point. Pour les rédacteurs du manuel de Tallinn, il est clair qu'une donnée est non matérielle et elle ne peut pas être considérée comme un objet. Mais cette position est remise en cause. Et ce en raison de plusieurs arguments. Tout d'abord, on peut considérer que les données sont avant tout matérielles (des lignes de codes peuvent être lues, modifiées). Ensuite, selon un autre point de vue, le terme d'objet ne doit pas être interprété comme étant synonyme de bien matériel, mais comme quelque chose pouvant être détruit, c'est ce que rappelle Kubo Macak au sujet du commentaire de l'article 52 du protocole additionnel des Conventions de Genève de 1977 : «Dans toute la partie en question du protocole, le terme "objet" est utilisé comme quelque chose susceptible d'être détruit, capturé ou neutralisé. Il importe donc peu que les données ne soient pas visibles ou tangibles comme l'est un pont. Ce qui importe, c'est que l'adversaire puisse s'en prendre aux deux, avec pour résultat que ce qui existait auparavant soit considérablement modifié ou complètement absent, c'est-à-dire endommagé ou détruit.»[1555]

Ajoutons que d'autres juristes donnent une réponse téléologique à cette question : la finalité du DIH étant de protéger les civils, ne pas traiter les données en tant qu'« objet » laisserait une faille de protection trop forte[1556]. Sur la base de ce raisonnement, si les données sont considérées comme des objets, alors on pourrait interpréter leur suppression ou manipulation comme étant une attaque. Cela signifierait en effet de porter atteinte à un objet. Et cela est valable même si une telle opération n'entraine pas de morts ou de blessés ou ne cause pas de

---

[1554] "something placed before the eyes, or presented to the sight or other sense, an individual thing seen, or perceived, or that may be seen or perceived; a material thing."PI 1977, commentaire 1987, art__52https://ihl-databases.icrc.org/fr/ihl-treaties/api-1977/article-52/commentary/1987

[1555] "Across the entire relevant section of the Protocol, the term "object" is used as something susceptible to destruction, capture or neutralization. It thus does not matter that data is not visible or tangible in the same way that a bridge is. What matters is that both may be attacked by the adversary with the result that what had been there before will be significantly altered or absent altogether: i.e., damaged or destroyed."
MACAK, Kubo, "This is Cyber: 1 +3 challenges for the application of international humanitarian law in Cyberspace", Exeter Centre for International Law, Working Paper Series, 2019/2 https://www.exeter.ac.uk/media/universityofexeter/collegeofsocialsciencesandinternationalstudies/lawimages/research/Macak_-_This_is_Cyber_ECIL_WP_2019-2.pdf

[1556] MAČÁK K., "Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law", *Israel Law Review*, 48(1), 2015, p.55-80. doi:10.1017/S0021223714000260
MAČÁK, K. "Unblurring the lines: military cyber operations and international law", *Journal of Cyber Policy*, *6*(3), 2021, p.411–428. https://doi.org/10.1080/23738871.2021.2014919

destruction directe d'un objet physique[1557]. Toutefois, une opération qui ne vise qu'à accéder à des données, sans les manipuler ou les supprimer, n'est pas une attaque. Mais, que signifie-t-on lorsqu'on parle de « manipuler » des données ? Ajouter des lignes de codes à un système informatique ? En modifier ? Toute cyber-opération n'implique-t-elle pas un minimum de manipulation de donnée ? Et donc toute cyber-opération est une cyber-attaque selon le DIH ? Une opération de cyber-espionnage est-elle considérée selon cette interprétation comme une attaque ?

En tout cas, les chercheurs Robin Geiss et Henning Lahmann considèrent qu' : « un acte militaire qui laisse les données intactes, telles que des opérations d'espionnage ou de surveillance qui ne visent que la confidentialité des données, n'est pas considéré comme une attaque aux yeux du DIH. » [1558] Ajoutons que si le CICR est clair sur le fait de ne pas prendre en compte les opérations de renseignement, comment ce choix est-il justifié, au-delà de la cohérence juridique vis-à-vis du DIH ?

Le CICR a donc adopté une conception large des cyber-attaques, mais il ne considère pas toutes les cyber-opérations comme telles. Les juristes du CICR, Laurent Gisel, Tilman Rodenhauser et Knut Dormann, sont clairs : même si les données sont considérées comme des « objets » selon le DIH, l'ensemble des opérations d'espionnage ne font pas considérés comme des cyberattaques, devant faire l'objet d'une protection spécifique. En effet, elles n'entrainent pas toujours des dommages physiques ni n'affectent nécessairement le fonctionnement d'un système informatique[1559], et elles n'entrainent pas nécessairement la destruction ou la manipulation de données.

Néanmoins, les activités de renseignement sont particulièrement difficiles à appréhender. Elles recoupent une multitude d'acteurs et de pratiques, qui englobent des activités plus larges que la collecte, l'analyse, la vérification et la dissémination d'informations actionnables par des acteurs étatiques. Elles peuvent inclure des opérations plus offensives de déstabilisation. Et pour ne rien faciliter, ces opérations sont marquées par une certaine forme de secret et de confidentialité, voire de clandestinité[1560]. Mais précisons que ces paragraphes se concentrent sur les opérations de cyberespionnage. Elles peuvent être décrites comme le fait d'accéder de façon non autorisée à des ordinateurs, des systèmes informatiques ou des réseaux, afin d'obtenir des informations. Le tout sans affecter la fonctionnalité du système accédé ni supprimer les données qu'il contient ou qui y transitent. Cette définition est très

---

[1557] JANCARKOVA, Tatana, MACAK, Kubo, "Scenario 12: cyber operations against computer data", International Cyber law in practice: interactive toolkit https://cyberlaw.ccdcoe.org/wiki/Scenario_12:_Cyber_operations_against_computer_data

[1558] "military conduct that leaves the data itself intact such as espionage or surveillance operations that are merely directed against the confidentiality of data would not count as an attack for the purpose of DIH."GEISS, Robin, LAHMANN, Henning, "Protection of data in armed conflict", *International law studies* n°97, 2021 https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2964&context=ils

[1559]" under the first approach, which considers data as objects under IHL, an operation designed or expected to delete or manipulate data would be an attack governed by all the relevant IHL rules because it would amount to destroying or damaging an object (the data). This would also be the case if such deletion or manipulation were not expected to cause death or injury to a person or to damage or disable a physical object an operation designed solely to access (possibly confidential) data without deleting or manipulating them – such as spying – would not be an attack." GISEL, Laurent, RODENHAUSER, Tilman, DORMANN, Knut, "Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts", *International review of the Red cross*, n°913, 2021

[1560] BROEDERS, Bennis, KAVANAGH, "Shades of grey : cyber intelligence and (inter)national security", *EU cyber d*irect, October 2023 https://eucyberdirect.eu/research/shades-of-grey-cyber-intelligence-and-inter-national-security

large, et le CICR reconnaît que « la distinction entre les attaques et les interférences dans les communications non constitutives d'une attaque est sans doute plus floue dans les cyberopérations que dans les opérations cinétiques ou électromagnétiques plus classiques. » et qu'« il est vrai qu'il pourrait être plus difficile pour celui qui fait l'objet de telles attaques de distinguer entre l'espionnage et les cyberattaques dans le cyberespace (par opposition aux opérations cinétiques), car la plupart des cyber-opérations reposent sur l'obtention de l'accès à un système informatique. Dès lors qu'il est obtenu, cet accès peut être utilisé pour recueillir des données (espionnage), manipuler ou détruire des données ou diriger le système de manière à causer des dommages à des biens physiques ou les détruire, soit directement, soit indirectement. »[1561]

Autre point, si le DIH couvre l'ensemble des opérations liées à un conflit, les liens entre cyberespionnage et guerre sont complexes. Elles sont menées par des acteurs aux objectifs et aux modes opératoires multiples, elles sont plus ou moins liées directement à des activités de combats cinétiques[1562]. Sachant que le DIH régit l'ensemble des moyens militaires mis en œuvre lors d'hostilités entre les parties prenantes, et que des opérations cyberespionnage, ces dernières peuvent se déployer en amont des affrontements armés, en phase préparatoire. La collecte de renseignement vise à anticiper l'action des autres acteurs du jeu géopolitique, elles peuvent ou non se dérouler dans l'espace numérique, et prendre la forme de cyberopérations ou non. Cela dit, pour le juriste Asaf Lubin, ancien analyste en renseignement militaire, l'ensemble de ces activités de collecte de renseignement sont couvertes par le DIH.

Par conséquent, elles devraient selon lui respecter toute une série de principe du DIH, dont l'article 57 stipulant la nécessité de respecter le principe de précaution qui enjoint de distinguer les cibles militaires des cibles civiles. Pour le juriste, il concerne donc l'ensemble de « la collecte de renseignements, sous quelque forme que ce soit et par quelque acteur que ce soit (entrepreneurs privés, agences civiles de renseignement), ainsi que d'autres activités plus larges de collecte et de gestion de données devraient déclencher l'application de l'obligation, pour autant que les informations en question soient collectées, stockées, traitées ou diffusées dans le but général de faire progresser le combat. »

Le juriste précise toutefois qu'« il est vrai que l'évaluation de la question de savoir si l'activité informationnelle en question est suffisamment liée dans l'espace, le temps et la relation aux objectifs de l'avancement du combat militaire sera sujette à une certaine discrétion. » [1563]

---

[1561] CICR, « Le droit international humanitaire et les défis posés par les conflits armés contemporains », XXXIIème Conférence internationale de la croix-rouge et du croissant rouge, 8-10 décembre 2015 https://rcrcconference.org/app/uploads/2015/10/32IC-Report-on-IHL-and-the-challenges-of-contemporary-armed-conflicts_FR.pdf

[1562]Pour rappel, si l'on s'en tient au DIH, un conflit est défini comme tel, selon l'article 2 de la Convention de Genève : » En dehors des dispositions qui doivent entrer en vigueur dès le temps de paix, la présente Convention s'appliquera en cas de guerre déclarée ou de tout autre conflit armé surgissant entre deux ou plusieurs des Hautes Parties contractantes, même si l'état de guerre n'est pas reconnu par l'une d'elles. / La Convention s'appliquera également dans tous les cas d'occupation de tout ou partie du territoire d'une Haute Partie contractante, même si cette occupation ne rencontre aucune résistance militaire. […]

[1563] « intelligence collection, in any of its forms and conducted by any actor (private contractors, civilian intelligence agencies), as well as other broader data collection and management activities should trigger the application of the duty, so long as the information in question is collected, stored, processed, or disseminated with the general purpose of advancing combat. »
"It is true that evaluating whether the informational activity in question is sufficiently connected in space, time, and relationship with the goals of advancing military combat will be subject to some discretion."
LUBIN, Asaf "The duty of constant care and data protection in war", DICKINSON, Laura, BERG, Edward (eds.), Big data and armed conflict : legal issue above and below the armed conflict threshold, Oxford University press, 2023

De surcroit, un bon nombre de cyberopérations liées à des pratiques d'espionnage se déroulent au cœur des guerres, comme on a pu le voir précédemment. Elles sont menées directement par les parties belligérantes à des fins stratégiques, afin d'appuyer des manœuvres militaires. Sachant que toute opération de cyberespionage n'est pas nécessairement menée par des États, ou par des services de renseignements étatiques. Il faut savoir que le DIH s'applique aussi aux situations de conflits intraétatiques. Des groupes armés non étatiques peuvent très bien conduire de telles opérations. C'est le cas au Yémen, dans ce cas un groupe armé partie prenante d'un conflit cible des humanitaires, la difficulté étant que leurs intentionnalités n'ont pas été objectivées de façon claire. Contrairement au cas syrien, où des plans des informations directement relatives au conflit ont été capturés. C'est également le cas dans le cadre du conflit israélo-palestinien : le Hamas a piloté des opérations de renseignement cyber[1564]. Cette « démocratisation » du cyberespionnage est facilitée par la plus grande disponibilité des outils offensifs en ligne, abaissant le cout de ce type d'opération[1565]. Un outil de spyware comme Pegasus a pu être utilisé en cours de conflits, notamment en Azerbaïdjan, en 2020, lors de l'affrontement avec l'Arménie au sujet du Haut-Karabakh[1566]. Cela dit, l'objectif des usagers de Pegasus n'était pas directement lié à des manœuvres militaires. Les différents rapports ne précisent pas l'intentionnalité et la nature des auteurs, mais les cibles étaient alors différentes personnalités de la société civile dénonçant les crimes de guerre menés par les forces azerbaïdjanaises (reporters, défenseurs des droits humains), et publics. Le téléphone de la porte-parole du ministre des Affaires étrangères d'Arménie a été ciblé. Cette dernière était impliquée dans des négociations liées à la crise et les médiations en vue d'un cessez-le-feu. Enfin, certaines opérations d'intrusion non autorisées dans des systèmes informatiques n'ont pas comme seule finalité le renseignement et peuvent se doubler de fuite de données ayant pour objectif l'intimidation des parties adverses. Le CyberPeace Institute a documenté de telles attaques au cours du conflit ukrainien[1567]. De tels exemples de collecte et de fuite de données n'ont pas (à notre connaissance) touché des ONG humanitaires, mais ce scénario reste de l'ordre du possible au regard des cas décrits précédemment. Ces exemples qu'ils soient ou non directement liés à des manœuvres militaires sont en tout cas suffisamment parlants pour surligner l'importance de protéger les données des civils et des bénéficiaires d'ONG en contexte de conflits armés.

Et donc pour reprendre le fil de notre propos, il convient de noter que le DIH ne proscrit pas les activités de renseignement en ligne ou hors ligne. Les espions ne bénéficient simplement pas du même statut et des mêmes protections que les combattants. Ils n'ont pas le droit au statut de prisonnier de guerre, mais doivent bénéficier selon le DIH d'un procès équitable

---

[1564] AridViper, an intrusion set allegedly associated with Hamas, Sekoia, 26/10/2023 https://blog.sekoia.io/aridviper-an-intrusion-set-allegedly-associated-with-hamas/

[1565] WIRTSCHAFTER, Valerie, "The implications of the AI boom for nonstate armed actors", Brookings, 16/01/2024https://www.brookings.edu/articles/the-implications-of-the-ai-boom-for-nonstate-armed-actors/

[1566]KRAPIVA, Natalia, COPPI, Giulio, RAND, "Hacking in a war zone : Pegasus spyware in the Azerbaijan-Armenia conflict", 25/05/2023, Access Now, https://www.accessnow.org/publication/armenia-spyware-victims-pegasus-hacking-in-war/
Amnesty International, "Armenia/Azerbaijan: Pegasus spyware targeted armenian public figures amid conflict", 25/05/2023 https://www.amnesty.org/en/latest/news/2023/05/armenia-azerbaijan-pegasus-spyware-targeted-armenian-public-figures-amid-conflict/
L'Arménie est aussi accusée d'avoir utilisé un logiciel espion, Cytrox.

[1567] https://cyberpeaceinstitute.org/wp-content/uploads/2023/09/Ukraine-Report-Q2_4.09.pdf
Data weaponisation attacks aim to steal/exfiltrate or acquire data for espionage, surveillance, or intelligence purposes. This includes hack and leak attacks through the theft and leak of data for political or ideological purposes. The leak of data and information from institutions and organisations sows distrust, demonstrates an inability to secure sensitive data, and potentially places individuals at risk.

selon le droit national[1568]. Le DIH établit également une différence entre les activités de collecte de renseignements militaires, sous son propre uniforme, des actions plus clandestines (quand bien même la frontière entre ces deux familles de renseignement peut être labile[1569].) L'article 29 de la convention de La Haye[1570] définit comme suit l'espionnage : « Une personne ne peut être considérée comme espionne que lorsque, agissant clandestinement ou sous de faux prétextes, elle obtient ou tente d'obtenir des informations dans la zone d'opérations d'un belligérant, avec l'intention de les communiquer à la partie hostile. » [1571] L'article 24 de la même Convention est clair : « les ruses de guerre et l'emploi des moyens nécessaires pour se procurer des renseignements sur l'ennemi et sur le terrain sont considérés comme licites. »[1572] [1573] Seule est prohibée la perfidie comme le stipule l'article 37 du protocole additionnel aux Conventions de Genève de 1977[1574]. Le tout est de pouvoir faire la nuance entre la ruse et la perfidie dans le cyberespace. Comment qualifier les opérations cyber nécessitant de s'introduire dans des systèmes informatiques en trompant l'utilisateur grâce à l'usage d'emblèmes d'objets protégés (l'emblème de la Croix-Rouge par exemple) [1575] ? Sachant que pour être qualifié de perfide, un acte doit remplir plusieurs critères selon le DIH : il doit constituer un abus confiance intentionnel, il doit laisser croire qu'un acteur bénéficie d'une protection particulière selon le DIH, par exemple en usant d'un emblème d'un acteur protégé (dont une ONG humanitaire), l'attaque doit aussi causer des blessures ou la mort de la cible ou à la capture de l'adversaire[1576]. Nuance supplémentaire, utiliser à d'autres finalités un emblème d'un objet protégé (par exemple l'emblème du CICR) reste proscrit par le DIH, y

---

[1568] Règle 107, droit international humanitaire coutumier https://ihl-databases.icrc.org/en/customary-ihl/v1/rule107

[1569] « Espion, espionnage », Dictionnaire pratique de droit humanitaire, MSF https://dictionnaire-droit-humanitaire.org/content/article/2/espion-espionnage/

POZNANSKY, Michael, "Covert action, espionage and the intelligence contest in cyberspace", *War on the Rocks*, 23/03/2021https://warontherocks.com/2021/03/covert-action-espionage-and-the-intelligence-contest-in-cyberspace/

[1570] Conventions adoptées durant les conférences de la Haye en 1899 et 1907. Elles constituent le corps du DIH consacré à la conduite des belligérants durant les hostilités. Il peut être qualifié de « droit de la violence », par opposition a « droit de l'assistance », formalisé par les conventions de Genève, votées dans l'après Seconde Guerre Mondiale, qui organise et formalise les secours en temps de conflit. https://dictionnaire-droit-humanitaire.org/content/article/2/conventions-de-la-haye/

[1571] « A person can only be considered a spy when, acting clandestinely or on false pretenses, he obtains or endeavors to obtain information in the zone of operations of a belligerent, with the intention of communicating it to the hostile party. » Convention (IV) respecting the Laws and Customs of War, Regulations: Art.29https://ihl-databases.icrc.org/en/ihl-treaties/hague-conv-iv-1907/regulations-art-29

[1572] ruses of war and the employment of measures necessary for obtaining information about the enemy and the country are considered permissible, PI1977, art 37
https://ihl-databases.icrc.org/fr/ihl-treaties/api-1977/article-37?activeTab=1949GCs-APs-and-commentaries

[1573] Protocol additional to the Geneva Convention of 12 August 1949, article 46, Spies
https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-46

[1574]Article 37, Convention de la Haye : « Les ruses de guerre ne sont pas interdites. Constituent des ruses de guerre les actes qui ont pour but d'induire un adversaire en erreur ou de lui faire commettre des imprudences, mais qui n'enfreignent aucune règle du droit international applicable dans les conflits armés et qui, ne faisant pas appel à la bonne foi de l'adversaire en ce qui concerne la protection prévue par ce droit, ne sont pas perfides. Les actes suivants sont des exemples de ruses de guerre : l'usage de camouflages, de leurres, d'opérations simulées et de faux renseignements. »

GEORGELIN, Estéban, HOLEINDRE, Jean-Vincent, « Des ruses de guerre numériques ? Le *hacking* comme ressource stratégique dans les conflits contemporains », *Quaderni*, 103 | Printemps 2021, http://journals.openedition.org/quaderni/2020 ; DOI : https://doi.org/10.4000/quaderni.2020

[1575] BILLER, Jeffrey, "The Misuse of Protected Indicators in Cyberspace: Defending a Core Aspect of International Humanitarian Law", in, ROIGAS, H, JACKCHIS, R, LINDSTROM, L, MINARIK, T. (eds) : *2017 9th International Conference on Cyber Conflict Defending the Core*,NATO CCD COE Publications, Tallinn, 2017

[1576] L'opération doit se rapporter à une protection dont bénéficie une personne, un objet ou une activité particulière, qui est spécifiquement prévue par le DIH (c'est-à-dire que la protection accordée sur la base de considérations morales ou de normes d'autres corpus juridiques n'est pas suffisante), l'opération doit inviter l'adversaire à croire qu'il a droit à la protection du DIH ou qu'il doit l'accorder ; l'auteur doit intentionnellement trahir la confiance de l'adversaire ; l'acte doit avoir pour effet prohibé de tuer ou de blesser l'adversaire (ou de le capturer, pour les partisans du point de vue plus large exposé ci-dessus). Les opérations cybernétiques, dont l'effet se produit uniquement dans le cyberespace ou se limite à endommager ou à détruire des biens matériels, ne sont pas couvertes par l'interdiction.
"Perfidy and ruses of war, International Cyber law in practice Cyberlaw " Cyberlaw Toolkit, 07/08/2021
https://cyberlaw.ccdcoe.org/wiki/Perfidy_and_ruses_of_war#cite_note-5

compris sur le terrain numérique. Cela rend donc toute cyberopération utilisant l'emblème du CICR pour « hameçonner » l'internaute illégale. Mais il existe un certain nombre d'ambiguïtés. Par exemple, les experts de Tallinn ne s'accordent pas sur le fait que passer pour un délégué du CICR ou se référer au nom de domaine « icrc.org » constitue ou non un mésusage de l'emblème[1577].

Plus généralement, la position des experts du manuel de Tallinn est à gros traits en accord avec les différents points évoqués sur le renseignement en temps de conflit. Cette position est valable pour l'ensemble des données : « La majorité du groupe international d'experts a estimé que la nature des informations recueillies n'a pas d'incidence sur la qualification de l'activité en tant que cyber-espionnage dès lors qu'elles sont recueillies pour le compte d'une partie au conflit. »[1578] Une minorité d'experts aurait été pour restreindre ce type d'opération aux données militaires et en exclure les données de « civils ». Cette proposition n'a pas été retenue. Cela dit, le CICR reconnait qu'il existe une faille de protection concernant les activités de surveillance vis-à-vis des civils : « Des niveaux sans précédent de surveillance de la population civile ont suscité l'inquiétude et un nombre croissant d'arrestations, parfois fondées sur la désinformation. La désinformation et la surveillance ne sont pas des phénomènes uniques ou nouveaux dans les conflits armés ; toutefois, la plus grande portée et l'effet multiplicateur de la technologie numérique peuvent exacerber — et ajouter — aux vulnérabilités existantes des personnes touchées par les conflits armés. (…) Le droit international humanitaire n'interdit pas nécessairement ces activités, mais il interdit les actes de menace de violence dont le but premier est de répandre la terreur parmi la population civile. » [1579] Le terme de « terreur » est cependant très fort et peut être tout à fait légitimé (en cas d'arrestations liées à des cas de surveillance), mais il laisse de côté toute une série d'émotions pouvant être liées à une atteinte à la vie privée.

Toujours est-il que concernant les ONG humanitaires et leurs bénéficiaires, il semblerait que selon les différentes interprétations existantes, que ce soit par les experts de Tallinn ou du CICR, les protections spécifiques accordées par le DIH aux humanitaires sont en partie transposables au terrain numérique. Tout d'abord, les différentes conventions de Genève imposent le fait que la délivrance de soin ne doit pas être entravée, et que la continuité médicale ne doit pas être interrompue. Les opérations humanitaires et le personnel humanitaire doivent être respectés et protégés (article 71 PI 1977). Ces protections sont applicables dans l'environnement numérique. Originellement, le brouillage des

[1577] "Misuse of any of the ICRC's symbols or their imitations in the physical space is expressly prohibited by IHL.[53] However, it is less clear whether this prohibition extends to cyber operations that falsely convey their origin as coming from or being affiliated with the ICRC, or that simulate, portray or graphically represent the ICRC's symbols in the digital space" "Perfidy and ruses of war", International Cyber law in practice Cyberlaw 07/08/2021
https://cyberlaw.ccdcoe.org/wiki/Perfidy_and_ruses_of_war#cite_note-5
Tallinn Manual 2.0, rule 124, commentary paras 5–7.

[1578] "The majority of the International Group of Experts took the position that the nature of the information gathered has no bearing on the characterisation of the activity as cyber espionage so long as it is gathered on behalf of a party to the conflict." Tallinn Manual 2.0, Rules 89

[1579]« Unprecedented levels of surveillance of the civilian population have caused anxiety and increasing numbers of arrests, in some instances possibly based on disinformation. Disinformation and surveillance are not unique or new to armed conflicts; however, the greater scope and force-multiplying effect provided by digital technology can exacerbate—and add to– –the existing vulnerabilities of persons affected by armed conflicts. (…) IHL does not necessarily prohibit such activities, but it does prohibit acts of threats to violence the primary purpose of which is to spread terror among the civilian population. « ICRC, "International humanitarian law and the challenges of contemporary armed conflicts",33rd international conference of the red cross and red crescent https://rcrcconference.org/app/uploads/2019/10/33IC-IHL-Challenges-report_EN.pdf?fbclid=IwAR3ksX7qBnQd61yJFgKqYlAhRKF3VPh9sFFhIZaQB2hNzxqAhksEjJJ83HM%3E

communications est permis selon le DIH, sauf lorsqu'il s'agit d'unités de soins, afin de ne pas perturber le travail du personnel médical. La suppression ou l'altération de données médicales est ainsi proscrite. Mais à vrai dire, à quoi bon protéger spécifiquement les données si les biens civils et les ONG humanitaires sont déjà en DIH considérés comme des objets protégées ? S'agirait-il d'une forme de protection redondante ? Mais que faire si les opérations de cyberrenseignements ne sont pas proscrites ? Les civils ou les bénéficiaires sont-ils protégés contre des activités de renseignements ? Est-ce que ce sujet relèverait du DIH ? En quoi est-ce problématique ? S'agit-il à d'autres droits de couvrir ce sujet ?

L'article 16 du protocole additionnel (I) de 1977 à la Convention de Genève impose le respect du secret médical[1580]. Cela dit, les ONG comprennent aussi des personnels non soignants, et l'article 16 ne couvre pas l'ensemble des traitements de données d'une ONG. Et surtout, il existe peu de littérature sur la prohibition d'accès à des données d'ONG humanitaires, hors données médicales. Mais la professeur de droit international Hellen O'Marry plaide pour l'extension de l'article 16 à un ensemble plus vaste de données personnelles[1581]. Dans un rare passage sur ce sujet, des juristes du CICR, Tilman Rodenhauser, Balthasar Stahelin et le DPO Massimo Marelli défendent l'argument qu'une atteinte à la confidentialité de données d'ONG irait à l'encontre du respect dû aux humanitaires selon le DIH : « Les parties qui envisagent de violer des données humanitaires — sans les endommager — doivent tenir compte du fait que leur comportement risque de saper la confiance dans les organisations humanitaires impartiales et, selon les circonstances, de mettre le personnel humanitaire en danger. Ce risque est particulièrement élevé si les données humanitaires sont extraites dans le but de cibler des adversaires ou des civils. Et même la violation de données humanitaires sans les endommager ou les utiliser à mauvais escient peut être difficile à concilier avec la lettre et l'esprit du droit international humanitaire. Par exemple, l'espionnage d'organisations humanitaires impartiales compromettrait la confidentialité des informations. Cela remettrait en cause une modalité de travail essentielle pour le CICR qui est explicitement reconnue par le DIH en ce qui concerne les visites de détention (article 126 de la CG III et 143 de la CG IV). » [1582]L'argument principal est double : ne pas mettre en danger des humanitaires, ce

---

[1580] Art 16, Convention de Genève, Protocole additionnel (I), 1977 : **«** Les personnes exerçant une activité de caractère médical ne peuvent être contraintes d'accomplir des actes ou d'effectuer des travaux contraires à la déontologie ou aux autres règles médicales qui protègent les blessés et les malades, ou aux dispositions des Conventions ou du présent Protocole, ni de s'abstenir d'accomplir des actes exigés par ces règles et dispositions. 3. Aucune personne exerçant une activité médicale ne doit être contrainte de donner à quiconque appartenant soit à une Partie adverse, soit à la même Partie qu'elle, sauf dans les cas prévus par la loi de cette dernière, des renseignements concernant les blessés et les malades qu'elle soigne ou qu'elle a soignés si elle estime que de tels renseignements peuvent porter préjudice à ceux-ci ou à leur famille. Les règlements régissant la notification obligatoire des maladies transmissibles doivent, néanmoins, être respectés »
https://ihl-databases.icrc.org/fr/ihl-treaties/api-1977/article-16?activeTab=1949GCs-APs-and-commentaries
MACAK, Kubo, RODENHAUSER, Tilman, GISEL, Laurent, "Cyber-attacks against hospital and the Covid 19 pandemic : how strong are international law protections?, *Humanitarian law &Policy, ICRC*, 02/04/2020 https://blogs.icrc.org/law-and-policy/2020/04/02/cyber-attacks-hospitals-covid-19/
RODENHAUSER, Tilman, MACAK, Kubo, "Scenario 20: Cyber operations against medical facilities", International cyber law in practice : interactive toolkit
https://cyberlaw.ccdcoe.org/wiki/Scenario_20:_Cyber_operations_against_medical_facilities

[1581] O'CONNELL, Mary Ellen, "Data privacy rights: the same in War and Peace", in BUCHAN, Russell, LUBIN, Asaf ( eds.), *The rights to privacy and data protection in armed conflict*, CCDOCOE, 2022,p.12-29

[1582] »parties that contemplate breaching humanitarian data – without damaging it – should consider that their conduct risks undermining trust in the impartial humanitarian organizations and, depending on the circumstances, put humanitarian staff in danger. This risk is particularly acute if humanitarian data is extracted with a view to targeting adversaries or civilians (see here). And even breaching humanitarian data without damaging or misusing it may be difficult to reconcile with the letter and spirit of IHL. For instance, spying on impartial humanitarian organizations would compromise the confidentiality of information, a key working modality for the ICRC that is explicitly recognized under IHL with regard to detention visits (article 126 GC III and 143 GC IV). Moreover, if States mandate an impartial

qui serait comme le fait remarquer Tilman Rodenhäuser une atteinte à l'article 31 du DIH coutumier[1583], et assurer la continuité de l'aide en conservant la confiance dans l'organisation qui serait altérée en cas de fuite de données. Cette posture est réaffirmée dans le rapport publié en octobre 2023 sur l'impact de menaces numériques sur les civil dans les conflits et regroupant une série de recommandation adressées aux Etats et aux acteurs prenant parties aux conflits[1584].

Enfin, en anticipation de la 34e conférence du mouvement de la croix rouge devant avoir lieu en octobre 2024 a été publié une proposition de résolution portant sur la protection des civils et des « objets protégés » (hôpitaux et ONG) contre les attaques cyber et informationnelles durant les conflits. On peut y lire que les rédacteurs de la résolution sont « préoccupés par l'impact que les cyber-opérations, y compris les violations de données, et les opérations d'information conçues pour interférer avec le travail des organisations humanitaires ou le compromettre, risquent d'avoir sur ces organisations et leur personnel, affectant la fourniture de services humanitaires aux personnes qu'elles servent. »[1585] Il n'est pas précisé ce qui est entendu par « violation de donnée », mais ce terme est usuellement utilisé pour décrire un « incident de cybersécurité au cours duquel des informations (…) sont consultées, vues, volées, modifiées ou utilisées par une personne ou entité non autorisée. »[1586] Le document ne revient pas sur le débat concernant le spectre d'application du DIH, mais fait référence à la nécessité de respecter les principes de la protection des données face aux cyberopérations. Cette interprétation est confortée par le fait qu'en toute fin de document on peut lire qu'est enjoint : « instamment aux États et au Mouvement de coopérer pour veiller à ce que les données à caractère personnel ne soient pas demandées ou utilisées à des fins incompatibles avec la nature humanitaire de l'action du Mouvement ou d'une manière qui porterait atteinte à la confiance des personnes qu'il sert ou à l'indépendance, à l'impartialité et à la neutralité des opérations du Mouvement. »[1587] Il reste à voir comment cette posture peut se frayer un chemin, si elle sera contestée ou non, portée au sein de quelles arènes. D'autres ONG –

humanitarian organization like the ICRC to perform services such as the tracing of missing people, these services must be facilitated and not undermined (article 81 API).RODENHAUSER, Tilman, STAEHELIN, Balthasar, MARELLI, Massimo, "Safeguarding humanitarian organizations from digital threats", *Humanitarian law &Policy, ICRC*, 13/10/2022 https://blogs.icrc.org/law-and-policy/2022/10/13/safeguarding-humanitarian-organizations-from-digital-threats/?utm_source=clipboard&utm_medium=text&utm_campaign=The+Homeanitarian_17+Oct_Week+42

[1583]https://ihl-databases.icrc.org/en/customary-ihl/v1/rule31

" if cyber operations undermine the trust in humanitarian organizations and thereby put humanitarian staff into danger, such operations would violate the obligation of all parties to respect and protect humanitarian relief personnel (Rule 31 of the ICRC's Customary IHL Study)." si les cyber-opérations sapent la confiance dans les organisations humanitaires et mettent ainsi le personnel humanitaire en danger, ces opérations violeraient l'obligation de toutes les parties de respecter et de protéger le personnel de secours humanitaire (règle 31 de l'étude sur le droit international humanitaire coutumier du CICR) ».
RODENHAUSER, Tilman, "Hacking humanitarian ? IHL and the protection of humanitarian organizations against cyber operations", *Ejilttalk*, 16/03/2020 https://www.ejiltalk.org/hacking-humanitarians-ihl-and-the-protection-of-humanitarian-organizations-against-cyber-operations/

[1584] protecting civilians against digital threats during armed conflict recommendations to states, belligerents, tech companies, and humanitarian organizations final report of the icrc global advisory board on digital threats during armed conflict

[1585]"deep concern about the impact that cyber operations, including data breaches, and information operations designed to interfere with or undermine the work of humanitarian organizations risk having on these organizations and their personnel, affecting the delivery of humanitarian services to the people they serve." Protecting civilians and other protected persons and objects against cyber and information operations during armed conflict", Draft Zero resolution, April 2024 34IC/24/XX / DRX.X https://rcrcconference.org/app/uploads/2024/04/34IC-Draft-0-Cyber-EN.pdf

[1586] https://www.proofpoint.com/fr/threat-reference/data-breach

[1587] « urges States and the Movement to cooperate to ensure that personal data is not requested or used for purposes incompatible with the humanitarian nature of the work of the Movement or in a manner that would undermine the trust of the people it serves or the independence, impartiality and neutrality of the Movement's operations." Protecting civilians and other protected persons and objects against cyber and information operations during armed conflict", Draft Zero resolution, April 2024 34IC/24/XX / DRX.X https://rcrcconference.org/app/uploads/2024/04/34IC-Draft-0-Cyber-EN.pdf

proches du milieu de la défense des droits en ligne cherche à défendre une autre conception de la protection des civils dans l'espace numérique.

Et donc on a vu que le DIH offre un cadre protecteur pour les civils face aux cyber-attaques. Il s'agit certes d'un cadre partiel, n'englobant pas certaines cyber-opérations. L'objectif est de se prémunir de dommages physiques et d'interruption de la fonctionnalité d'un système informatique ou de l'arrêt de l'allocation de l'aide. Seules les données de santé restent explicitement protégées par le secret médical. Mais certains juristes plaident pour une extension de cette protection aux ONG non médicales, ceci non pas au nom de la protection de la vie privée, mais de la nécessité de la continuité de l'aide. Parallèlement, la nécessité de mieux protéger les données des civils, avec une ouverture vers la prise en compte d'opérations qui n'étaient pas jusqu'alors considérées comme des cyberataques, et qui restaient à l'écart des débats sur l'application du DIH, à savoir des violations de données.

§ 3 - Droits de l'homme, vie privée et conflictualité numérique

Hors du CICR, des juristes invitent à choisir un autre cadre juridique que le DIH et revenir au droit de la protection des données. Il est aussi possible de défendre l'application des droits de l'homme durant des conflits, ou bien étendre les règles du DIH existantes afin de couvrir de nouveaux objets de protection. À vrai dire, il existe de multiples avis sur le choix du cadre le plus approprié, mais l'idéal selon le juriste Asaf Lubin serait d'adopter une combinaison de différents corpus juridiques[1588], en fonction du contexte et du type de cyberopération.

Première option, Robin Geiss et Henning Lahman proposent de s'inspirer du droit à la protection des données pour encadrer les cyberopérations lors de conflits[1589]. Cette approche est délicate : certains juristes estiment que le RGPD ne peut s'appliquer dans de tels contextes. En effet, l'article 2 du règlement comprend une exemption concernant les traitements relatifs par les « autorités compétentes » ( et donc les Etats) à la sécurité nationale, à l'ordre public et à la recherche des infractions pénales. Pour être claire, les ONG sont toujours tenues d'appliquer le Règlement, mais tout un ensemble de traitement de données par les entités rattachées aux Etats (administrations, collectivités, ministères, etc.) échappent au RGPD dans un contexte d'affrontement armé. Cela dit, pour Peter Geiss et Henning Lahman, il est essentiel de trouver un cadre inspiré du droit à la protection des données pouvant s'appliquer aux affrontements armés. Ils évoquent la nécessité d'établir un « changement de paradigme », et de sortir du débat sur le DIH et revenir au droit à la protection des données. L'enjeu n'est pas de s'assurer de la fonctionnalité d'un réseau informatique ou des dommages physiques, mais d'assurer la protection des données de contenu. Ils se réfèrent au RGPD et envisagent de s'appuyer sur sa définition des « données sensibles » pour assurer la protection d'informations civiles en contexte de conflit armé face

[1588] LUBIN, Asaf, BUCHAN, Russell (ed.),*The rights to privacy and data protection in times of armed conflict*, CCDOCOE, 2022, 318 p.

[1589]« In light of this, it is submitted that these inherent limitations call for a prospective discussion that transcends the purely ontological inquiries revolving around the object-quality of computer data that have dominated the discourse so far. Given the significance of data for modern digitalized societies, one might propose a paradigm shift: To date, as was shown, the prevalent debate has taken the rules and principles of existing IHL (in particular the notions of "object" and "attack") and applied them to "data." A different and novel approach would be to take, as a starting point, the principles of existing data protection, data security, and other pertinent legal frameworks and attempt to apply them to contemporary armed conflict. Such an approach might be better suited to accommodate the actual relevance of data for the information society and to address the resultant protection needs during armed conflict. »
GEISS, Robin, LAHMANN, Henning, "Protection of data in armed conflict", *International law studies*, vol 97, 2021

aux attaques des parties prenantes du conflits, des Etats. Notons que cette proposition met de côté les autres types de données personnelles. Deuxièmement, les chercheurs n'appellent pas à l'interdiction de l'intégralité des cyberopérations d'espionnage, ce qui serait selon eux inconcevable. Mais ils évoquent, très brièvement, la nécessité de mieux les encadrer. Les cyberopérations d'espionnage devraient être couvertes par « une règle interdisant certaines utilisations spécifiques des données collectées, telles que la publication ou la fuite de données personnelles sensibles, et/ou une règle interdisant l'exploitation de ces ensembles de données à des fins de coercition, d'extorsion ou de manipulation. » [1590]

Ensuite, il existe une deuxième option : s'appuyer sur les droits de l'homme. Et effectivement, un certain nombre d'acteurs défendent la nécessité d'inclure la protection des droits humains dans les politiques de cybersécurité. Cette position est propre à la « société civile », et différents activistes et universitaires regrettent que cette approche resterait minoritaire au sein des Etats, reliant tendanciellement la cybersécurité à des enjeux régaliens de défense[1591]. L'approche « droit de l'hommiste » de la cybersécurité serait surtout portée par des ONG comme Amnesty International, Access Now[1592], Centre for internet and Society, ICT4Peace Foundation, l'association for progressive communication (APC)[1593], le Cyberpeace Institute[1594] ,etc.[1595] Ainsi, Pavlina Pavlova — Public Policy Advisor au Cyberpeace institute — déclare ainsi que les « Les droits de l'homme sont abordés dans ce cadre, mais la conception dominante de ce qui constitue la cybersécurité reste fortement axée sur le niveau de l'État souverain — son territoire et son infrastructure — plutôt que sur l'individu. Ce phénomène peut être compris, du point de vue des relations internationales, comme une approche realpolitik de la gouvernance, qui privilégie les intérêts de l'État, et une approche militaro-centrée de la question. »[1596] Le souhait de se distancier du récit régalien est clairement exprimé : « Les discussions sur les normes visant à garantir la sécurité dans le cyberespace sont de plus en plus dirigées et dominées par les gouvernements. Par conséquent, elles sont principalement sécurisées et encadrées en termes de menaces. » [1597] Notons malgré tout qu'il existe parmi certains Etats une évolution relative d'une lecture « régalienne » de la cybersécurité. La prise en compte et la défense des droits de l'homme au sein du cyberespace est défendue par l'Appel de Paris, lancé en 2018 par la France, soutenu par 80 Etats environ, dont depuis 2021

---

[1590] « a rule against certain specified uses of the collected data such as publishing or leaking sensitive personal data and/or a rule against exploiting such data sets for the purpose of coercion, extortion, or manipulation GEISS, Robin, LAHMANN, Henning, *ibid*.

[1591] « The human rights dimension of the cyber security agenda is usually separated out from the "international security" agenda, at least in the context of the UN. This is due in part to the structure of the UN itself, but possibly also because it's politically awkward—some of the countries that are the largest proponents of cyber stability and norm development, for example, are also quietly permitting the export of digital surveillance technologies produced by companies in their jurisdiction. » PYTLAK, Allisson, « Solving the Rubik's cube : what's next for norms in cyber space », *Forum on the Arms Trade*, 27/12/2018
https://www.forumarmstrade.org/blog/solving-the-rubiks-cube-whats-next-for-norms-in-cyber-space

[1592] MITNICK, Drew, « Access now to join the Paris Call for Trust and stability in Cyberspace »Access now, 12/11/2018, https://www.accessnow.org/access-now-to-join-the-paris-call-for-trust-and-stability-in-cyberspace

[1593] FERRARI, Veronica, KUMAR, Sheetal, PYTLAK, Allison, MARTINS, Paula, PAVLOVA, Pavlina, "Promoting stakeholder engagement at the Open Ended working group on ICTs », APC, 26/10/2021
https://www.apc.org/fr/node/37718

[1594] Paris Call for Trust and Security in Cyberspace Working Group 5: Building a Cyberstability Index
https://cyberpeaceinstitute.org/wp-content/uploads/PWGR5_8.11.21_Finale.pdf

[1595] PYTLAK, Allison, « In search of human rights in multilateral cybersecurity dialogues », in: TIKK, Eneken, KERTTUNEN, Mika (des), *Routledge handbook of international cybersecurity*, Routledge, 2020,402 p.

[1596] « human rights are discussed as part of the framework but the prevailing understanding of what constitutes cybersecurity remains heavily focused on the level of sovereign state - its territory and infrastructure - rather than the individual. This phenomenon can be understood from an international relations perspective as a realpolitik approach to governance when state interests are privileged, and a military-centric approach to the issue prevail. » PAVLOVA, Pavlina, "Human rights-based approach to cybersecurity: addressing the security risks of targeted groups", *Peace Human Rights Governance*, 4(3), November 2020.

[1597] "Discussions on norms for ensuring security in cyberspace are increasingly government-led and dominated. As a result they are mostly securitized, and framed in terms of threat narratives…"Ibid.

les Etats-Unis[1598]. Différents acteurs poussent cet agenda au sein des instances onusiennes, au sein du OEWG[1599], ainsi qu'au sein de groupements multi-gouvernementaux comme la « Freedom Online coalition ». [1600] L'ampleur de cette évolution est discutée parmi les activistes et les organisations de défense de droits en ligne [1601], ces derniers critiquant également le manque d'engagement d'Etats comme la Russie ou la Chine[1602].

Et surtout, cette position reste minoritaire au sein des ONG humanitaires. Notons aussi que le sujet de l'humanitaire est marginal au sein de l'agenda d'ONG de défense des droits de l'homme en ligne. En effet, les ONG militent pour une meilleure protection des activistes, des minorités, des journalistes, etc. Et surtout, elles ont une conception spécifique de la protection de la vie privée, en lien avec l'exercice de la liberté d'expression, d'association, permettant d'assurer le développement d'une société démocratique. Contrairement au CICR, ces discours ne concernent pas les répercussions sur les infrastructures vitales et sur les besoins primaires des individus. Il faut dire que le mandat du CICR est concentré sur les conflits armés, qu'il est attaché au principe de neutralité. Succinctement, les droits humains sont considérés comme étant plus « politiques ». Et l'idée a longtemps prévalu que les droits de l'homme s'appliquaient qu'en temps de paix. Ce point est cependant très discuté, l'articulation entre droits de l'homme et droit humanitaire fait l'objet de nombreuses analyses[1603]. Mais rares sont encore les réflexions portant spécifiquement sur le droit à la vie privée, comme le surlignent Asaf Lubin et Rusell Buchan : « Malgré la dépendance croissante des armées à l'égard des données, les droits de l'homme numériques sont encore, souvent par réflexe, considérés comme une préoccupation juridique de temps de paix. »[1604] Pourtant certains juristes, comme la professeure de droit international Mary Ellen O'connell, défendent leur

---

[1598] L'appel de Paris consiste en un accord lancé à l'initiative de la France en 2018, il a pour finalité le renforcement de la lutte contre les cybermenaces ( cyberopérations, cyberattaques), et l'application et la protection des droits des individus en ligne. Il comprend notamment les 9 principes suivants : protéger les individus et les infrastructures critiques des cyber-activités malveillantes ; protéger la disponibilité et l'intégrité d'Internet ; prévenir les interférences destinées à déstabiliser les processus électoraux ;de défendre la propriété intellectuelle face aux menaces cyber ;d'empêcher la prolifération de logiciels et de pratiques informatiques malveillants ;d'accroître la sécurité des produits et services numériques ; d'améliorer l'hygiène informatique de tous ; d'empêcher les acteurs non-étatiques, y compris le secteur privé, de mener des actions de cyber-riposte ;de renforcer les normes internationales de comportements responsables et les mesures de développement de la confiance. » https://parispeaceforum.org/fr/initiatives/appel-de-paris-pour-la-confiance-et-la-securite-dans-le-cyberespace/

[1599] Workshop on the Human-centric approach to cybersecurity in the context of the OEWG, EU Cyber direct, 26/07/2023https://eucyberdirect.eu/events/workshop-on-the-human-centric-approach-to-cybersecurity-in-the-context-of-the-oewg

[1600] https://freedomonlinecoalition.com/aims-and-priorities/

[1601] « Malheureusement, notre message sur l'impératif d'utiliser le cyberespace à des fins pacifiques n'est pas actuellement reflété par le comportement des États dans le cyberespace. Le fossé entre notre vision du cyberespace et celle de plusieurs États s'est creusé au lieu de s'atténuer, malgré des années de discussions au sein des groupes successifs des Nations unie. » « Unfortunately, our message of the imperative to use cyberspace for peaceful purposes is not currently being reflected by state behaviour in cyberspace. The disconnect between our vision of cyberspace and that held by several states has been growing rather than lessening despite years of discussion in successive UN groups. »
Joint civil society statement on cyber peace and human security, APC, 11/10/2023, updated 10/06/2024https://www.apc.org/en/pubs/joint-civil-society-statement-cyber-peace-and-human-security-1

[1602] PYTLAK, Allison, "Joint civil society statement on cyber peace and human security », 13/10/2022 https://documents.unoda.org/wp-content/uploads/2022/10/13Oct_cyber.pdf
BROWN, Deborah, « It's time to treat cybersecurity as a human rights issue », *Human Rights watch*, 26/05/2020,https://www.hrw.org/news/2020/05/26/its-time-treat-cybersecurity-human-rights-issue
BROWN, Deborah, ESTERHUYSEN, Anriette, « Why cybersecurity is a human rights issue, and it is time to start treating it like one », *Incyber*, 23/12/2023https://incyber.org/en/article/why-cybersecurity-is-a-human-rights-issue-and-it-is-time-to-start-treating-it-like-one-by-deborah-brown-anriette-esterhuysen-association-for-progressive-communications/

[1603] International legal protection of human rights in armed conflict, United Nations of human rights, 2011 https://www.ohchr.org/sites/default/files/Documents/Publications/HR_in_armed_conflict.pdf

[1604] "Despite the militaries' increasing dependency on data, digital human rights are still, often reflexively, considered a peacetime legal concern. It is tacitly assumed that, should war break out, there would be more specific norms to rely on. Yet in fact, when it comes to the right to privacy, IHL is surprisingly silent." LUBIN, Asaf, BUCHAN, Russell (ed.),*The rights to privacy and data protection in times of armed conflict*, CCDOCOE, 2022, p.

application en contexte conflictuel. Elle s'appuie sur des décisions de la Cour internationale de justice[1605] et au Pacte international relatif aux droits civils et politiques, et plus précisément à son article 4 qui indique que certains droits ne peuvent pas être suspendus lors d'urgences nationales [1606]. Cela dit, le droit à la vie privée n'en fait pas partie. Ce point devrait être discuté. Pour Mary Ellen O'Connel, le fait de ne pas maintenir le droit à la vie privée n'apporterait pas d'avantages militaires. La juriste ajoute que la suspension des droits de l'homme — même en cas de conflit — doit être permise qu'en cas exceptionnels et doit être précisément motivée[1607].

Le juriste Assaf Lubin explore une autre voie : il cherche à extraire le droit à la vie privée du DIH par un travail d'analogies. Asaf Lubin a mené une analyse serrée et fine sur la nécessité de protéger la vie privée des parties prenantes d'un conflit ainsi que des civils. Mais point important, il commence par reconnaitre que cette tâche peut paraitre absurde : la défense de la vie privée semble dérisoire à côté de drames humains bien plus graves ayant lieu durant les guerres[1608]. Pour Asaf Lubin, préserver cette dernière est malgré tout essentiel au nom de la dignité humaine. Ce principe, qui est au cœur du DIH, lui permet de justifier sa démarche. Le respect d'autrui et de sa dignité reste crucial, afin de préserver toute personne, dans ce qu'elle a de plus humain, et protéger tout à chacun d'une éventuelle humiliation [1609]. Mais la conception de la dignité contenue dans le DIH est « négative » : sa finalité est de défendre la personne contre de potentielles humiliations et traitements dégradants. Or, il existe une autre conception de la dignité, fondée sur la notion d'autonomie. Cette dernière est aussi centrale dans le droit à la protection des données, comme on le verra dans notre troisième partie consacrée aux droits des bénéficiaires. Revenons pour le moment aux réflexions d'Asaf Lubin. Ce dernier reste dans le champ du DIH pour chercher un cadre protecteur adapté à la défense du droit à la vie privée. Ce cadre tient en trois points : ce devoir de précaution, le devoir de vigilance constante ainsi que celui de manœuvre militaire. Le devoir de vigilance constante pourrait servir de rustine permettant de combler les manques du DIH en matière de protection des données : « le devoir de précaution peut servir à combler temporairement la lacune qui existe en matière de protection des données dans le droit international humanitaire, du moins

---

[1605] ICJ advisory opinion on Nuclear Weapons : "that the protection of the International Covenant of Civil and Political Rights does not cease in times of war, except by operation of Article 4 of the Covenant whereby certain provisions may be derogated from in a time of national emergency. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, 240.

[1606] le droit à la vie, le droit de ne pas être soumis à la torture et à d'autres traitements dégradants ou humiliants, le droit de ne pas être réduit en esclavage, le droit à une nationalité, le droit de ne pas être soumis à une disparition forcée ou le droit positif d'être une personne légale, le droit de ne pas être discriminé, le droit de ne pas être emprisonné pour une dette, la liberté de pensée et de religion, et le droit de ne pas être soumis à des charges légales ex post facto

[1607] O'CONNELL, Mary Ellen, "Data privacy rights : the same in War and Peace", in BUCHAN, Russell, LUBIN, Asaf ( eds.), *The rights to privacy and data protection in armed conflict*, CCDOCOE , 2022,p.12-29

[1608] ASAF, Lubin, "The Rights to Privacy and Data Protection Under International Humanitarian Law and Human Rights Law, in: KOLB, Robert, GAGGIOLI, Gloria, KILIBARDA, Pavle, eds, *Research Handbook on Human Rights and Humanitarian Law: Further Reflections and Perspectives*, Edward Elgar, 2022, p.463-492

[1609] La convention de Genève proscrit en effet un ensemble de comportements jugés dégradants et humiliants. Certains passages le vocabulaire employé est celui de l'honneur. Art 13 traitement humain des prisonniers « En particulier, aucun prisonnier de guerre ne pourra être soumis à une mutilation physique ou à une expérience médicale ou scientifique de quelque nature qu'elle soit qui ne serait pas justifiée par le traitement médical du prisonnier intéressé et qui ne serait pas dans son intérêt. » Article 14 - Respect de la personne des prisonniers. Les prisonniers de guerre ont droit en toutes circonstances au respect de leur personne et de leur honneur. Les femmes doivent être traitées avec tous les égards dus à leur sexe et bénéficier en tous cas d'un traitement aussi favorable que celui qui est accordé aux hommes. Article 52 - Travaux dangereux ou humiliants. Aucun prisonnier de guerre ne sera affecté à un travail pouvant être considéré comme humiliant pour un membre des forces armées de la Puissance détentrice. Le chapitre V est consacré au principe de dignité, dans le sens où il porte sur le traitement des personnes civiles et des combattants hors de combat ; en définissant ce que doit être un « traitement humain » de ces derniers. Cette notion est explicitée par différents textes de droit international humanitaire et de droit des droits de l'homme.

jusqu'à ce que des régimes de protection des données plus étendus et plus restrictifs soient mis en œuvre par le biais de l'évolution des traités et de la formation d'une coutume. » [1610]

Le devoir de vigilance constante découle du principe de précaution formulé comme suit dans l'article 57 du protocole I additionnel aux Conventions de Genève de 1949 : « Les opérations militaires doivent être conduites en veillant constamment à épargner la population civile, les personnes civiles et les biens de caractère civil. » Il nécessite donc de vérifier la nature de l'objet de l'attaque, de minimiser les dommages accidentels par le choix de la méthode et des moyens employés, de suspendre une opération si elle s'avère disproportionnée, de prévenir les populations civiles avant une attaque. Mais cette liste n'est pas arrêtée. Elle peut être complétée. Reste à savoir si ce principe s'applique au-delà des attaques. Pour Asaf Lubin, c'est le cas. Le devoir de veille constante couvre aussi les manœuvres militaires, sachant que ce terme désigne « tous mouvements, manœuvres et autres activités quelconques effectués par les forces armées en vue du combat » (art. 57, PA I) Le devoir de précaution doit être constant, ce qui lui donne une certaine latitude d'application, quand bien même sa frontière d'application reste sujette à discussion. En tout cas, pour Asaf Lubin, il va au-delà des dommages physiques [1611] . Dans l'espace numérique, il correspond pour Asaf Lubin à l'ensemble des opérations informationnelles nécessaires au déploiement d'une activité militaire. La seule condition étant qu'il s'agisse d'un traitement de données effectuées afin de mener un combat. Asaf Lubin, en tant qu'ancien analyste, s'intéresse aux activités de renseignement militaire et aux enjeux de protection des données qu'elles impliquent. On peut faire l'hypothèse que sa démarche peut s'appliquer à des opérations de cyberespionnage touchant les ONG humanitaires. Et pour réaliser ce principe de précaution, il propose d'appliquer différentes obligations du droit à la protection des données (légalité, transparence, minimisation des données).

Le principe de précaution peut effectivement faire écho au principe de minimisation de collecte de données (il s'agit de réduire les dommages potentiels d'un traitement). On peut ajouter qu'un parallèle existe entre le ciblage des opérations et les méthodes d'évaluation de risque. Il faut prendre toutes les précautions possibles quant au choix des moyens militaires pour réduire les dommages civils. La possibilité de contrôler le ciblage d'une cyberattaque est hautement discutée, du fait de l'interconnexion d'Internet. Et la place des droits des civils dans le DIH est moins claire. Asaf Lubin fait référence à l'obligation d'avertissement des populations civiles au préalable d'une attaque pouvant causer des dommages collatéraux. Il nous parait difficile de pouvoir défendre ce type de principe dans un contexte de cyberconflictualité quand bien même Asaf Lubin appelle les États à plus de transparence.

---

[1610] "thus argue that the duty of constant care may serve as a temporary gap-filler to the lacuna that exists around data protection in IHL, at least until more expansive and restrictive data protection regimes are implemented through treaty evolution and custom formation.

[1611] "But the duty of constant care could theoretically be said to extend beyond physical harms. Indeed, the parallel duty of defenders, in Article 58, refers to an even broader category of "dangers" and not mere damages." "Mais on pourrait théoriquement dire que le devoir de diligence constante s'étend au-delà des préjudices physiques. En effet, le devoir parallèle des défenseurs, à l'article 58, se réfère à une catégorie encore plus large de "dangers" et non de simples dommages. »

LUBIN, Asaf, "The duty of constant care and data protection in War", in, DICKINSON A., Laura, BERG, Edward, *Big data and armed conflict: legal issues above and below the armed conflict threshold*, Oxford University Press,2024, p.229-248

LUBIN, Asaf, " Liber studies big data volume, algorithms of care: military AI, digital rights, and the duty of constant care", *Article of war*, 13/02/2024

https://lieber.westpoint.edu/algorithms-care-military-ai-digital-rights-duty-constant-care/

Toujours est-il que l'analyse d'Asaf Lubin est sous-tendue par la conviction qu'il est nécessaire de défendre les individus contre des situations humiliantes, avec pour conséquence le fait qu'il faille réguler des opérations de renseignement selon les principes cités[1612]. Florian Egloff et James Shires appellent également à prendre au sérieux les affects des personnes dans leur analyse des cyberopérations, notamment en redéfinissant la notion de violence. Point crucial, puisque pour rappel, la violence est au cœur de la définition d'une attaque selon le DIH[1613].

Et donc Florian Egloff et James Shires contestent l'idée que les attaques cybernétiques seraient moins violentes que les attaques cinétiques, sans rejoindre pour autant un discours catastrophiste sur les menaces numériques, puisqu'ils rappellent que la majeure partie des cyberopérations ne causent pas directement des dommages physiques[1614]. Pour les deux chercheurs, la violence peut être définie comme un dommage intentionnel et direct. Sachant que ce dernier terme signifie le fait de porter atteinte à la santé ou à l'existence d'une personne ou annihiler un objet[1615]. Les dommages peuvent porter sur trois dimensions de la personne : son corps, sa vie affective, sa dimension sociale. Ils ne fixent pas de seuil d'intensité définissant un fait de violence. Il ne faut pas oublier les micro-agressions, un acte causant peu de dommages peut être violent, d'autant que ce qui fait sa sévérité est contextuel et culturel. Ils mettent à l'épreuve leur définition en examinant son application à différentes catégories d'opérations, non considérées comme des attaques : l'espionnage ou le sabotage. Ils précisent que toutes les cyberopérations ne sont pas considérées comme violentes. L'espionnage industriel a peu de chance de générer de la violence, et ce n'est pas l'intention première des attaquants. En revanche, le cyberespionnage peut violer l'intimité et la vie privée des individus et avoir un « effet glaçant » (« chilling effect »). Il peut affecter une communauté entière et mener à de la détention ou à de la torture, et donc constituer des formes de violence. Quant aux actes de sabotage (ils prennent l'exemple de Notpeya), il est possible qu'ils ne causent pas de morts, mais ils peuvent être violents. L'intentionnalité de tels actes peut être d'éroder la confiance dans l'État et créer un sentiment de vulnérabilité. On l'a vu pour eux, toute cyberopération ne constitue pas une forme de violence pour les individus, mais leur réflexion offre un cadre d'analyse permettant de prendre en compte un plus large panel de répercussions, dont les atteintes à la vie privée[1616], contrairement au DIH qui se concentre sur la fonctionnalité des serveurs informatiques et les effets matériels, avec pour argument premier la nécessité d'assurer la continuité de l'aide, sauf pour des cas bien spécifiques (les données médicales par exemple).

---

[1612] ASAF, Lubin, "The Reasonable intelligence agency", Articles by Maurer Faculty, 3034, 2022https://www.repository.law.indiana.edu/facpub/3034

[1613] EGLOFF, Florian, SHIRES, James, « The better angels of our digital nature ? Offensive cyber capabilities and state violence", *European Journal of international security,* 2023, 8, p. 130-149.

[1614] "Given the extensive overlap between cyber capabilities deployed for espionage and disruptive purposes, we do not exclude such activity by definition." EGLOFF, Florian, SHIRES, James, ibid.

[1615] « the diminishing, damage, or destruction of areas of human value. »ibid.

[1616] « It therefore adds analytical value to current insights of strategic studies on the kinds of harm caused by cyber operations, parsing more finely different forms of espionage, sabotage, and subversion. It also emphasises that violent uses of OCCs are likely to occur in repressive situations, while canonical forms of cyber-espionage remain non-violent. Furthermore, the examples in this section underline that interference with data in a digitalized society may result in harm commensurate with or exceeding the destruction of physical objects or bodily injury. »ibid.

Le discours régalien faisant de la cybersécurité un enjeu de défense nationale est contesté, notamment par une série d'organisations relatives à la défense des droits de l'homme en ligne, mais il faudrait encore donner plus de corps aux acteurs de la société civile. Il faudrait détailler la façon dont ils inscrivent leur conception de la cybersécurité à l'agenda d'arènes comme l'« Open Working Group » onusien, et la façon dont ils tentent de se différencier des acteurs étatiques. Quant au CICR, l'organisation se situerait aux frontières de ces deux récits, dans le sens où ses positionnements vont certes à l'encontre des positionnements étatiques, en mettant l'accent sur la protection des civils, mais ils ne sont pas pour autant dénués de proximité avec les discours de sécuritisation portés par les acteurs étatiques. Ils reprennent en partie les représentations faisant du cyberespace comme un espace de menace dans le cadre de conflits entre grandes puissances. Mais si les États concentrent leur attention sur les dommages physiques des cyberopérations portés sur infrastructures critiques, le CICR reprend cette façon de cadrer les menaces, en mettant également l'accent sur la nécessité de protéger ses infrastructures informatiques afin d'assurer la continuité de l'aide. Et même si l'on commence à trouver des traces de la nécessité de protéger les individus face aux cyberopérations de cyberespionage, ce n'est pas en premier lieu en raison de la défense de la vie privée des personnes concernées. Il est surtout nécessaire pour le CICR d'assurer la confiance entre ONG et bénéficiaires, ainsi que leur protection. Ainsi, on peut lire dans une déclaration écrite de juin 2021 du CICR « qu'une utilisation inadaptée des nouvelles technologies ne conduise à la stigmatisation, à une vulnérabilité et une fragilité accrues, à la discrimination, à la persécution et à des atteintes à l'intégrité physique et psychologique de certaines populations dans des environnements peu sûrs. En ce sens, la bonne utilisation des nouvelles technologies est une question de vie ou de mort. »[1617] Cette lecture du risque numérique pourrait sembler stratégique, et découler d'un désir d'attirer l'attention sur un risque pouvant paraitre abstrait, il s'inscrit en tout cas dans le mandat du CICR, dédié à la protection des civils dans le cadre de conflits.

On pourrait lui adresser la critique que cette approche de la cybersécurité tend plus ou moins implicitement à réduire les bénéficiaires à de simples victimes et de simples objets de protection. Comment s'assurer aussi qu'il s'agit des sujets de droit ? C'est à ces questions que sera dédiée notre dernière partie. On se souvient qu'Asaf Lubin a évoqué la nécessité de revenir sur la notion de dignité comme fondement du droit à la vie privée. Cette conviction sert de point de départ à notre troisième partie. On s'appuiera donc dans nos prochains développements sur cette notion et en mettant l'accent sur les tensions qu'elle implique entre autonomie et vulnérabilité.

[1617] "The ICRC is concerned that unsuitable usage of new technologies could lead to stigmatisation, increased vulnerability and fragility, discrimination, persecution, and attacks on the physical and psychological integrity or certain populations in insecure environments. In this sense, the proper use of new technologies is a matter of life and death." Written evidence from International Committee of the Red Cross (ICRC) (TFP0029) https://committees.parliament.uk/writtenevidence/36625/pdf/

Cette nécessité de garantir l'autonomie des bénéficiaires peut faire écho au concept souveraineté. Il désigne le fait d'être maitre de ses données et il a pu être utilisé par différentes chercheurs et chercheuses travaillant sur les enjeux de protection des données de populations indigènes, cherchant à se défaire de legs coloniaux. La notion de dignité m'a paru intéressante, notamment parce qu' elle fait écho à toute une tradition juridique (notamment germanique) liant autodétermination informationnelle et dignité. Elle prend racine dans un terreau philosophique spécifique, notamment kantien, qui met l'accent sur sa définition de la dignité sur l'autonomie de l'individu. Elle a connu différentes interprétations plus contemporaines. Et elle occupe une bonne place dans les théories du care, qui met en perspective la définition « traditionnelle » de la dignité fondée sur l'autonomie du sujet, pour mieux articuler vulnérabilité et autonomie. Ce qui nous a paru être très intéressant concernant l'humanitaire, dont les sujets sont marqués par certaines formes de vulnérabilité.

## Introduction de partie

La question qui sert de fil rouge à ce chapitre est la possibilité pour des « indésirables » d'exercer leurs droits accordés par le RGPD en contexte humanitaire. On se distanciera donc des analyses biopolitiques, réduisant l'existence des bénéficiaires à des « vies nues », en faisant des victimes passives dont seule la subsistance compte. Pour ce faire, on va s'appuyer sur la notion de dignité en la liant à celle d'autodétermination informationnelle. La notion de dignité permet en effet de les considérer comme des acteurs autonomes pouvant exercer leurs droits. Sachant qu'on a affaire à des personnes vulnérables, ou du moins catégorisées comme telles. Or il existe une tension entre la notion de vulnérabilité et de dignité, qui est profondément liée à celle d'autonomie. Cette tension semble nous concerner tous. Nous sommes ontologiquement vulnérables, citoyens comme parias. Notre fragilité serait propre à notre condition humaine. On ne peut pas y échapper, seulement la nier. Nous sommes des êtres vivants, et c'est ceci qui nous rend vulnérables, à la maladie, aux blessures et au bout du compte à la mort. La vulnérabilité n'est pas nécessairement un label, une catégorie assignant à une perte de possibilité d'exercice de ses droits. C'est qu'il existe deux sources de vulnérabilité : une source inhérente (liée à notre condition humaine) et une source situationnelle[1618], pouvant être exacerbée ou au contraire résorbée en fonction de la situation sociale, politique, économique ou encore environnementale. Cette vulnérabilité situationnelle n'est pas nécessairement stigmatisante. Elle ne caractérise pas l'individu de façon profonde. Il existe donc du « jeu », une forme de fluidité. Par voie de conséquence, un individu vulnérable n'est pas nécessairement réduit à sa fragilité. Toutefois, on peut distinguer les personnes étant considérées en soi comme vulnérables (les enfants) et les personnes dont on évalue le « degré » de vulnérabilité (on parle alors de vulnérabilité « graduelle »). Cette dernière forme de vulnérabilité est ambiguë. Elle rentre en jeu lorsqu'il est question afin de déterminer le statut administratif ou judiciaire d'un individu (personne majeure protégée, travailleur handicapé, etc.). Dans l'humanitaire aussi on détermine le degré de vulnérabilité

[1618]MAILLARD, Nathalie, *La vulnérabilité, une nouvelle catégorie morale ?,* Genève, Labor et Fides, coll. « Le champ éthique », 2011, 386 p.

des individus afin d'identifier leur besoin et le type d'assistance devant leur être délivrés. L'évaluation de la vulnérabilité des bénéficiaires repose sur des critères propres déterminés par les agences humanitaires[1619]. Par conséquent, le fait d'être considéré ou non comme vulnérable a des conséquences directes et matérielles sur la vie des bénéficiaires. L'usage du terme de vulnérabilité n'est pas simplement rhétorique. Or ce travail de catégorisation accorde des droits (à une aide sociale, humanitaire), mais elle risque de « figer » les vulnérabilités des individus. Il va de pair, pour Michel Agier, avec une réduction des bénéficiaires à un statut de « victime ». Ces derniers ne seraient plus que de simples corps souffrants et silencieux[1620]. Cette victimisation des sujets tend à constituer « un espace et un langage qui, eux, sont humanitaires et ne connaissent que le sujet/objet, image et corps silencieux du vulnérable/indésirable. »[1621] Et donc ce travail de catégorisation place l'individu dans une posture de dépendance. Sa perte d'autonomie entrainerait une remise en cause de la possibilité d'exercer comme sujet politique. Or le fait d'être « vulnérable » n'implique pas nécessairement une perte d'agentivité et une forme d'exclusion du groupe social et de la possibilité d'y être un citoyen actif. Les théories du care pensent au contraire la notion de vulnérabilité comme facteur d'inclusion et non pas comme facteur d'exclusion. La reconnaissance de l'universalité de la vulnérabilité nourrit un sentiment de sollicitude fondateur d'un groupe social. Les philosophes Catriona Mackenzie ou Nathalie Maillard ont utilisé le concept de vulnérabilité comme une catégorie critique permettant de pointer les limites d'une conception libérale de l'individu[1622]. Selon cette tradition philosophique (venant notamment de Kant), l'autonomie de la personne est fondée sur la capacité de juger, de conduire un raisonnement librement, sans qu'entre en jeu l'influence d'autrui. Or pour la pensée du care, le concept de vulnérabilité devient un instrument critique visant à contester la focalisation des théories morales sur la figure du sujet autonome[1623]. La philosophe Nathalie Maillard souligne toutefois qu'il ne s'agit pas de se positionner pour ou contre la vulnérabilité et l'autonomie. Au contraire. Les deux concepts s'enrichissent mutuellement. Le but de Nathalie Maillard est de penser ce que pourrait être une forme d' » autonomie relationnelle. » En effet, l'autonomie et l'agentivité d'une personne dépendent fortement des soins apportés afin de réparer ses vulnérabilités. Le soin pourrait bien être le fondement de cette autonomie non autocentrée, voire d'une dignité. Citons alors les réflexions de Cynthia Fleury qui déclare que : « seule la clinique de la dignité rend possible cette dignité. Et cette clinique est l'œuvre du soin : d'abord d'un juste diagnostic sur les conditions matérielles et existentielles d'un vécu, puis du déploiement d'outils de guérison, de méthodes (traitements), d'observance desdits sujets, sachant qu'il n'y aura "dignité" que parce qu'il y a cocréation de celle-ci, autrement dit, participation active, agente, desdits sujets. »[1624] On peut partir de la citation de Cynthia Fleury pour explorer différentes manières de sortir du discours de victimisation des bénéficiaires, et donc respecter leur dignité. Et il ne sera a priori pas ici question des notions

---

[1619] SÖZER, H., "Humanitarianism with a neo-liberal face: vulnerability intervention as vulnerability redistribution", *Journal of Ethnic and Migration Studies*, *46*(11), 2020, p. 2163–2180. https://doi.org/10.1080/1369183X.2019.1573661
SECONI, Isadora, "The continuous and inextricable interaction between gender and humanitarian technology as a site of production of vulnerability The case of UNHCR's assessment framework in Jordan", Mémoire, Humanities and Social Sciences, Uppsala University 2022
TURNER, Lewis, "The Politics of Labeling Refugee Men as "Vulnerable"", *Social Politics: International Studies in Gender, State & Society*, Volume 28, Issue 1, Spring 2021, p. 1–23, https://doi.org/10.1093/sp/jxz033

[1620] AGIER, Michel, « Le camp des vulnérables. Les réfugiés face à leur citoyenneté niée », *Les Temps Modernes*, 2004/2 (n° 627), p. 120-137 https://www.cairn.info/revue-les-temps-modernes-2004-2-page-120.htm

[1621] AGIER, Michel, « Penser le sujet, observer la frontière », *L'Homme*, 203-204 | 2012, http://journals.openedition.org/lhomme/23096

[1622] GARRAU, Marie, *Politiques de la vulnérabilité*, CNRS éditions, 2018, 370 p.

[1623] MACKENZIE, Catriona, ROGERS Wendy, DODDS Susan, (eds), *Vulnerability : New Essays in Ethics and Feminist Philosophy*, Studies in Feminist Philosophy, New York, 2013, 336 p. https://doi.org/10.1093/acprof:oso/9780199316649.001.0001

[1624] CYNTHIA, Fleury, *La Clinique de la dignité*, Paris, Seuil, 2023, P.24

de résilience ou d'empowerment, qui sont associés à un autre univers conceptuel. Rendre quelqu'un résilient passe par une responsabilisation normative des bénéficiaires. Le but est alors de les inciter à faire en sorte d'acquérir les ressources pour dépasser une condition fragilisée et acquérir à nouveau une forme d'autonomie. Le terme de dignité quant à lui est entendu dans un sens plus politique, puisqu'on verra qu'il recentre la réflexion sur la possibilité d'exercer de manière active ses droits. Mais ce concept est particulièrement ardu à manier, du fait de sa polysémie, de son caractère élastique. Clef de voute des droits humains, il est employé dans des contextes variés, jusqu'à être vidé de son sens fort. Il risque en effet d'être réduit à usage plus mou et quasi rhétorique. En sommes, son usage excessif aboutirait à une dépolitisation des droits humains, comme le déplore la chercheuse Hélène Thomas[1625] .

Ce concept est aussi difficile à aborder en raison du caractère irréductible de l'essence humaine, d'où la proposition de penser que le concept est parfois comme un axiome. Cette expression désigne en effet le premier terme d'un raisonnement qui reste de l'ordre de l'indéfinissable[1626]. Une autre solution est de tenter de définir la notion en listant l'ensemble de situations portant atteinte à la dignité. Cela risque de restreindre le principe de dignité à une notion normative, voire rétrograde, puisqu'au nom de la dignité humaine de nombreuses libertés et droits peuvent être condamnés[1627]. Certains penseurs libéraux sont donc critiques à l'encontre de la dignité, puisqu'ils défendent qu'au nom de la liberté tout comportement puisse être légitimé, y compris ceux portant atteinte à la dignité d'une personne. Cette conviction va pourtant à l'encontre de Kant, penseur libéral, dont la pensée accorde une large place à la dignité.

La dignité kantienne incarne le refus de se traiter comme une chose, de porter atteinte à soi (Kant condamne donc l'idée de suicide). Il faut absolument ne pas considérer l'autre et soi-même comme un moyen pour atteindre une fin. Ceci consiste en une loi morale, présente en chaque personne, qui doit être capable de l'« écouter », en toute indépendance. La dignité est le propre de tout être raisonnable dans le sens où il est capable de moralité, c'est-à-dire en tant qu'il est capable de s'autodéterminer et de se donner librement des fins. La définition kantienne de la dignité est donc fondée sur la notion d'autonomie. Dans son ouvrage, les Fondements de la Métaphysique des mœurs, Kant écrit donc que : « la raison rapporte ainsi chacune des maximes de la volonté conçue comme législatrice universelle à chacune des autres volontés, et même à chacune des actions envers soi-même, et cela non pas pour quelque autre motif pratique ou quelque futur avantage, mais en vertu de l'idée de la dignité d'un être raisonnable qui n'obéit à d'autres lois que celle qu'il institue en même temps lui-même. »[1628] Cette loi morale est d'une valeur supérieure et incomparable, mais n'a pas de prix : « Nulle chose en effet n'a de valeur en dehors de celle que la loi lui assigne. Or la législation même qui détermine toute valeur doit avoir précisément pour cela une dignité, c'est-à-dire une valeur inconditionnée, incomparable que traduit le mot de respect, le seul qui fournisse l'expression convenable de l'estime qu'un être raisonnable en doit faire.

[1625] THOMAS, Hélène, *Les vulnérables : la démocratie contre les pauvres*, Paris, Éditions du Croquant, 2010, 254 p

[1626] FABRE-MAGNAN Muriel, « La dignité en droit : un axiome », *Revue interdisciplinaire d'études juridiques*, 2007/1 (Volume 58), p. 1-30. https://www.cairn.info/revue-interdisciplinaire-d-etudes-juridiques-2007-1-page-1.htm

[1627] HENNETTE-VAUCHEZ Stéphanie, « Une dignitas humaine ? Vieilles outres, vin nouveau », *Droits*, 2008/2 (n° 48), p. 59-86. https://www.cairn.info/revue-droits-2008-2-page-59.htm

[1628] KANT, Emmanuel, Fondements de la métaphysiques des moeurs,Paris, Le Livre de Poche, 1993, P.152

L'autonomie est donc le principe de la dignité de la nature humaine et de toute nature raisonnable. »[1629] La dignité est donc au fondement de l'éthique morale kantienne, mais il ne s'agirait pas d'un principe transcendant, comme le note la philosophe Michaela Marzano : « lorsque Kant parle de la dignité et de ses liens avec l'autonomie individuelle, il ne prétend cependant pas soumettre l'individu à quelque chose qui le transcende, à une instance objective qui définirait ce qui est humain et ce qui ne l'est pas. La dignité dont il nous parle est celle qui appartient à un être humain à partir du moment où il justifie ses choix en s'appuyant sur une norme (nomos) qu'il s'est donnée à lui-même (autos) selon son jugement et sa raison propres. »[1630]

Dans le même temps, sa définition se veut universelle, chaque être humain a la faculté d'entendre cette loi morale. Mais Kant laisse de côté les êtres non rationnels. Pour lui, la dignité est réservée à l'être humain. Il existe certes des tentatives de reconsidérer le droit à la dignité des êtres non « humain », des animaux, voire des plantes[1631]. Mais généralement, la dignité reste une notion anthropocentrée. La dignité est le propre de l'homme, il s'agit d'une propriété ontologique et nier sa dignité, c'est nier son essence[1632]. La dignité devient une protection contre la déshumanisation, le fait d'être traité comme une chose, d'être l'objet d'un traitement indigne et de barbarie[1633], de crime contre l'humanité[1634]. Il existe différents exemples de réification d'une personne : cela peut signifier le fait d'avoir un statut d'esclave, devenir la propriété d'autrui, ou être le sujet d'expériences médicales sans consentement. L'exemple le plus terrible reste le cas d'expérimentations par des médecins nazis. Mais dans d'autres situations, cela peut aussi signifier le fait de volontairement se considérer comme une chose, pouvant être commercialisée (et par exemple vendre volontairement ses propres organes). Toutefois, les atteintes à la dignité des personnes peuvent recouvrir des circonstances a priori moins extrêmes, comme le fait de se retrouver dans une situation dégradante ou humiliante, que ce soit sur le plan psychique, corporel[1635] ou matériel. Rester digne, c'est donc aussi bénéficier de condition de vie décente[1636], et non pas être réduit à subir une vie invivable[1637]. Ajoutons que le terme de dignité signifie le fait d'être reconnu comme une personne digne de respect. La dignité a donc aussi une dimension relationnelle. Elle peut être analysée via la notion de reconnaissance, par le prisme des textes d'Axel Honneth[1638]. Elle est aussi liée à l'appartenance à un corps politique, comme le soutient Hannah Arendt, pour

[1629] KANT, Emmanuel, *Fondements de la métaphysiques des moeurs*,Paris: Le Livre de Poche, 1993, p.142-143
[1630] MARZANO, Michaela, *Je consens, donc je suis, éthique de l'autonomie*, Presse universitaire de France, 2006, p.61.
[1631]Par exemple, la *Déclaration de Barcelone* de 1998, référence en matière de bioéthique, proposait d'élargir le sens du principe de dignité notamment, précisant que l'être humain a des devoirs envers la partie non humaine de la nature vivante , à savoir les animaux, les plantes et l'environnement.
[1632] DELMAS-MARTY Mireille, « Humanité, espèce humaine et droit pénal », *Revue de science criminelle et de droit pénal comparé*, 2012/3 (N° 3), p. 495-503 https://www.cairn.info/revue-de-science-criminelle-et-de-droit-penal-compare-2012-3-page-495.htm
[1633] REVAULT d'ALLONES, Myriam, *Ce que l'homme fait à l'homme. Essai sur le mal politique*, Paris : Seuil, 1995, 176 p.
[1634] JUROVICS Yann, « Le crime contre l'humanité, définition et contexte », *Les Cahiers de la Justice*, 2011/1 (N° 1), p. 45-64.
[1635] BIOY, Xavier « Le corps humain et la dignité », *Cahiers de la recherche sur les droits fondamentaux*, 15, 2017, http://journals.openedition.org/crdf/541
[1636] MESURE ,Sylvie, « Dignité et société. Approche sociologique et critique », *Raisons politiques*, 2017/2 (N° 66), p. 211-224. https://www.cairn.info/revue-raisons-politiques-2017-2-page-211.htm
[1637] BUTLER, Judith, WORMS, Frédéric, *The Livable and the unlivable*, Fordham University Press, 2023, 96 p.
[1638] HONNETH, Axel, « Intégrité et mépris, Principes d'une morale de la reconnaissance », *Recherches sociologiques*, 1999/2, p.11-22

qui les exilés et les parias se retrouvent donc dénués de leur dignité et de leurs droits[1639]. Mais bien plus encore, elle possède une portée politique, il peut s'agir d'exprimer la dignité d'un collectif. Les marches pour la dignité expriment la volonté d'un groupe social d'acquérir une forme de reconnaissance de ses droits, de sa légitimité[1640]. La notion de dignité devient un slogan politique. Et comme l'écrit Cynthia Fleury : « un vent de radicalité souffle sur le concept de dignité, alors même que celui de reconnaissance trahit — peut-être — encore le désir sourd, ou la nécessité, d'être estimé par l'autre. »[1641]

Le philosophe Norman Ajari rejoint cette lecture critique de la notion, en renforçant sa facette postcoloniale. Il pointe les limites d'une définition de la dignité fondée sur la notion de reconnaissance, qui serait pour lui trop proche d'un acte d'assimilation : « La reconnaissance asymétrique, c'est l'assimilation : l'abolition d'une différence forte au profit d'une différence minimale qui, en dernière instance, vise à la conservation de l'identité première de la communauté. »[1642] Et il critique donc à l'acception libérale de la dignité, qui exclurait une part des marginaux et gommerait la dimension subversive de la notion : « La postulation de la pureté et de la désirabilité du modèle démocratique européen est un biais qui rend aveugle aux violences qui s'y déploient et l'omniprésence de la notion de « dignité » dans les constitutions des États modernes apparaît alors comme un instrument pour en étouffer la dimension scandaleuse et mobilisatrice, pour en émousser la radicalité. La dignité des constitutions et celle des émeutes portent le même nom ; elles ne charrient pas pour autant le même concept ni ne suscitent les mêmes manières d'exister. »[1643]

La lecture de la notion de dignité par Norman Ajari fait écho à celle d'Hélène Thomas. Pour la chercheuse, utiliser la notion de dignité pour revendiquer le respect des droits de l'homme ce serait prendre le risque de les dépolitiser. Ils seraient vidés de leur contenu et d'exclure les non-citoyens au nom d'un universel abstrait[1644]. Et ce alors que ce principe a une place centrale dans certaines architectures juridiques, comme c'est le cas dans la loi Fondamentale allemande. En effet, la notion de dignité y sert de garantie à l'exercice de différents droits de

[1639]« la conception des droits de l'homme s'est effondrée au moment même où ceux qui prétendaient y croire ont été confrontés pour la première fois à des personnes qui avaient effectivement perdu toutes leurs autres qualités et relations spécifiques, à l'exception du fait qu'elles étaient toujours humaines. Le monde n'a rien trouvé de sacré dans la nudité abstraite de l'être humain. » ARENDT Hannah, *L'impérialisme, Les origines du totalitarisme*, Paris, Quarto Gallimard, 2002, p. 603.

[1640] MARTIG, Alexis, *La Reconnaissance sociale et le Mouvement des Sans Terre au Brésil : en quête de dignité*, Paris, Academia/L'Harmattan, coll. « Anthropologie prospective », 2014, 290 p.

[1641] CYNTHA, Fleury, *La Clinique de la dignité*, Paris, Seuil, 2023, P.21

[1642] NORMAN, Ajari, *La Dignité ou la mort. Éthique et politique de la race*, Paris, Éd. La Découverte, coll. Les Empêcheurs de penser en rond, 2019,p.257

[1643] NORMAN, Ajari, ibid, p.63

[1644] THOMAS, Hélène, *Les vulnérables : la démocratie contre les pauvres*, Paris, Éditions du Croquant, 2010, 254 p

la personne[1645]. Et si des droits fondamentaux peuvent être mis en balance[1646], ce n'est pas le cas de la dignité humaine qui est dans la loi Fondamentale allemande intangible.

Or le principe de dignité est associé, toujours dans la loi Fondamentale allemande, à l'autodétermination informationnelle. Cette dernière prend en effet racine dans la combinaison des articles 1 et 2 de la Loi Fondamentale. Pour rappel l'art. 2 garantit le libre épanouissement de sa personnalité, l'art.1 proclame l'intangibilité de la dignité humaine. Ainsi, la loi de 1983 définit l'autodétermination informationnelle comme le droit pour chacun de contrôler la divulgation et l'utilisation de ses données personnelles et, en conséquence, celui de décider quand et à l'intérieur de quelles limites les circonstances de sa vie personnelle peuvent être rendues publiques (Arrêt « Volkzählungsgesetz »)[1647]. Et comme le rappellent Antoinette de Rouvroy et Yves Poullet : « les grands principes de la protection des données découlent directement de ces deux dispositions constitutionnelles qui consacrent la valeur de l'autonomie (autodétermination) et l'incommensurabilité (dignité) de chaque personne dans la société. Plus précisément, le régime de protection des données est un outil permettant de garantir ces valeurs fondamentales et doit être interprété à la lumière de ces valeurs. »[1648]

Toutefois, précisons que la consécration de l'autodétermination informationnelle traduit la sensibilité des Allemands au droit à la vie privée[1649], cela ne signifie pas que ce principe laisse une totale licence quant à l'usage de ses données[1650]. L'autodétermination informationnelle est protégée par le caractère intangible du principe de dignité, mais les restrictions de ce droit doivent être uniquement fondées sur un intérêt général majeur et s'appuyer sur une base juridique conforme à la loi Fondamentale allemande.

Ce lien entre dignité et autodétermination informationnelle se retrouve chez Shoshana Zuboff. La réification de l'internaute est analysée de façon extensive par l'auteure dans son ouvrage phare dédié à l'étude du capitalisme de surveillance. Et sa conception du pouvoir « instrumentarien » est directement liée au système éthique kantien, fondé sur l'impératif

---

[1645] Art 1. 1) la dignité de l'être humain est intangible.Tous les pouvoirs publics ont l'obligation de la respecter et de la protéger. 2) En conséquence, le peuple allemand reconnait à l'être humain des droits inviolables et inaliénables comme fondement de toute communauté humaine, de la paix et de la justice dans le monde 3)Les droits fondamentaux énoncés ci-après lient les pouvoirs législatifs, exécutif et judiciaire à titre de droit directement applicable.
ENDERS, Christoph, "The Right to have Rights:The concept of human dignity in German Basic Law", *Revista de Estudos Constitucionais, Hermenêutica e Teoria do Direito (RECHTD),* 2(1): 1-8 janeiro-junho, 2010 – doi: 10.4013/rechtd.2010.21.0
ENDERS, C., "Human Dignity in Germany" In: BECCHI, P., MATHIS, K. (eds) *Handbook of Human Dignity in Europe*, Springer,2018 https://doi.org/10.1007/978-3-319-27830-8_14-1

[1646] Ainsi, l'article premier annexée à la Charte des droits fondamentaux de l'Union européenne précise : « La dignité de la personne humaine n'est pas seulement un droit fondamental en soi, mais constitue la base même des droits fondamentaux. […] Il en résulte, notamment, qu'aucun des droits inscrits dans cette Charte ne peut être utilisé pour porter atteinte à la dignité d'autrui ».

[1647] https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html

[1648] « the major data protection principles derive directly from these two Constitutional provisions that consecrate the value of autonomy (self-determination) and the incommensurability (dignity) of each person in the society. To be more precise, the Data Protection regime is a tool for ensuring those fundamental values and must be interpreted in light of those values. » ROUVROY, Antoinette, POULLET, Yves, « The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy. », In: GUTWIRTH, S., POULLET, Y., DE HERT, P., DE TERWANGNE, C., NOUWT, S. (eds), *Reinventing Data Protection?,* Springer, Dordrecht, 2009

[1649] LINHARDT, Dominique, « La "question informationnelle" éléments pour une sociologie politique des fichiers de police et de population en Allemagne et en France (années 1970 et 1980) », *Déviance et Société*, 2005/3 (Vol. 29), p. 259-272. https://www.cairn.info/revue-deviance-et-societe-2005-3-page-259.htm

[1650] Par exemple l'article 13 de la décision de 1983 précise qu'un individu ne peut pas avoir accès à ses données dans les cas suivants : 1. la fourniture des informations demandées compromettrait l'exécution légale des tâches incombant à l'organisme qui contrôle les données,2. la fourniture des informations demandées constituerait un danger pour la sécurité et l'ordre publics, ou porterait atteinte aux intérêts légitimes de la Fédération ou d'un Land,3. une disposition légale ou la nature des données exige que les données personnelles en question, ou le fait qu'elles soient enregistrées, soient gardées confidentielles, en particulier pour des raisons d'intérêts légitimes prépondérants de tiers.

catégorique de non-instrumentalisation d'autrui. Ce pouvoir s'attaque directement à l'autonomie des individus, protégée par ce que Shoshana Zuboff nomme « un sanctuaire »[1651] permettant le libre épanouissement de la personne[1652]. La conviction de Shohana Zuboff s'ancre dans l'ensemble du corpus juridique du droit de la vie privée qui laisse une bonne place à la notion de dignité. On en retrouve la trace dans le préambule de la Convention 108+ qui stipule : « qu'il est nécessaire de garantir la dignité humaine ainsi que la protection des droits de l'homme et des libertés fondamentales de toute personne, et, eu égard à la diversification, à l'intensification et à la mondialisation des traitements des données et des flux de données à caractère personnel, l'autonomie personnelle, fondée sur le droit de la personne de contrôler ses propres données à caractère personnel et le traitement qui en est fait. » On peut encore y lire que : « La dignité humaine requiert la mise en place de garanties lors du traitement de données à caractère personnel, afin que les individus ne soient pas traités comme de simples objets. » Le CEPD défend également le principe d'autodétermination informationnelle et la dignité des personnes. Dans le premier rapport de 2015, le CEPD défend l'idée que « La dignité de la personne humaine n'est pas seulement un droit fondamental en soi, mais aussi un fondement des libertés et des droits ultérieurs, y compris le droit à la vie privée et à la protection des données à caractère personnel. Les atteintes à la dignité peuvent inclure l'objectivation, lorsqu'une personne est traitée comme un outil au service de quelqu'un d'autre. »[1653]

Et pourtant, le RGPD mentionne le terme de « dignité » simplement de façon marginale dans l'article 88. Ce dernier porte sur le traitement de données dans le cadre du travail salarié. Mais il n'empêche que l'esprit du Règlement est, pour le philosophe Luciano Floridi, inspiré par la notion de dignité, notamment en raison des droits qu'il accorde aux personnes concernées, dont le consentement et donc une forme d'autodétermination informationnelle[1654]. Plus profondément, réfléchir sur la place de la dignité au sein du RGPD pose la question du statut du droit de la protection des données ainsi que son lien avec le droit à la vie privée. La forme que prend ce lien peut être discutée. Le droit de la protection des données peut être considéré comme un sous-ensemble de la vie privée. Ou bien l'on peut considérer qu'il s'agit de deux

---

[1651] « Les nouveaux maux auxquels nous sommes confrontés posent des défis au caractère sacré de l'individu, et je compte au premier rang de ces défis les droits élémentaires qui touchent à la souveraineté individuelle, y compris le droit au futur et le droit au sanctuaire. Chacun de ces droits invoque la revendication de l'agence individuelle et de l'autonomie personnelle en tant que conditions préalables essentielles à la liberté de volonté et au concept même d'ordre démocratique ». « The new harms we face entail challenges to the sanctity of the individual, and chief among these challenges I count the elemental rights that bear on individual sovereignty, including the right to the future tense and the right to sanctuary. Each of these rights invokes claims to individual agency and personal autonomy as essential prerequisites to freedom of will and to the very concept of democratic order. » ZUBOFF, Shoshana, the age of surveillance capitalism, the fight fo a human future at the new frontier of power, New York : PublicAffairs, 2019, ibid, p.57

"the freedom of will is the existential bone structure that carries the moral flesh of every promise, and my insistence on its integrity is not an indulgence in nostalgia or a random privileging of the pre-digital human story as somehow more truly human. This is the only kind of freedom that we can guarantee ourselves, no matter the weight of entropy or inertia, and irrespective of the forces and fears that attempt to collapse time into an eternity of shadowboxing now, and now, and now. These bones are the necessary condition for the possibility of civilization as a "moral milieu" that favors the dignity of the individual and respects the distinctly human capacities for dialogue and problem solving. Any person, idea, or practice that breaks these bones and tears this flesh robs us of a self-authored and we-authored future." ZUBOFF, Shoshana, Ibid, p. 313

[1652] ibid.

[1653] « The dignity of the human person is not only a fundamental right in itself but also is a foundation for subsequent freedoms and rights, including the rights to privacy and to the protection of personal data. Violations of dignity may include objectification, where a person is treated as a tool serving someone else's purposes. »

European Data protection supervisor, Towards a new digital ethics, data, dignity and technology, Opinion 4/2015

https://www.edps.europa.eu/sites/default/files/publication/15-09-11_data_ethics_en.pdf

[1654] FLORIDI, L. "On Human Dignity as a Foundation for the Right to Privacy", *Philos. Technol.* 29, 2016, p. 307–312 https://doi.org/10.1007/s13347-016-0220-8

droits distincts, mais se chevauchant, l'autodétermination informationnelle laissant la possibilité pour la personne concernée de communiquer ou non des informations, de préserver ainsi sa vie privée. La finalité du droit de la protection des données peut être plus large que le droit à la vie privée, et le droit à la vie privée dépasse une stricte dimension informationnelle et inclut la vie privée familiale et corporelle[1655].

Pour en venir à l'éthique humanitaire, il est évident que la notion de dignité y occupe une place non négligeable. On retrouve cette notion dans le DIH. Et elle fait écho au principe d'humanité, qui est au cœur de l'éthique humanitaire[1656]. Le terme de dignité signifie le fait d'accorder une attention à l'autre. Le respect de la dignité d'autrui implique donc de le reconnaitre en tant que personne, en tant qu'égal et non pas en tant que victime. Dans certaines interprétations, notamment chez Hugo Slim, la notion d'humanité est proche de celle de fraternité. Ce sentiment se traduit par une forme « sollicitude », Hugo Slim reprend cette notion à Ricoeur : « Notre sollicitude les uns envers les autres « révèle notre similitude » et constitue le moment « comme moi » et « toi aussi » où nous reconnaissons notre humanité commune et vulnérable avec quelqu'un d'autre qui souffre. »[1657] Cette attention à l'autre va de pair avec l'importance d'être proche de la victime, et l'acte humanitaire est défini comme relation. Il s'agit aussi de respecter la dignité d'autrui en ne le traitant pas comme une pure « victime » [1658]. L'humanitaire est décrit comme une rencontre « d'être humain à être humain ». Il est question « des "moments d'humanité partagée" et de "reconnaissance mutuelle" dans lesquels le travailleur humanitaire et la personne affectée se présentent tous deux ouvertement, donnant quelque chose d'eux-mêmes et recevant quelque chose l'un de l'autre. »[1659]

Le principe d'humanité est aussi au cœur du DIH. Son objet est de protéger les hommes de la barbarie de la guerre et de préserver leur dignité. En substance, le DIH compose avec la réalité de la guerre et essaye d'atténuer la souffrance des civils et des parties prenantes, notamment des soldats hors de combats et des prisonniers, qu'il faut préserver de tout traitement dégradant et humiliant[1660]. Il en serait même la raison d'être si on en croit le juriste Daniel

---

[1655] GPA, GTSP3 : La protection de la vie privée et la protection des données en tant que droits fondamentaux : exposé de faits, 05 /2022. https://globalprivacyassembly.org/wp-content/uploads/2022/05/PSWG3-Privacy-and-data-protection-as-fundamental-rights-A-narrative-FRA.pdf

[1656] The dignity principles in humanitarian ethics emphasize that enabling people to restore and achieve their dignity in the practical method of humanitarian programs is a moral obligation with deep roots in the principle of humanity itself »
SLIM, Hugo, *Humanitarian ethics : a guide to the morality of aid in war and disaster*, London : Hurst & Company, 2015, p.91.
FUH D. " Human Dignity ", In *Humanitarianism*, Leiden, The Netherlands: Brill. 2020 doi: https://doi.org/10.1163/9789004431140_041
BARNETT, Michael, *Empire of humanity a history of humanitarianism*, Cornell University Press, 2011, 296 p.

[1657] "Our solicitude for one another "reveals our similitude" and is the "like me" and "you too" moment when we recognize our common and vulnerable humanity with someone else who suffers. "SLIM, Hugo, *Humanitarian ethics : a guide to the morality of aid in war and disaster*, London : Hurst & Company, 2015,p.52

[1658] MCKNIGHT HASHEMI, Valérie, « L'identité des victimes et le respect de la dignité humaine : analyse terminologique », *La Revue internationale de la Croix Rouge*, n°876, 2009 https://international-review.icrc.org/fr/articles/lidentite-des-victimes-et-le-respect-de-la-dignite-humaine-analyse-terminologique

[1659] "moments of shared humanity" and "mutual recognition" in which the humanitarian worker and the affected person both present themselves openly, giving something of themselves and receiving something of each other." SLIM, Hugo, *Humanitarian ethics : a guide to the morality of aid in war and disaster*, London : Hurst & Company, 2015,p.151

[1660] Art 13 traitement humain des prisonniers « En particulier, aucun prisonnier de guerre ne pourra être soumis à une mutilation physique ou à une expérience médicale ou scientifique de quelque nature qu'elle soit qui ne serait pas justifiée par le traitement médical du prisonnier intéressé et qui ne serait pas dans son intérêt. » Article 14 - Respect de la personne des prisonniers Les prisonniers de guerre ont droit en toutes circonstances au respect de leur personne et de leur honneur. Les femmes doivent être traitées avec tous les égards dus à leur sexe et bénéficier en tous cas d'un traitement aussi favorable que celui qui est accordé aux hommes. Article 52 - Travaux dangereux ou humiliants Aucun prisonnier de guerre ne sera affecté à un travail pouvant être considéré comme humiliant pour un membre des forces armées de la Puissance détentrice. »

Thurer : « la raison d'être du droit international humanitaire et des droits de l'homme [....] vise à protéger les êtres humains contre les atteintes à leur dignité personnelle, qu'il s'agisse d'atteintes illégales au corps ou d'humiliations et d'abaissements de l'honneur, du respect de soi ou du bien-être mental d'une personne.»[1661] Le sens qui est ici donné au terme de « dignité » est bien spécifique. Il n'est pas considéré comme un principe métajuridique, comme une garantie d'avoir des droits, mais comme le fait d'être « traité de façon humaine ». Le DIH adopte le langage de l'humiliation[1662]. Le chapitre V est consacré à ce principe dans le sens où il porte sur le traitement des personnes civiles et des combattants hors de combat en définissant ce que doit être un « traitement humain » de ces derniers. D'ailleurs, certains articles mentionnent expressément le terme de dignité : le n° 88 sur les discriminations, le n° 90 sur la torture, le n° 93 sur les viols, le n° 98 sur les disparitions forcées. D'autres articles du chapitre V ne citent pas le terme de dignité, mais concernent directement ce principe. Ils portent sur l'esclavage, le travail forcé, les mutilations et les expériences médicales, scientifiques ou biologiques. Encore une fois, le concept de dignité est associé à celui d'humanité, sans faire référence à la notion d'autonomie ou au fait de pouvoir disposer de droits fondamentaux au développement de la personne. Il s'agit en sommes d'une définition « négative » de la dignité.

L'interprétation de la dignité dans le DIH se distingue donc de sa fonction métajuridique, garantissant le « droit d'avoir des droits » [1663] tel qu'il est développé au sein de la loi Fondamentale allemande. Cela est peut-être dû au fait qu'il existe toujours une certaine distance vis-à-vis des droits de l'homme dans l'humanitaire. Cela dit, le lien entre humanitaires et droits de l'homme est complexe[1664]. Les humanitaires ont pu prôner l'adoption de « rights based approach ». Cette prise en compte du droit des bénéficiaires découle également du glissement à la fin des années 1990 d'une action humanitaire strictement fondée sur les besoins à une action de secours fondée sur les droits, de type « right based approach » : « Fondée sur les droits de l'homme, la RBA est présentée comme centrée sur la victime et met l'accent sur la participation, la non-discrimination et la responsabilisation. Ces impératifs impliquent non seulement un devoir moral d'aider les victimes en temps de crise, mais aussi d'adopter une approche globale visant à prévenir les crises, les conflits et les violations des droits de l'homme. »[1665] Mais les humanitaires ne s'accordent pas sur la nécessité d'inclure ou non d'autres types de droits que le droit humanitaire ou le droit des réfugiés, le risque étant de politiser l'action humanitaire, contrevenant ainsi au principe de neutralité[1666].

Au-delà du DIH, on retrouve aussi chez les humanitaires une autre conception de la dignité, plus matérielle, cette dernière étant liée à la nécessité d'assurer aux bénéficiaires des

---

[1661] « the very raison d'être of international humanitarian law and human rights law, [….] is intended to shield human beings from outrages upon their personal dignity, whether such outrages are carried out by unlawfully attacking the body or by humiliating and debasing the honor, the self-respect or the mental well-being of a person. » THURER, Daniel, 'Dunant's pyramid: Thoughts on the "humanitarian space"', *International Review of the Red Cross*, Vol. 89, No. 865, March 2007, p. 47–61

[1662] KAUFMANN, Paulus, KUCH, Hannes, NEUHAEUSER, Christian, WEBSTER, Elaine (ed.) *Humiliation, Degradation, Deshumanization : Human Dignity violated*, Springer Dordrecht, 2010, 266p.

[1663] Ainsi l'article premier annexée à la Charte des droits fondamentaux de l'Union européenne précise : « La dignité de la personne humaine n'est pas seulement un droit fondamental en soi, mais constitue la base même des droits fondamentaux. […] Il en résulte, notamment, qu'aucun des droits inscrits dans cette Charte ne peut être utilisé pour porter atteinte à la dignité d'autrui ».

[1664] BARNETT, Michael (eds), *Humanitarianism and human rights, a world of differences?,* Cambridge University Press, 2020, 344 p.

[1665] « Based in human rights, RBA is presented as victim-centred, and emphasises participation, non-discrimination and responsibilisation. These imperatives imply not only a moral duty to aid victims in times of crisis, but also to take a comprehensive approach that aims to prevent crises, conflicts and human rights violations. » BORGREVINK, K., SANDVIK, K. B. « The afterlife of buzzwords: the journey of rights-based approaches through the humanitarian sector. » The International Journal of Human Rights, 26(2), 2022, p.285–305. https://doi.org/10.1080/13642987.2021.1916476

[1666] FERRIS, Elizabeth G, *The Politics of Protection: The Limits of Humanitarian Action,* Washington : Brookings Institution Press, 2011, p.359.

conditions de vie décentes. Et son respect va de pair avec le fait de leur assurer une existence satisfaisant les standards en vigueur dans le milieu, comme les principes Sphères[1667]. Le fait d'avoir ses besoins de base couverts permettrait aux bénéficiaires de regagner une forme d'autonomie. Être digne signifie la possibilité de retrouver une forme d'indépendance financière[1668]. Cette conception de la dignité est liée à un paradigme libéral, liant dignité et autonomie. Elle peut également faire écho avec la notion d'« encapacitation », et d'emporwerment associée à la possibilité pour un individu de mener des choix[1669]. Et il n'est donc pas étonnant que l'on retrouve de façon récurrente le terme de « dignité » au sujet des programmes de transfert monétaire[1670]. Cette interprétation libérale de l'empowerment est critiquée, notamment pour sa dimension normative et injonctive.

Ainsi, les chercheurs Arnaud Dandoy[1671] et Sofia Duran Cardenas proposent alors de repenser le cadre éthique humanitaire en décentrant la place accordée à la notion de dignité entendue selon une interprétation libérale et liée au principe d'autonomie, pour ce faire, ils proposent de s'appuyer davantage sur les théories du care[1672]. Il s'agirait aussi, comme nous invite à le faire Larissa Fast, de repenser le principe d'humanité à partir d'une conception plus relationnelle, dépassant son universalisme, qui gommerait les dynamiques socioculturelles[1673]. Il nous parait alors pertinent de s'appuyer sur ce cadre pour repenser le consentement de personnes vulnérabilisées dans le cadre du droit à la protection des données. Mais il nous semble que les humanitaires restent plutôt partagés entre le modèle libéral, valorisant l'autonomie du sujet, et un retour d'un prisme plus « paternaliste », centré sur le modèle de la confiance.

L'objectif des chapitres qui suivent est donc d'explorer la façon dont les humanitaires cherchent à garantir la dignité des bénéficiaires en prenant en compte les droits que leur accorde le droit de la protection des données, et notamment le droit à l'autodétermination informationnelle. Ce sera l'objet d'un premier chapitre, centré sur le consentement. Puis on verra comment « outiller » techniquement ce dernier, notamment grâce à des dispositifs

---

[1667] Le Manuel Sphère,La Charte humanitaire et les Standards minimum de l'intervention humanitaire, 2018, https://spherestandards.org/wp-content/uploads/Le-manuel-Sphere-2018-FR.pdf

[1668] MOSEL, Irina, HOLLOWAY, Kerrie, "Dignity and humanitarian action in displacement", *HGP Report*, March 2019, https://cdn.odi.org/media/documents/Dignity_synthesis_paper.pdf

[1669]« Dans la tradition féministe militante, l'empowerment désigne un processus continu et ouvert, orienté la transformation des rapports de genres et des inégalités de classes à travers la conscientisation des femmes et leurs mobilisations collectives politiques. Par contraste, pour les institutions de développement international orthodoxes qui adoptent pour la plupart une perspective néolibérale, le terme empowerment est plus ou moins restreint à sa dimension individuelle, à la capacité de mener des choix rationnels pour accroître son bien-être matériel. » BIEWENER, Carole, BACQUE, Marie-Hélène, « 4. *Empowerment*, développement et féminisme : entre projet de transformation sociale et néolibéralisme », dans : Marie-Hélène Bacqué éd., *La démocratie participative. Histoire et généalogie.* Paris, La Découverte, « Recherches », 2011, p. 82-101.

[1670] La dignité en action, données et enseignement clés sur l'assistance en espèces et coupons dans l'ensemble du mouvement de la Croix-Rouge et du Croissant-Rouge, IFRC, juin 2021 https://cash-hub.org/wp-content/uploads/sites/3/2022/02/FRENCH_Dignity-in-Action_Key-data-and-learning-on-CVA-from-across-the-RCRC-Movement.pdf

BURTON, Jo, « » Doing no harm » in the digital age: what the digitalization of cash means for humanitarian action", International review of the Red Cross, 2020, 102(913), p.43-73 https://international-review.icrc.org/sites/default/files/reviews-pdf/2021-03/doing-no-harm-digitalization-of-cash-humanitarian-action-913.pdf

DEVEREUX, S., JERE P. "Choice, dignity and empowerment" – cash and food transfers in Swaziland: an evaluation of Save the Children's emergency drought response", 2007/08, Final report, Institute of Development Studies and Save the Children UK. https://library.alnap.org/help-library/choice-dignity-and-empowerment-cash-and-food-transfers-in-swaziland

[1671] DANDOY, Arnaud, « L'éthique du care contre l'exceptionnalisme humanitaire », *Alternatives humanitaires*, n°5, Juillet 2017https://www.alternatives-humanitaires.org/fr/2017/07/03/lethique-care-contre-lexceptionnalisme-humanitaire/

[1672] DURAN CARDENAS, Sofia," l'aide humanitaire au prisme du care », *Alternatives humanitaires*, n°24, novembre 2023 https://www.alternatives-humanitaires.org/fr/2023/11/20/laide-humanitaire-au-prisme-du-care/

[1673] FAST, Larisa, « Unpacking the principle of humanity: Tensions and implications. » *International Review of the Red Cross, 97*(897-898), 2015, p. 111-131

techniques décentralisés. On abordera différents projets d'ONG humanitaire fondés sur le développement de blockchains afin de garantir la gestion des données par les bénéficiaires eux-mêmes et leur autonomie. Ces deux premiers chapitres nous permettront de rendre plus concrètes les limites d'un modèle libéral de la dignité, notamment du fait de fortes inégalités de pouvoir entre bénéficiaires et humanitaires. Puis dans notre dernier chapitre, on s'intéressera à une autre façon de penser la notion de dignité, qui ne repose plus sur l'autonomie des sujets, puisqu'on parlera de la dignité des morts. Effectivement, les morts ne sont plus tout à fait du côté du monde des humains, en tant que cadavres, ils sont dépourvus de personnalité juridique. Il est malgré tout nécessaire de prendre soin de leur dignité, leur préserver des droits. Assurer leur dignité passe notamment par le fait de s'assurer que les morts bénéficient d'une « belle mort », qui ne dérogent pas aux normes d'un groupe social, notamment le fait de garder un nom. Or un bon nombre de victimes de catastrophes ou de guerre sont des morts anonymes. Et il parait étrange que ce « travail des morts » soit effectué par des personnes consacrant leur existence à sauver des vies[1674], mais il se trouve que certaines ONG humanitaires ont pris en charge la difficile tâche d'identifier les corps de personnes décédées. On reviendra donc sur la façon dont elles envisagent leur mission comme une façon de défendre la dignité des morts. Et surtout, on précisera comment ce travail d'identification s'articule à un certain nombre d'enjeux en matière de protection des données, que ce soit la protection de la vie privée des morts ou bien celle de leurs proches.

[1674] LAQUEUR, W, Thomas, *Le travail des morts, une histoire culturelle des dépouilles mortelles*, Paris, Gallimard, 2018,928 p.

## Chapitre 06 — Paradoxe du consentement humanitaire et autodétermination informationnelle des personnes vulnérables

### Introduction de chapitre

Comment des personnes fuyant des guerres et des catastrophes peuvent-elles ne pas consentir lorsque des humanitaires leur demandent s'ils agréent ou non à un traitement de données dans le cadre d'une distribution alimentaire ? « L'éthique du consentement ne s'applique pas aux personnes qui meurent de faim» déplore le chercheur Mark Latonero[1675]. Et pourtant, le consentement reste dans une certaine mesure la base légale la plus utilisée, bien qu'elle ne soit pas « adaptée » au contexte de l'aide et que le RGPD comprend d'autres bases légales. Pour comprendre ce paradoxe apparent, il est nécessaire de préciser le concept de consentement, inscrit dans le droit à la protection des données dès 1995, et rattaché à la notion d'autodétermination informationnelle et donc au principe de dignité. Comprendre le soubassement éthique du consentement permet d'expliquer l'attachement des humanitaires pour le consentement, malgré toutes les difficultés qu'ils rencontrent lors de son recueil. On verra qu'elles sont dues à la fois à la nature du numérique et de l'humanitaire, et du public de l'aide, placé dans des situations vectrices de vulnérabilité.

### Section 1 — Consentement, philosophie morale et définition juridique

Les racines du consentement tel qu'on le trouve dans le RGPD proviennent tout d'abord de la philosophie morale et de l'éthique médicale. C'est à la fin de la Seconde guerre mondiale que ce principe se cristallise, lorsque les premiers principes de l'éthique médicale ont été formulés en réaction aux expérimentations de docteurs nazis sur des êtres humains[1676]. En effet, en 1947, le code de Nuremberg impose la nécessité de respecter l'autonomie du patient et son consentement[1677]. Mais il faut attendre la fin des années 1970 pour que s'effectue un travail de formalisation plus poussé, avec notamment un texte de référence en bioéthique, le rapport Belmont publié en 1979. Mais l'inscription du consentement dans le droit de la santé est encore plus tardive, et s'est faite en grande partie sous l'impulsion d'associations de malades,

---

[1675] « the ethics of consent don't apply for people who are starving. » LATONERO Mark, « Stop Surveillance Humanitarianism », *The New York Times*, 11/07/ 2019. https://www.nytimes.com/2019/07/11/opinion/data-humanitarian-aid.htm

[1676] Les premières formulations éthiques du consentement seraient antérieures et remonteraient à la fin du XIX avec l'émergence de la médecine expérimentale, comme l'a montré Grégoire Chamayou dans son ouvrage « Les corps vils ». La fin de la seconde guerre mondiale marque cependant un tournant sur ce sujet. CHAMAYOU, Grégoire, *Les corps vils, expérimenter sur les êtres humains au XVIIIème et au XIXème siècle,* Paris : la Découverte, 2014, 424 p.

[1677] « Le consentement volontaire du sujet humain est absolument essentiel. Cela veut dire que la personne concernée doit avoir la capacité légale de consentir ; qu'elle doit être placée en situation d'exercer un libre pouvoir de choix, sans intervention de quelque élément de force, de fraude, de contrainte, de supercherie, de duperie ou d'autres formes sournoises de contrainte ou de coercition ; et qu'elle doit avoir une connaissance et une compréhension suffisantes de ce que cela implique, de façon à lui permettre de prendre une décision éclairée. Ce dernier point demande que, avant d'accepter une décision positive par le sujet d'expérience, il lui soit fait connaître : la nature, la durée, et le but de l'expérience ; les méthodes et moyens par lesquels elle sera conduite ; tous les désagréments et risques qui peuvent être raisonnablement envisagés ; et les conséquences pour sa santé ou sa personne, qui pourraient possiblement advenir du fait de sa participation à l'expérience. L'obligation et la responsabilité d'apprécier la qualité du consentement incombent à chaque personne qui prend l'initiative de, dirige ou travaille à, l'expérience. Il s'agit d'une obligation et d'une responsabilité personnelle qui ne peuvent pas être déléguées impunément. « AMIEL, Philippe, *Des cobayes et des hommes : expérimentation sur l'être humain et justice,* Paris, Belles Lettres, 2011,344 p.

notamment Aides et Act Up. Ainsi, en France, le consentement n'est consacré qu'au début des années 2000 avec la loi sur les droits des malades du 4 mars 2002, ou loi Kouchner[1678].

L'inscription du consentement dans le droit de la protection des données est aussi relativement tardive. Ce principe n'étant entériné qu'à la fin des années 1990. Et en France, le consentement occupe d'abord une place marginale dans la loi informatique et libertés de 1978. Sa section 31(1) précise que l'accord exprès est nécessaire au traitement ou au stockage de données personnelles associées aux origines raciales, ou à des affiliations politiques, philosophiques ou religieuses. Le consentement ne concerne pas l'intégrité des données personnelles. C'est la législation allemande qui a été la première à accorder une large place à ce principe. L'acte fédéral de protection des données — voté en 1977 — n'autorise en effet le traitement de données qu'à deux conditions. Tout d'abord, le traitement doit être autorisé par la loi. Ensuite, le sujet du traitement doit avoir donné son consentement. L'autodétermination informationnelle est ensuite ancrée dans la Loi fondamentale allemande en 1983 qui lui donne une valeur forte, en le liant avec le principe de dignité.

Une autre étape est franchie dans la Directive européenne de 1995 : le consentement côtoie les cinq autres bases légales (contrat, intérêt vital, intérêt légitime, intérêt public, obligation légale). Toutefois, les différentes versions nationales de la Directive ne s'accordent pas sur la façon de définir ce dernier et notamment sur son caractère implicite ou non. C'est le RGPD qui va trancher et donner une définition plus restrictive du consentement : ce dernier doit être explicite. Sachant qu'un consentement implicite est traditionnellement équivalant à la phrase « qui ne dit mot consent », alors qu'un consentement explicite peut être formulé comme « si ce n'est pas oui, c'est non ». Ce caractère explicite signifie que le consentement doit se manifester de façon à être entendu et compris.

Le RGPD désigne donc dans son article 7 comme étant un consentement valide : « *toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement.* » Dans le RGPD, le consentement est décrit comme devant être libre, univoque, éclairé et spécifique. Ces quatre termes semblent profondément liés : comment imaginer un consentement libre qui n'est pas éclairé ? Est-il possible de s'assurer de la liberté d'un consentement sans qu'il soit explicitement exprimé ?

En guise de précision, citons le considérant 42 du RGPD qui rappelle que : « *le consentement ne devrait pas être considéré comme ayant été donné librement si la personne concernée ne dispose pas d'une véritable liberté de choix ou n'est pas en mesure de refuser ou de retirer son consentement sans subir de préjudice*. » Le règlement prévient dans son considérant 43 que « *Pour garantir que le consentement est donné librement, il convient que celui-ci ne constitue pas un fondement juridique valable pour le traitement de données à caractère personnel dans un cas particulier lorsqu'il existe un déséquilibre manifeste entre la personne concernée et le responsable du traitement. »* Dans le RGPD, le caractère libre du consentement est défini comme une absence de contrainte, de violence ou de coercition : « *En termes généraux, toute*

[1678] Le projet de loi a été présenté par Bernard Kouchner, ministre de la santé de l'époque, fondateur de Médecins du Monde.

*pression ou influence inappropriée exercée sur la personne concernée (pouvant se manifester de différentes façons) l'empêchant d'exercer sa volonté rendra le consentement non valable.* » ; « *Le consentement ne sera pas libre lorsque tout élément de contrainte, de pression ou d'incapacité d'exercer un véritable choix sera présent.* »[1679]

Il doit être également spécifique, et être donné pour une finalité précise de traitement, afin de limiter tout « détournement d'usage » (« function creep » en anglais). Les lignes directrices du G29 précisent que « la nécessité d'obtenir un consentement spécifique sert de garantie contre l'élargissement ou l'estompement progressif des fins auxquelles les données sont traitées après qu'une personne concernée a donné son consentement à la collecte initiale de ses données. »[1680]

Enfin, le consentement doit être également éclairé, il faut s'assurer que l'information peut être comprise par le sujet, qui, à partir de cette dernière, a la capacité de prendre une décision en connaissance de cause. Consentir nécessite de disposer d'une faculté de compréhension et de prise de décision. Le caractère éclairé du consentement va donc de pair avec la notion d'autonomie, tel qu'elle définit dans l'éthique médicale. Pour rappel, dans le rapport Belmont, l'autonomie est définie comme le fait d'une personne « capable de réfléchir sur ses objectifs personnels et de décider par elle-même d'agir conformément à cette réflexion. Ainsi, la philosophe Micheala Marzano rappelle que dans ce cas : « *l'autonomie renvoie toujours à la capacité d'un être humain d'assumer ses choix et de les justifier en s'appuyant sur une vision particulière du bien ; elle n'est pas, tout simplement, l'expression d'une vie subite et irréfléchie. Le consentement auquel on se réfère exprime ainsi un projet de gouvernement de soi et non pas seulement une protection contre l'ingérence d'un tiers.* »[1681]

La définition forte du consentement tel qu'elle est donnée par le RGPD est liée à la notion d'autodétermination informationnelle, consacrée par le droit germanique en 1983. Cette notion découle de deux premiers articles de la Loi fondamentale allemande[1682] protégeant la dignité de la personne et garantissant son libre épanouissement de son être [1683] . L'autodétermination informationnelle donc repose sur une conception fortement « personnaliste » de la protection des données, centrée sur l'individu et sa dignité. Puisque mes données me constituent comme une personne, il est donc légitime d'en maitriser l'usage. Contrairement à un paradigme patrimonial qui justifie un contrôle des données d'un sujet par un droit de propriété (laissant la possibilité de les monnayer), les données sont l'expression de l'individualité de cette dernière, de son image, de sa voix, de son corps.

Mais jusqu'où peut aller ce contrôle ? On ne peut maitriser l'intégralité des données nous concernant. C'est de façon spontanée que l'individu projette dans la société une certaine image de lui, une image captée par autrui, qui prend aussi un sens aux yeux de celui qui la

[1679] Groupe de travail « Article 29 » Lignes directrices sur le consentement au sens du règlement 2016/679 »,10 avril 2018. https://www.cnil.fr/sites/cnil/files/atoms/files/ldconsentement_wp259_rev_0.1_fr.pdf

[1680] Groupe de travail « Article 29 » Lignes directrices sur le consentement au sens du règlement 2016/679 »,10 avril 2018. https://www.cnil.fr/sites/cnil/files/atoms/files/ldconsentement_wp259_rev_0.1_fr.pdf

[1681] MARZANO, Maria Michela,*Je consens, donc je suis… Ethique de l'autonomie*, Presses universitaires de France, PUF, 2006,p.86.

[1682] Il s'agit de la constitution allemande établie pour l'Allemagne de l'Ouest depuis 1949 et pour l'Allemagne réunifiée depuis 1990.

[1683] ROBUSTELLI, Ludovica, « Le droit à l'autodétermination informationnelle en droit européen », thèse de doctorat, Université Grenoble Alpes, Droit européen, 2022

traite. Comment maitriser des données liées à l'apparence physique, au genre, et à d'autres signes extérieurs ?

Ensuite, le droit à la protection des données n'est pas absolu. Le droit à la vie privée est toujours en tension avec différents droits, droit à la santé, à la sécurité. Et l'interprétation personnaliste du droit à la protection des données reste critiquée par certains chercheurs. Par exemple, pour Yves Poullet et Antoinette Rouvroy, le droit à la vie privée doit rester fonctionnel, c'est-à-dire permettre la réalisation de certaines libertés nécessaires au bon fonctionnement d'une démocratie. Ils en font une valeur instrumentale, qui constitue un outil servant à la préservation et à la promotion de valeurs fondamentales plus essentielles : le développement de soi et la participation politique. Cette interprétation de l'autodétermination informationnelle est propre à la doctrine de la Cour fédérale allemande[1684].

Ajoutons qu'il existe d'autres interprétations de l'autodétermination informationnelle qui lui redonnent une dimension politique et collective. Pour Luciano Floridi, il est nécessaire de dépasser l'ancrage libéral de la dignité qui imprègne une partie du droit à la protection des données, il est nécessaire de se distancier d'une approche anthropocentrée de la dignité, bien que cela puisse paraitre paradoxal, puisque le droit à la vie privée est un droit de la personne. Il en donne une première piste en défendant une conception « anthropo-eccentriste » de la dignité, en concevant la personne humaine comme plurielle et relationnelle[1685]. De surcroit, l'idée d'une maitrise de ses données peut s'inscrire dans des luttes collectives. Retrouver une forme de souveraineté est au cœur de plusieurs initiatives portées par des peuples indigènes

[1684] Le droit à l'autodétermination informationnelle est associé à deux articles de la Loi Fondamentale : l'art. 1, garantissant le respect de la dignité humaine, et l'art.2, garantissant le droit d'agir librement. Ceci fait que le droit à l'autodétermination informationnelle devient un droit fondamental. Toute personne peut choisir si et à qui elle transmet des informations personnelles.
« If he reckons that participation in an assembly or a citizens' initiative will be registered officially and that personal risks might result from it, he may possibly renounce the exercise of his respective rights. This would not only impact his chances of development but would have also impact the common good ("*Gemeinwohl*"), because self-determination is an elementary functional condition of a free democratic society based on its citizen's capacity to act and to cooperate », « S'il estime que la participation à une assemblée ou à une initiative citoyenne sera enregistrée officiellement et que des risques personnels peuvent en résulter, il peut éventuellement renoncer à l'exercice de ses droits respectifs. Cela aurait non seulement un impact sur ses chances de développement, mais aussi sur le bien commun ("Gemeinwohl"), car l'autodétermination est une condition fonctionnelle élémentaire d'une société démocratique libre fondée sur la capacité de ses citoyens à agir et à coopérer. »
ROUVROY, A., POULLET, Y., « The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy. », In: GUTWIRTH, S., POULLET, Y., DE HERT, P., DE TERWANGNE, C., NOUWT, S. (eds) *Reinventing Data Protection ?*. Dordrecht : Springer, 2009,p. 45-76

[1685]Il cherche à défendre une conception « anthropo-eccentriste » de la dignité, en concevant la personne humaine comme plurielle et relationnelle. Il se sert pour ceci le terme de polytrope (désignant dans la littérature grecque Ulysse) : n tant que voyageurs, nous sommes entre les mains de nos hôtes : les autres, la nature, le monde physique, mais aussi la société, la culture, le monde que nous construisons, et pas seulement celui que nous trouvons. (…) Ainsi, la dignité humaine, comprise en termes de polytropie, fournit la base anthropo-eccentrique pour le droit à la vie privée et le contrôle individuel sur nos propres informations constitutives. L'essentiel de notre moi, compris comme un récit, est écrit par d'autres auteurs. écrits par d'autres auteurs, ce qu'il reste à chacun d'entre nous à contribuer doit être soigneusement protégé et encouragé. soigneusement protégé et encouragé "As travellers, we are in the hands of our hosts: the others, nature, the physical world, but also society, culture, the world we build, not just the world we find. None of us is ever at the centre, we endlessly travel from centre to centre Thus, human dignity, understood in terms of polytropy, provides the anthropo-eccentric ground for the right to privacy and individual control over our own constitutive information. Most of our selves, understood as narratives, are written by other authors, what is left to the each of us to contribute must be carefully protected and fostered." FLORIDI, L. "On Human Dignity as a Foundation for the Right to Privacy", *Philos. Technol.* 29, 2016, p. 307–312 https://doi.org/10.1007/s13347-016-0220-8

(au Canada, Australie, Nouvelle-Zélande, etc.). La finalité de ces initiatives étant alors de sortir de gouvernances informationnelles héritées de la mise en nombre de peuples colonisés[1686].

Les lignes qui suivent feront référence à des legs coloniaux et leur répercussion en matière d'autodétermination informationnelle, mais à l'échelle individuelle. On s'intéressera aux voies d'autonomisation se jouant non pas au sein d'un groupe social, mais à la hauteur de personnes, jugées vulnérables, fortement dépendantes de l'aide apportée par les ONG. Cela nécessite de creuser la question du consentement dans des contextes de fortes inégalités de pouvoir. Or, ne consent pas un individu qui est forcé d'accepter une situation contre sa propre volonté. Et ce alors qu'il subit des rapports de pouvoir ou qu'il est placé dans une position de dépendance. Mais comment déterminer l'absence de contraintes ? À vrai dire, il existe toujours une forme minimale de contrainte au sein du consentement. On ne consent pas lorsqu'on doit collecter des données de sa propre initiative pour les rendre publiques ensuite. D'ailleurs, selon le RGPD, les données de la personne concernée seront « contrôlées » dans une certaine mesure par le responsable de traitement, qui détermine les moyens et les finalités d'un traitement de données[1687]. Et il s'agit alors d'accepter une situation qui nous est présentée comme un état de fait et dont on n'est pas soi-même à l'origine. Geneviève Fraisse, philosophe féministe, pointe alors la dimension contradictoire du concept du consentement : « le consentement peut être interprété comme un bien, une qualité estimable de l'individu, ou comme un mal, un aveu de faiblesse du même individu. Prouver sa liberté ou tendre le dos pour se faire battre. La tension entre intériorité et extériorité du consentement nous montre aussi combien cette question ne saurait se régler simplement ». [1688] Consentir signifie donc adhérer à une proposition externe, en accord avec sa propre volonté. Elle résulte d'une délibération non contrainte, en toute connaissance de cause. Marie Anne Frison Roche différencie d'ailleurs ce qu'elle nomme un « consentement pur » et un consentement découlant de sa volonté[1689].

Cette approbation peut cependant résulter non pas d'un acte de volonté pur, mais d'une intériorisation de dominations. Il arrive qu'on adhère aux formes d'hégémonies existantes, qu'on nie leur existence, et qu'on en ait plus conscience. Sachant que cette inconscience apparente peut être fluctuante, changeante[1690]. Il est aussi possible de persuader une personne, de faire en sorte qu'elle accepte une situation qui lui faisait auparavant violence. Obtenir le consentement peut signifier qu'un sujet passe d'une opposition initiale à l'assentiment. Cette transition ne résulte pas nécessairement d'un acte de contrainte, mais de persuasion. Or, le RGPD et les lignes directrices du groupe de l'article 29 sont clairs : un

---

[1686] GENTELET, Karine, BAHARY-DIONNE, Alexandra, « Stratégies des Premiers Peuples au Canada concernant les données numériques : décolonisation et souveraineté », *tic&société*, Vol. 15, N° 1 | 1er2021 http://journals.openedition.org/ticetsociete/6063
RABOUAM, Célestine, "Le stockage et le contrôle des données au Nunavut : un outil politique et économique pour les organisations Inuites", Conférence "la donnée comme ressource stratégique dans les conflits contemporains, 6 et 7 juin, Observatoire des conflits multidimensionnels de la Chaire Raoul-Dandurand

[1687] Il s'agit même de la définition d'un responsable de traitement, qui est décrit comme suit par la CNIL : « le responsable de traitement est la personne morale (entreprise, commune, etc.) ou physique qui détermine les finalités et les moyens d'un traitement, c'est-à-dire l'objectif et la façon de le réaliser. » https://www.cnil.fr/fr/definition/responsable-de-traitement

[1688] FRAISSE, Genièvre, *Du consentement*, Paris : édition Du seuil, 2017, p.22

[1689] FRISON ROCHE, Marie Anne, « Oui au principe de la volonté, Non aux consentements purs », document de travail pour une contribution aux Mélanges dédiés à Pierre Godé, 2018, http://mafr.fr/fr/article/oui-au-principe-de-la-volonte-non-aux-consentement/

[1690] COSTE, Florent, COSTEY, Paul, TANGY, Lucie, « Consentir : domination, consentement et déni », *Tracés. Revue de Sciences humaines*, 14, 2008, http://journals.openedition.org/traces/365

consentement obtenu par une forme d'« influence inappropriée » n'est pas valable. Cela dit, le sens du terme « inapproprié » n'est pas précisé. Pour compliquer les choses, ajoutons qu'il est aussi possible de consentir à une situation d'oppression et d'agir contre soi en toute conscience. L'acceptation de son destin est même considérée selon les préceptes stoïques comme une marque de force morale. Consentir volontairement à une forme de domination exprimerait une forme de dignité, de contrôle sur soi[1691]. Le cas contraire est également violent. Il arrive qu'on retire le droit au consentement d'une personne au nom de son bien, de sa dignité, comme cela peut être le cas lors d'hospitalisation psychiatrique sous contrainte. Un sujet encore d'actualité[1692].

Il nous vient alors une question : qu'en est-il du consentement pour des personnes n'étant pas autonomes ? Il peut s'agir de personnes vulnérables, subissant des formes de dominations et de dépendances, ne disposant pas de leur libre arbitre. L'éthique médicale donne des éléments de réponse à ces interrogations. Les médecins sont en effet aux prises quotidiennement avec le consentement à l'acte médical au sein des relations inégales qui les lient à leurs patients. Ces enjeux sont les plus brulants (et brutaux) pour des personnes vulnérables[1693], dont on considère qu'ils ne disposent pas ou plus d'une rationalité complète : les enfants, les personnes âgées, les personnes atteintes de troubles psychiques et mentaux[1694]. Chaque groupe de personnes présente ses propres traits de vulnérabilité, influant de façon spécifique sur la possibilité de recueillir leur consentement. On retiendra que souvent il n'existe pas de situation binaire. Qu'on ne peut pas opposer une pleine prise en compte du consentement à l'imposition unilatérale d'un acte sans prise en compte de la volonté de la personne. Par exemple, au sujet des personnes majeures placées sous protection, le Comité national consultatif d'éthique conseille, en cas d'impossibilité de recueillir le consentement, de rechercher l'assentiment du patient. Il désigne par là des formes plus « subtiles et moins formelles d'une certaine volonté », et comme une forme de « consentement atténué ». Il peut s'exprimer de façon non verbale, comme un indice plus faiblement perceptible de consentement[1695]. Et cela est bien le problème : l'assentiment étant de l'ordre de l'imperceptible, le recueillir peut dépendre de la sensibilité, de l'écoute du médecin, et être hautement subjectif.

Si l'on revient au RGPD, ce sont les responsables de traitement qui ont la tâche de s'assurer que le consentement est libre. Ils doivent être certains que le choix de la personne concernée est libre et affirmé. Or le consentement explicitement signifié n'est pas forcément le signe d'un acte autonome et libre, et n'implique pas nécessairement une adhésion complète. On peut se rapporter aux réflexions de James C. Scott opposant un texte public, produit par les

---

[1691] MONET, Éric, « Faiblesse de volonté et consentement. À partir de *Agir contre soi* de Jon Elster », *Tracés. Revue de Sciences humaines*, 14, 2008, http://journals.openedition.org/traces/399

[1692] Hospimedia, « Psychiatrie : l'objectif de réduction des soins sans consentement n'est pas atteint », 12/07/2022 https://www.hospimedia.fr/actualite/articles/20220712-psychiatrie-l-objectif-de-reduction-des-soins-sans

[1693] VERON, Paul, « Les décisions de soins en contexte de vulnérabilité : quels arbitrages du droit entre autonomie et contrainte ? Commentaire », *Sciences sociales et santé*, 2020/2 (Vol. 38), p. 67-75. https://www-cairn-info.ezproxy.utc.fr/revue-sciences-sociales-et-sante-2020-2-page-67.htm

Avis sur le consentement des personnes vulnérables, NOR : CDHX1513727V, JORF n°0158 du 10 juillet 2015, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000030862460

[1694] PECHILLON, Éric, DAVID, Michel, « Du consentement et du programme de soin », *L'information psychiatrique*, 2018/2 (Volume 94), p. 143-145. https://www.cairn.info/revue-l-information-psychiatrique-2018-2-page-143.htm

EYRAUD, Benoît, VIDAL-NAQUET, Pierre, « Consentir sous tutelle. La place du consentement chez les majeurs placés sous mesures de protection », *Tracés. Revue de Sciences humaines*, 14, 2008, 103-127.

[1695] Comité consultatif national d'éthique, Avis n°136, « L'évolution des enjeux éthiques relatifs au consentement dans le soin », avril 2021 https://www.ccne-ethique.fr/sites/default/files/2021-07/Avis%20136.pdf

plus faibles pour donner le change, et un « texte caché », qui correspondrait à la vérité du sujet. Et au contraire, le silence est ambigu. Il donne libre cours à l'interprétation, et donc à la déformation et à l'imposition d'un consentement non réellement accepté, mais le silence peut être aussi la seule forme de résistance possible, notamment pour les « sans voix ». Gayatri Spivak se demandait si les subalternes peuvent parler. On peut renchérir : les subalternes peuvent-ils consentir ?

Que faire ? Faut-il renoncer au consentement dans le cas où le rapport de pouvoir est trop inégal ? Mais est-ce nécessairement renoncer à l'autonomie du sujet ? Cela parait en soi un paradoxe. Le consentement garantit de l'autonomie et la dignité du sujet. Mais en cas de rapport de force trop contraint, et concernant des sujets catégorisés comme vulnérables, il ne parait plus pouvoir être convoqué, ce qui risque de renforcer les inégalités existantes. Ce paradoxe est d'autant plus criant en contexte humanitaire.

## Section 2 — Licéité du traitement de données pour une ONG humanitaire : consentement et l'intérêt légitime

Il nous semble qu'il existe au sein des ONG de la solidarité internationale un « paradoxe du consentement ». En effet, on a pu constater que le consentement reste la base légale la plus utilisée et la plus valorisée. Or il apparait qu'elle n'est pas tout à fait adaptée au contexte de la solidarité internationale.

### § 1 — Le paradoxe du consentement dans l'humanitaire

Ce n'est que dans de rares cas que le recueil du consentement est tout à fait désinvesti de toute valeur et perçu comme une tâche purement administrative. De la « paperasse » en somme. Ainsi, ce geste serait, aux yeux d'un enquêté, en complet décalage avec l'action humanitaire. Ce dernier nous glisse lors d'un entretien que : « *le consentement au Mali, ou en Mauritanie, au milieu de nulle part, dans le désert, ça peut être lunaire, on va pas parler du RGPD dans la relation d'aide »*[1696]

Plus habituellement, c'est le discours opposé que l'on peut entendre. Recueillir le consentement permettrait de se conformer à une série de valeurs essentielles de l'action humanitaire. On peut ainsi lire dans un article que : « dans le contexte du développement et de l'aide humanitaire, le consentement éclairé réaffirme à la fois l'engagement à soutenir la dignité des bénéficiaires et le fait de "ne pas nuire" aux vulnérables, aux marginaux et aux personnes privées de leurs droits. » [1697] Il permettrait d'assurer la « dignité numérique » des

[1696] Entretien n° 35, OI 2, 14/05/2020

[1697] « In the context of international development and humanitarian assistance, informed consent for data collection both reaffirms the commitment to upholding the dignity of individuals who are served and to "doing no harm" especially to the vulnerable, marginalized, and disenfranchised. »
« How to Add Informed Consent to Your Responsible Data Practices », *ICTworks,* 15/05/2019
https://www.ictworks.org/informed-consent-responsible-data/

individus. Ce terme désigne alors le « renforcement de l'agence, de l'autonomie et de l'identité d'individus, ainsi que de communautés auxquels ils appartiennent par la collecte, le traitement et l'usage de données qui leur sont relatives et qui leur sont propres (ainsi que toute intervention utilisant ces données) dans une façon qui rend effectifs les droits humains et qui assure la sécurité humaine de ces individus et de leurs communautés. »[1698] On retrouve une mention de cette notion dans une conférence organisée par le CICR sur la « dignité numérique dans les conflits armés ». Les participants en viennent à conclure que « pour promouvoir la dignité numérique, les bénéficiaires de l'aide doivent être perçus comme des agents de données qui ont la maîtrise de leur identité et de leur anonymat numériques. »[1699]

Par conséquent, le consentement doit dépasser le simple acte de conformité au RGPD. Ainsi, dans un webinaire auquel nous avons assisté, un intervenant affirmait qu'il n'est pas question simplement que de « compliance » et qu'il est nécessaire de conserver « l'esprit du consentement » pour l'ensemble du travail humanitaire[1700].

Cependant, on va voir que la mise en œuvre du consentement pose problème aux humanitaires. Ce n'est que dans quelques entretiens que des enquêtés nous ont confié ne pas rencontrer de difficultés sur le recueil de ce dernier : *« Bah, moi j'aurais déjà l'impression que c'est fait de la manière la plus éthique possible, parce qu'il y a vraiment une… moi j'ai vu ça sur le terrain, y a le respect des individus, y a le consentement, y a toutes ces approches-là c'est certain. Moi ça me semble assez éthique. »*[1701] Ce type de discours est minoritaire ; la plupart des DPO nous ont, au contraire, partagé sur ce point leur difficulté, voire leur colère : « *Le consentement c'est un fiasco. Les équipes arrivent, obtiennent un consentement sans en informer de la finalité des données. Ce n'est pas un consentement informé*. »[1702]

Ces difficultés sont renforcées par ce qu'on avait noté au chapitre 2 : un manque de formation des DPO, et un bon nombre de points flous au sein du RGPD. D'où le fait que des DPO attendent des éclaircissements de la part des autorités de données sur le consentement : « *Aujourd'hui, il y a une grosse incompréhension des autres organisations qui n'ont pas compris ce qu'implique le consentement, et je pense que dans les mois ou les années à venir, on aura des éclaircissements de la CNIL ou d'autres autorités, qui vont nous expliquer que le consentement n'est pas applicable, à l'heure actuelle, tel qu'il est écrit sous le RGPD. »*[1703]

Ce constat est corroboré par différents travaux de recherches, portant sur des organisations internationales comme l'UNHCR[1704] ou encore le WFP. On peut lire dans un rapport du WFP

---

[1698] « the state when the agency, autonomy and identity of individuals, as well as the communities they are part of, is respected, enhanced and empowered through how data that is both derived from them and pertaining to them (inclusive of any interventions that utilise this data) are collected, handled, and employed in ways that realise the human rights and enhance the human security of these individuals and their communities » GOODMAN Ric,SCHOEMAKER, Emrys,MESSENGER, Chloe,STELLER, Rachael, "Review and analysis of identification and registration systems in protracted and recurrent crises, Development alternative incorporated", *Carabou Digital*, may 2020. https://assetify-dai.com/pdfs/BASIC%20MIS%20in%20Crises%20Full%20Report%20External%20Version.pdf

[1699] "to promote digital dignity, individuals who receive aid should be perceived as data agents who have agency over their digital identity and digital anonymity." Wilton Park, "Digital Dignity in Armed Conflict: A Roadmap for Principled Humanitarian Action in the Age of Digital Transformation", October 2019, www.wiltonpark.org.uk/wp-content/uploads/WP1698-Report.pdf

[1700] "How Can you truly manage informed consent in practice?", Cartong, November 2020. https://www.youtube.com/watch?v=jIeB-i5fWR0&list=PLDuxmnTc4fTroeNltntD8HaYrs6xHiuBG&index=6

[1701] Entretien n° 10, OI3, information manager Officer, 06/01/2020

[1702] Entretien n° 84, ONG1, DPO, ONG 5, 14/10/2022.

[1703] Entretien n° 7, OI2, DPO, 11/12/2019

[1704] PARAGI B., ALTAMIMI, A, «Caring control or controlling care? Double bind facilitated by biometrics between UNHCR and Syrian refugees in Jordan », *Society and Economy*, *44*(2), 2022, p.206-231. https://doi.org/10.1556/204.2021.00027

que « dans certains cas des bénéficiaires du WFP ont même semblé ne pas être au courant qu'ils avaient donné un quelconque consentement au fait de collecter, stocker et partager leurs données personnelles et des informations, et pourtant jusqu'au trois quarts des enquêtés ont affirmé qu'ils se sentaient à l'aise avec l'idée de partager des données personnelles avec le WFP. »[1705] Cependant, le gros de la littérature grise existante nous apprend peu de choses sur les causes des difficultés que rencontrent les humanitaires. C'est pourquoi les prochains paragraphes se proposent de mettre en lumière ces dernières en essayant de mieux déterminer les différentes racines du problème.

Un premier type de contrainte pesant sur le recueil du consentement est relative à la temporalité de l'humanitaire, à savoir l'urgence. Il se trouve que le considérant 46 du RGPD utilise ce terme pour parler de l'action humanitaire. Remarquons d'emblée que le considérant recommande de ne pas recourir à cette base légale dans ce genre de situation : « *Certains types de traitement peuvent être justifiés à la fois par des motifs importants d'intérêt public et par les intérêts vitaux de la personne concernée, par exemple lorsque le traitement est nécessaire à des fins humanitaires, y compris pour suivre des épidémies et leur propagation, ou dans les cas d'urgence humanitaire, notamment les situations de catastrophe naturelle et d'origine humaine.* »[1706]

Et effectivement, différents rapports mentionnent le fait que les humanitaires n'ont concrètement pas le temps de collecter le consentement des bénéficiaires de façon appropriée. Dans des situations d'urgence, il est également difficile d'anticiper tous les risques, et par principe de précaution certains DPO recommandent de minimiser la collecte de données au maximum. Afin de limiter les traces compromettantes et éviter de mettre en danger les bénéficiaires, certains DPO font parfois le choix d'éviter de recueillir le consentement par écrit, même si cela contrevient aux exigences de redevabilité.

Les crises sont en effet marquées par une forte instabilité, et par une évolution rapide des acteurs et de leurs relations, d'où des difficultés pour anticiper les différentes chaines d'échange de données. L'UNHCR a ainsi été accusé d'avoir recueilli des données de Rohingyas sans leur consentement éclairé. Or ces dernières ont été transmises au gouvernement du Bangladesh. Et ce dernier les a ensuite partagés avec le gouvernement birman, à l'origine des persécutions touchant les exilés (cf. chapitre 3). Encore une fois, les ONG peuvent ne pas avoir une vue sur le long terme de la situation et des risques existants. Il est difficile de communiquer sur l'ensemble des informations concernant un traitement. Et indubitablement, obtenir un consentement valide sur le long terme reste une gageure, en raison de la fluidité du contexte : « C'est particulièrement problématique concernant les États fragiles touchés par des conflits, dans ce cas la forme du futur gouvernement est incertaine, ainsi qu'à qui les bénéficiaires donnent leur consentement, les institutions ne sont pas encore établies, limitant la possibilité pour le responsable de traitement d'expliquer, et pour le bénéficiaire, la capacité

[1705] « In some cases, people served by WFP even appeared unaware that they had provided any form of consent to WFP about data usage. In Iraq, a quarter of beneficiaries reported in the phone survey that they had not given consent for WFP to collect, store and share their personal data and information, and yet over three quarters of respondents noted they felt comfortable with sharing personal data with WFP. » OEV/2020/002, Office of Evaluation, WFP evaluation Strategic," Evaluation of WFP's Use of Technology in Constrained Environments", Janvier 2022.https://docs.wfp.org/api/documents/WFP-0000136278/download/

[1706] Règlement UE 2016/67, Raison 46 https://www.privacy-regulation.eu/fr/r46.htm

de comprendre et de prendre une décision quant aux risques impliqués par un transfert de données. »[1707] Dans ce cas, il existe deux options. Une première option est de multiplier le recueil du consentement de façon itérative, ce qui semble fastidieux. Une deuxième option est d'établir un genre de « click wrap », soit un contrat dans lequel la personne concernée est encouragée de consentir pour une vaste quantité de données.

Théoriquement, dans des contextes de grande fluidité, et en cas d'autre échange d'information, il est nécessaire de réitérer le recueil du consentement des personnes concernées. Cela n'est pas toujours le cas dans les faits. Effectivement, pour certains enquêtés, ce type de procédure peut devenir fastidieux : « *c'est aussi une tension qui émerge avec le HCR, des ONG refusent de partager leurs données. Les bénéficiaires avaient donné leur consentement pour que leurs données soient partagées avec l'Organisation, pas le HCR. Ça demande que les messages d'information soient plus explicites aussi, et que le consentement soit explicite aussi, ce qui complexifie aussi les choses.* »[1708]

Cependant, toute crise humanitaire n'est pas caractérisée par une temporalité d'urgence. De nombreuses organisations projettent leur action dans un temps plus long. Les ONG montent des programmes d'intervention post-crise, des programmes de santé et de prévention, des programmes d'appui à des infrastructures hospitalières locales. Elles interviennent au sein de camps de réfugiés, dont Michel Agier avait décrit la temporalité suspendue[1709]. Il est alors possible de recueillir le consentement des bénéficiaires une fois la situation d'urgence stabilisée. Cela rejoint le positionnement de certains DPO, n'ayant pas une vision « absolutiste » du consentement. Son recueil ne peut se faire qu'au cas par cas, en prenant en compte si la situation est adaptée ou non au recueil de cette base légale. D'ailleurs, les bénéficiaires étant moins paralysés par l'urgence, et moins dépendants à l'aide disposeraient de plus de ressources pour librement consentir ou non au traitement de données les concernant.

Une deuxième difficulté que rencontrent les humanitaires est relative au caractère éclairé du consentement et à la nature de l'information communiquée aux personnes concernées. Ainsi, le responsable de traitement, selon le WG29, joue un rôle de médiation auprès des personnes concernées pour leur délivrer différents éléments d'information[1710]. Les explications fournies doivent être exhaustives, afin de ne pas limiter le formulaire de consentement à une case à cocher. Mais ces derniers doivent aussi être compréhensibles et adaptés aux personnes concernées. Cela dit, le RGPD ne détaille pas les modalités de communication des

[1707] « This is particularly problematic in fragile and conflict-affected states, where: It is unclear who will form the future government, and therefore to whom beneficiaries are providing their consent; Government systems are not yet established, limiting the data collector's ability to explain, and the beneficiary's ability to understand and make a decision regarding the risks involved in the data transfer » MESSENGER, Chloe, STELLER, Rachael, « Consent to Data Processing in Humanitarian and Development Contexts, Part 2: Beyond Consent », *DAI Global*, 21/01/2021 https://dai-global-digital.com/beyond-consent-why-seeking-consent-for-data-processing-can-be-problematic-in-humanitarian-and-development-contexts.html

[1708] Entretien n° 9, ONG3, DPO, 19/12/2019

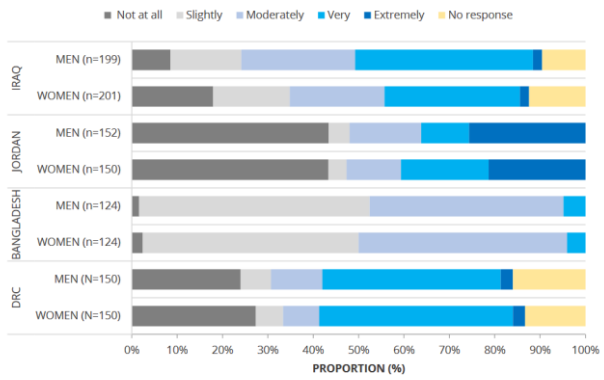
[1709] AGIER, Michel, « Urgence et attente », *Écrire l'histoire*, 16, 2016, http://journals.openedition.org/elh/1086

[1710] Le G29 précise que le responsable de traitement peut communiquer les informations suivantes : « identité du responsable du traitement, (ii) la finalité de chacune des opérations de traitement pour lesquelles le consentement est sollicité, (iii) les (types de) données collectées et utilisées, (iv) l'existence du droit de retirer son consentement, (v) des informations concernant l'utilisation des données pour la prise de décision automatisée conformément à l'article 22, paragraphe 2, point c), le cas échéant, et (vi) des informations sur les risques éventuels liés à la transmission des données en raison de l'absence de décision d'adéquation et de garanties appropriées telles que décrites à l'article 46. » « Lignes directrices sur le consentement au sens du règlement 2016/679 », Groupe de travail article 29 sur la protection des données. https://www.cnil.fr/sites/cnil/files/atoms/files/ldconsentement_wp259_rev_0.1_fr.pdf

informations. Dans les rapports du WG29, on peut lire que peuvent être employés de messages audio, vidéos, écrits, etc. Le seul prérequis consiste dans la clarté de l'information. En contexte humanitaire, il existe différentes façons de transmettre des messages aux bénéficiaires. Ces derniers peuvent être communiqués par des annonces, éventuellement faites au micro dans des « focal point », lors de consultations collectives, par l'affichage de posters, par l'enregistrement de messages préenregistrés, mais aussi plus classiquement via des formulaires.

Or, comme le tableau suivant — issu d'un rapport du WFP — le montre, le degré d'information des bénéficiaires varie grandement.

Figure 18: Degree to which beneficiaries are informed about the type and amount of personal information that WFP holds on them




ADE, case studies surveys

**DEGRE D'INFORMATION DES BENEFICIAIRES QUANT AU TYPE DE DONNEES QUE LE WFP DETIENT SUR EUX[1711].**

Ajoutons qu'il n'est pas toujours évident de prendre en compte les barrières linguistiques. L'UNHCR s'est attiré de nombreuses critiques sur ce point. L'organisation aurait distribué des formulaires rédigés en anglais dans des camps au Bangladesh, alors que cette langue n'est pas comprise par la majorité des réfugiés rohingyas [1712]. Il est en outre fréquent que les bénéficiaires soient analphabètes ou illettrés. Pour tenter d'atténuer ce risque, Oxfam a pu proposer l'usage de formulaires préenregistrés dans la langue native des bénéficiaires. Une gageure dans certains contextes : l'Afrique est par exemple caractérisée par une très forte diversité linguistique, qui peut être tempérée par des formes d'intercompréhensions entre ethnies.

Un autre point important concerne le type d'information à communiquer. Au-delà de la nature des données collectées, des finalités leur étant associées, il s'agit aussi d'informer les bénéficiaires sur l'action des ONG, son mandat déterminant l'utilisation des données. Or ce dernier peut faire l'objet de quiproquos, voire de rumeurs, qui peuvent être alimentées et renforcées par un défaut d'information. Il est donc essentiel pour les ONG de communiquer sur leurs actions : « *Ça dépend des cas… Y a de la mécompréhension de nos activités, donc il y*

[1711] OEV/2020/002, Office of Evaluation, "WFP evaluation Strategic Evaluation of WFP's Use of Technology in Constrained Environments", Janvier 2022.https://docs.wfp.org/api/documents/WFP-0000136278/download/

[1712]"UN Shared Rohingya Data Without Informed Consent", *Human Rights Watch*, 15/06/2021 https://www.hrw.org/news/2021/06/15/un-shared-rohingya-data-without-informed-consent

*a souvent de la peur de la part des personnes, qui ont été déplacées, du fait d'un conflit, que les données puissent être transmises à un gouvernement, et donc qui puissent se retrouver attaquées du fait de leur situation, y a cette chose-là, et ça demande un peu de temps, avant d'expliquer*. »[1713]

Pour faire court, un bon nombre de DPO s'inquiètent des limites du caractère éclairé du consentement. Ce point est confirmé par les recherches de la chercheuse Vicki Squire : « *Les migrants avec qui nous nous sommes entretenus ne savaient souvent pas très bien pourquoi leurs données avaient été collectées, à quelles fins et par qui elles seraient utilisées, et quels étaient leurs droits par rapport à ce sujet. La plupart décrivent le consentement comme oral ou parfois écrit, et si beaucoup reconnaissent que la collecte de données n'est pas obligatoire, ils semblent néanmoins souvent supposer que l'obtention d'une assistance est liée au fait de donner des données*. » Elle déclare plus loin que « *plusieurs migrants suggèrent qu'ils sont conscients que le consentement éclairé n'est pas pris correctement avant la collecte des données, et expliquent qu'ils ne peuvent rien y faire parce que se plaindre pourrait remettre en cause le fait de bénéficier d'une assistance*. » [1714]La chercheuse Dragana Kaurin a également décrit dans son travail d'enquête sur le HCR le manque de compréhension par les exilés de la nature du traitement des données par des organisations humanitaires[1715].

Ajoutons que l'importance que les bénéficiaires accordent au consentement varie grandement selon le contexte socioculturel. Tout d'abord, il est courant de lire que le consentement serait un concept « occidental », fondé sur la notion d'individu. Il semblerait que des bénéficiaires peuvent également désinvestir le recueil du consentement de toute valeur éthique. Ce dernier peut être perçu comme une tâche purement administrative, de la « paperasse » : « les énumérateurs comme les bénéficiaires considèrent le consentement comme étant une obligation ennuyeuse, bureaucratique et inutile d'origine occidentale, un préambule avant de commencer les choses sérieuses. »[1716] Cela dit, des enquêtes montrent au contraire que les bénéficiaires comprendraient les enjeux concernant le consentement, comme le montre le rapport du WFP[1717], sans expliciter les différences existant entre les terrains d'enquête[1718].

---

[1713] Entretien n° 10, OI3, information manager officer, 06/01/2020

[1714] *« The IDPs we spoke with were often unclear about why their data had been collected, for what purposes and by whom it would be used, and what their rights were in relation to the provision of data. Most describe consent as oral or sometimes written, and while many recognise that data collection is not compulsory, they nevertheless often seem to assume that the receipt of assistance is linked to the provision of data » « Several IDPs suggest that they are aware that informed consent is not taken properly before data collection, and explain there is nothing they can do about it because complaining about it may affect the assistance they receive.* » SQUIRE V. et. al.," Data and Displacement:Assessing the Practical and Ethical Implications of Data- Driven Humanitarianism for Internally Displaced Persons in Camp-Like Settings", Final Project Report, 2022 www.warwick.ac.uk/datadisplacement
SQUIRE, V., ALOZIE, M. « Coloniality and frictions: Data-driven humanitarianism in North-Eastern Nigeria and South Sudan », *Big Data & Society*, *10*(1), 2023https://doi.org/10.1177/20539517231163171

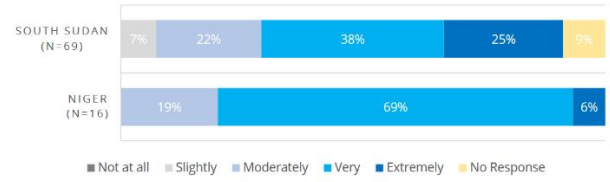
[1715] KAURIN, Dragana," Data Protection and Digital Agency for Refugees", World Refugee Council Research Paper No. 12, Mai 2019, https://www.cigionline.org/static/documents/documents/WRC%20Research%20Paper%20no.12.pdf

[1716] « Both the enumerator and the respondent see the consent part as an annoying bureaucratic useless Western-style obligation before the real thing starts. », "Consent' Examples for Mobile Data Collection?", the engine room mailing list, 07/04/2022. https://lists.theengineroom.org/lists/arc/responsible_data/2022-04/msg00013.html

[1717] OEV/2020/002, Office of Evaluation, "WFP evaluation Strategic Evaluation of WFP's Use of Technology in Constrained Environments", Janvier 2022.https://docs.wfp.org/api/documents/WFP-0000136278/download/

[1718] OEV/2020/002, Office of Evaluation, "WFP evaluation Strategic Evaluation of WFP's Use of Technology in Constrained Environments", Janvier 2022.https://docs.wfp.org/api/documents/WFP-0000136278/download/

Figure 24. Extent to which beneficiaries understood concepts such as informed consent, data protection, data privacy and data breaches




Source: ADE, case studies surveys.

**COMPREHENSION PAR LES BENEFICIAIRES DU WFP DE CONCEPTS PROPRES A LA PROTECTION DES DONNEES (CONSENTEMENT, VIE PRIVEE, FUITE DE DONNEES).** [1719]

En tout cas, il est clair qu'un facteur semble déterminant en matière de consentement : le degré de littératie numérique. Effectivement, pour un bon nombre de DPO, les bénéficiaires manquent de connaissance sur les NTIC. Cependant, il faut impérativement rappeler qu'il est difficile pour tout à chacun d'avoir une vision complète des flux de données transitant à travers nos ordinateurs et smartphones. Et à rebours d'un imaginaire de la transparence du numérique, le monde numérique serait au contraire caractérisé par une forte opacité. Il serait composé de multiples boites noires technologiques[1720]. Comprendre son fonctionnement est complexe et coûteux. Et au-delà de l'intériorité de la machine, de ses engrenages internes, l'opacité du numérique réside dans son extériorité, à savoir la complexité des flux d'échange de données qu'il permet, du fait de la multiplicité des lieux de stockages (Internet ubiquitaire, cloud), ou d'acteurs impliqués dans la chaine informationnelle.

En outre, l'opacité technologique fait également partie du modèle économique des entreprises du numérique (et notamment des GAFAM), fondé sur la privatisation de la connaissance, que ce soit par la prévalence de logiciels propriétaires, la multiplication de brevets, ou la défense du secret industriel[1721]. Rappelons que l'ensemble de l'exploitation des traces numériques repose sur des chaines d'acteurs multiples, dont les courtiers en données, peu visibles au grand public[1722]. Traduire cette complexité ne va pas de soi. Le temps de lecture des CGU d'Apple ou d'Amazon se compte en centaines d'heures. Shoshana Zuboff parle à ce sujet de « dé-contrat ». Toutes ces dysmétries informationnelles et ces déséquilibres de pouvoir sont au fondement du capitalisme informationnel dont parle la chercheuse. Ce dernier repose pour elle sur une privatisation du savoir. Cet accaparement fonctionne sur la coexistence de deux textes. Le premier, le plus visible, comprend l'ensemble de nos actions sur le Net, nos recherches Google, nos petits pouces laissés sur les réseaux. Le deuxième texte est, comme elle le baptise, un « texte fantôme », exploité par les « data analysts » et les concepteurs d'algorithmes de Google. Ces derniers forment ce que la chercheuse nomme un

[1719] OEV/2020/002, Office of Evaluation, "WFP evaluation Strategic Evaluation of WFP's Use of Technology in Constrained Environments", Janvier 2022.https://docs.wfp.org/api/documents/WFP-0000136278/download/

[1720] MASURE, Anthony, « Résister aux boîtes noires. Design et intelligences artificielles », Paris, Puf, *Cités*, n° 80, décembre 2019, anthonymasure.com/articles/2019-12-resister-boites-noires-design-intelligences-artificielles

« Plus les systèmes techniques prolifèrent, plus ils deviennent opaques, si bien que la croissance de la rationalité des moyens et des fins (...) se manifeste justement par l'accumulation successive de couches dont chacune rend les précédentes plus sombres. »

LATOUR, Bruno. « La fin des moyens », *Réseaux,* volume 18, n° 100, 2000, p. 39-58. https://doi.org/10.3406/reso.2000.2211

www.persee.fr/doc/reso_0751-7971_2000_num_18_100_2211

[1721] DURAND, Cédric, *Techno-féodalisme. Critique de l'économie numérique,* Paris : Éd. Zones, 2021, 256 pages

[1722] CRAIN, M. « the limits of transparency: Data brokers and commodification. » *New Media & Society*, 20(1), 2018, p.88–104. https://doi.org/10.1177/146144481665709

nouveau clergé. Google concentrerait donc à la fois les compétences, les ingénieurs, et les capacités de calcul et de traitement de données.

Au regard de cette opacité, il est peu probable que le consentement puisse être « éclairé », et cela est d'autant plus le cas pour des bénéficiaires d'ONG. Pour certains humanitaires, ces derniers n'auraient qu'une compréhension limitée des NTIC : « *Déjà nous quand on donne notre consentement, on sait pas trop à quoi on le donne, mais une personne au Congo, on lui dit, on collecte le point GPS de ta maison, alors déjà elle comprend pas grand-chose, ça n'a aucun sens, la compréhension est très compliquée… Y a du travail qui a été fait sur des choses simples, pour prendre une photo, ils reformulent les questions, c'était comme est ce que vous acceptez de donner votre photo à votre belle-mère ou à vos enfants, c'est intéressant, mais ça ne peut pas marcher pour tout.* »[1723]

Précisons toutefois que cette fracture numérique est nécessairement plurielle, touche inégalement les acteurs selon leurs appartenances sociales, les catégories générationnelles, genrées, etc. Évaluer les compétences numériques avant le recueil du consentement serait particulièrement complexe. Le terme de littératie numérique recoupe de multiples compétences et il peut en outre exister un hiatus entre la perception qu'on peut avoir de nos usages numériques et le manque de maitrise avéré des NTIC.

Il est clair qu'on peut nuancer l'inégalité de savoir verticale, opposant des acteurs occidentaux acculturés au numérique et des populations locales dépourvues de ce type de savoir[1724]. La difficulté d'appréhension de l'ensemble des flux numériques concerne à la fois les humanitaires et les bénéficiaires. Un rapport de Patrick Vinck est éclairant sur ce point[1725]. Il fait part d'un manque de littératie numérique et de formation du personnel d'ONG sur la protection des données, qui est de toute manière contrainte par la forte rotation du personnel. Il est donc justifié de nuancer l'inégalité de savoir verticale, opposant des acteurs occidentaux acculturés au numérique et des populations locales dépourvues de ce type de connaissance[1726].

En tout cas, pour acquérir une meilleure littératie numérique des organisations proposant des services de type H2H, comme Cartong, délivrent des formations de type webinaires ou portails de ressources[1727] ; et on a déjà évoqué dans le chapitre 2 la formation en matière de protection des données que propose l'université de Maastricht en partenariat avec le CICR. Des fablabs peuvent aussi remplir cette fonction, et certains lieux proposent d'être des espaces ouvert de création et d'apprentissage, accueillant des exilés comme des

[1723] Entretien n° 9, ONG 3, DPO, 19/12/2019.
[1724] FROST L, KHAN S, VINCK P.,"Technologies in Humanitarian Settings: Digital Upskilling of Humanitarian Actors", Harvard humanitarian initiative, 2022. https://hhi.harvard.edu/sites/hwpi.harvard.edu/files/humanitarianinitiative/files/digitalcasestudy_5_digitalliteracy_final.pdf?m=1672678941
[1725] DOWNER, Matthew, "Digital skills development for equitable and dignified humanitarian assistance", ITU Digital Skills Insights, 2021. https://academy.itu.int/sites/default/files/media2/file/21-00668_Digital-Skill-Insight-210831_CSD%20Edits%206_Accessible-HD.pdf
[1726] FROST L, KHAN S, VINCK P. "Technologies in Humanitarian Settings: Digital Upskilling of Humanitarian Actors", Harvard humanitarian initiative, 2022. https://hhi.harvard.edu/sites/hwpi.harvard.edu/files/humanitarianinitiative/files/digitalcasestudy_5_digitalliteracy_final.pdf?m=1672678941
[1727] "How to promote the right level of data literacy amongst your staff", GEONG, 2020 https://www.youtube.com/watch?v=cHJvz6ot668&list=PLDuxmnTc4fTroeNltntD8HaYrs6xHiuBG&index=7

bénévoles[1728]. D'autres personnes proposent de faire du recueil de consentement un espace d'apprentissage et d'échange sur le numérique[1729]. On gardera à l'esprit que la notion de « fracture numérique » a été critiquée pour son aspect normatif. Le chercheur Koen Leurs montre ainsi que chez les humanitaires, l'inclusion numérique est associée à la notion de « résilience », qu'il relie à un soubassement théorique libéral[1730]. Il propose une approche critique de cette dernière, en axant son analyse sur des pratiques d'« auto-média », d'ateliers participatifs visant à acquérir une pratique autonome du numérique.

S'acculturer au numérique permettrait donc de reprendre le contrôle de nos vies numériques. La motivation est d'ordre politique. L'objectif est de renverser un rapport de pouvoir entre individus et technologistes. Ce ne sont pas simplement d'enjeux strictement épistémologiques. L'objectif est de retrouver une forme d'indépendance et d'autonomie. Cependant, les chercheurs ne s'accordent pas sur ce que recouvre concrètement ce terme. Faut-il ou non apprendre à coder ? Quel degré d'érudition est-il nécessaire d'atteindre afin d'ouvrir la boite noire ? Est-ce que prôner la littératie numérique conduit à mettre de côté les racines des boites noires qui plongent en partie dans le capitalisme informationnel ? Les ambitions entourant la littératie numérique divergent. Il s'agit d'avoir un usage plus efficace du numérique, un usage plus critique, avoir une perception plus adéquate des risques, ou acquérir une plus grande confiance dans le numérique. Sachant qu'une solution est aussi de proposer une alternative « papier » aux NTIC afin de réduire les inégalités dues à la fracture numérique.

Et surtout, chaque outil technique porte en soi une série de caractéristiques techniques qui entraine des difficultés spécifiques en matière de consentement. Un premier exemple délicat concerne l'exploitation de données massive[1731]. En général, les données massives peuvent être anonymisées. Mais l'ampleur des traitements et la diversité des sources (données publiques, administratives, données collectées sur des réseaux sociaux) facilitent la réidentification des personnes. Des interrogations persistent donc sur la nécessité de collecter le consentement des personnes concernées dans ce type d'opération.

Pour illustrer cette problématique, prenons l'exemple d'Ushaidi, à savoir un logiciel de cartographie d'abord conçu afin de monitorer les violences postélectorales au Kenya en 2008.

---

[1728] DELLA-TORRE, Laetitia, « Formes horizontales d'organisation humanitaire. "Fablabs" et "Makerspaces" en Grèce pour l'aide aux réfugiés : réparer les vivants, réparer les choses », Master-2, mémoire, 19 janvier 2019, *Cahiers COSTECH* numéro 2. http://www.costech.utc.fr/CahiersCOSTECH/spip.php?article76

[1729] "How can you truly manage informed consent in practice?", GEONG, 2020 https://www.youtube.com/watch?v=jIeB-i5fWR0&list=PLDuxmnTc4fTroeNltntD8HaYrs6xHiuBG&index=6

[1730] LEURS, K. « Resilience and Digital Inclusion: The Digital Re-making of Vulnerability? », In: Tsatsou, P. (eds), *Vulnerable People and Digital Inclusion*, Palgrave Macmillan, 2022, 373 p.
GARRET, Paul Michael, "Questioning Tales of « Ordinary Magic »: 'Resilience' and Neo-Liberal Reasoning", *The British Journal of Social Work*, Volume 46, Issue 7, October 2016, p. 1909–1925, https://doi.org/10.1093/bjsw/bcv017

[1731] « Leur principe même de collecte massive rend extrêmement difficile le respect du consentement individuel de chaque personne concernée et, par construction, ne répond ni à une "finalité déterminée" ni à une logique de "proportionnalité" à une telle finalité. Au contraire, l'intérêt de la collecte et du traitement des *big data* réside dans l'infinie variété de leurs utilisations possibles, et les "réutilisations", si tant est que ce mot conserve un sens dès lors qu'il n'y a pas d'utilisation prédéfinie, interviennent elles aussi sans consentement de la personne concernée. Enfin, la conservation des données tend à être quasiment indéfinie. » DUBOIS, Jean-Pierre, « Nos droits face aux "*big data*" : quels enjeux, quels risques, quelles garanties ? », *Après-demain*, 2016/1 (N ° 37, NF), p. 6-9. https://www.cairn.info/revue-apres-demain-2016-1-page-6.htm
CEPD, avis n°7/2015, « Relever les défis des données massives, un appel à la transparence, au contrôle par l'utilisateur, à la protection des données dès la conception et à la reddition de comptes » https://www.edps.europa.eu/sites/default/files/publication/15-11-19_big_data_fr.pdf

Il a été massivement utilisé lors des opérations de crowdsourcing à Haïti. Ces dernières ont fait l'objet d'une couverture médiatique très enthousiaste, surlignant le potentiel d'organisations décentralisées, reposant sur l'« intelligence collective ». Et la date de 2010 aurait marqué une réelle rupture quant à l'ampleur du flux d'information à traiter. Patrick Meier raconte que plus de 2 millions de Tweets avec le mot « Haïti » ou « croix rouge » ont été publiés dans les 48 heures suivant le tremblement de terre. Parallèlement, un numéro d'urgence a été mis en place par la compagnie locale, Digicel, qui a envoyé un message d'information à ses abonnés (soit environ 1,4 million de personnes). Ces derniers étaient informés de l'opération de cartographie, et un numéro d'urgence, le 4636 permettait de faire remonter des appels d'urgence pour les équipes de « search and rescue ». Différentes métadonnées liées à leurs messages étaient ensuite publiées sur une carte gérée par Ushaidi.[1732] Cela dit, pour déterminer la base légale employée pour encadrer les données des utilisateurs du 4636, Patrick Meier ne s'est pas référé au RGPD. Le projet date de 2010 et a lieu dans un contexte extraeuropéen. Patrick Meier s'est alors inspiré du manuel de protection de données de l'OIM. Patrick Meier précise donc que : « dans la section "Consentement", le manuel énumère différentes façons d'obtenir le consentement. La plus *pertinente* dans le cadre de notre discussion est peut-être le "consentement implicite" : Ni un consentement oral ou écrit n'est obtenu, mais l'action ou l'inaction du sujet indique de façon non équivoque la participation volontaire à un projet de l'OIM. » [1733]

Le choix du consentement implicite est confirmé par un professeur de droit de la Fletcher School of Law and Diplomacy. Ce dernier a en effet été consulté pour déterminer si les messages SMS devaient ou non être publiés sur la carte[1734]. L'avis du professeur de droit est le suivant : le consentement implicite est une base légale adéquate, participer au projet est donc considéré comme un acte de consentement[1735]. Patrick Meier ajoute qu'il aurait été possible, mais couteux de recueillir le consentement explicite des personnes concernées. Ce choix n'a pas fait consensus. Patrick Meier le défend en arguant que : « certains diront (et l'ont fait) qu'il n'était pas pratique d'envoyer des SMS à tous les Haïtiens pour obtenir leur consentement, car nous fonctionnions déjà à une capacité bien supérieure et nous avions du mal à dormir pendant des jours. En effet, les deux principaux bénévoles de Fletcher chargés de filtrer les milliers de messages textuels et de répertorier les plus urgents ont rapidement été confrontés à un arriéré. Cette fonction pourrait peut-être être automatisée à l'avenir. »[1736]

---

[1732] MEIER, Patrick, « New information technologies and their impact on the humanitarian sector », *International Review of the Red Cross*, Vol. 93, N° 884, December 2011, p. 1239-1263. https://international-review.icrc.org/sites/default/files/irrc-884-meier.pdf

[1733] MEIER, Patrick, "On Crowdsourcing, Crisis Mapping and Data Protection Standards", *IRevolutions*, 05/02/2012. https://irevolutions.org/2012/02/05/iom-data-protection/
« In the section on "Consent", the manual lists various ways that consent can be acquired. Perhaps the most *a propos* to our discussion is "Implicit Consent:no oral declaration or written statement is obtained, but the action or inaction of the data subjects un-equivocally indicates voluntary participation in the IOM project. »

[1734] https://www.mission4636.org/access-to-data/

[1735] MEIER, Patrick, « Haiti: Lies, Damned Lies and Crisis Mapping »,*IRevolution*, 26/02/2013 https://irevolutions.org/2013/02/26/haiti-lies/

[1736]« some may argue (and indeed have) that texting every Haitian back for consent may not have been practical since we were already operating at way-beyond capacity and hardly getting any sleep for days on end. Indeed, the two main volunteers at Fletcher who were tasked with the job of filtering through thousands of text messages and mapping the most urgent ones were quickly facing a backlog. Perhaps this feature could be automated in the future » USHAIDI, "Crisis mapping Haiti : some final reflections, 14/10/2010 https://www.ushahidi.com/about/blog/crisis-mapping-haiti-some-final-reflections/

Patrick Meir ajoute que les personnes ont été informées de l'objectif du numéro d'urgence, notamment par des messages radiophoniques et qu'aucun haïtien ne se serait opposé au projet ou à ces opérations de collecte de données[1737]. Toutefois, la chercheuse Kate Crawford affirme que la population locale n'était pas toujours au courant des finalités d'usage du numéro d'urgence[1738]. Il n'empêche que pour Kate Crawford tout come Theodora Gazi, le consentement est la base de données légitime en cas de traitement de données massives[1739]. Or cette fracture de connaissance entre les humanitaires et les bénéficiaires peut être renforcée en cas d'usage d'outils de gestion à distance de crise, comme des agents conversationnels ou encore d'images satellitaires. Il est évident que les images satellitaires ne posent pas d'enjeu en matière de consentement des individus. Le cas est différent dans le cas des drones. Ces derniers peuvent être utilisés pour recueillir des données géographiques, lors d'exercices de cartographie. Un drone peut servir à collecter des données sur une zone précise, mais filmer (intentionnellement ou non) des individus s'y trouvant. S'agit-il de recueillir ou non leur consentement[1740] ? Le code de conduite des drones humanitaires recommande de se fonder (quand cela est possible) sur le consentement éclairé. Il est aussi préconisé de recueillir, stocker, partager et supprimer les données de façon responsable selon une approche fondée sur le besoin. Il conseille d'appliquer le consentement informé, quand cela est possible. Et enfin, il rappelle qu'il est nécessaire d'utiliser des mesures d'atténuation de risque quand le recueil du consentement n'est pas possible[1741]. Le guide sur la protection des données du CICR adopte un positionnement plus critique à l'égard du consentement. Il présente le recours à cette base légale pour le traitement de données de drones comme irréaliste, puisqu'il reste difficile de contrôler l'ensemble des personnes évoluant dans une zone de vol afin de les informer d'une opération de cartographie en cours. Le guide critique également l'idée de compter sur le consentement de la communauté. Cela irait en effet à l'encontre du cadre juridique (fondé sur l'individu). Il est donc conseillé de recourir à d'autres bases légales comme l'intérêt légitime.

---

[1737] MEIER, Patrick, « Haiti: Lies, Damned Lies and Crisis Mapping »,*IRevolution*, 26/02/2013 https://irevolutions.org/2013/02/26/haiti-lies/

[1738] CRAWFORD, Kate, MEGAN, Finn. "The Limits of Crisis Data: Analytical and Ethical Challenges of Using Social and Mobile Data to Understand Disasters." *GeoJournal*, vol. 80, no. 4, 2015, p. 491–502. *JSTOR*, http://www.jstor.org/stable/44076312. « For his Masters research, journalist and academic Jean- Yves Clémenzo went to Haiti where he had spent years as a journalist and conducted fifteen qualitative interview with people who had used the 4636 code. Clémenzo found that almost none spoke to had heard of Ushahidi, and were unaware that their messages were being made public, thy considered them private messages. »

[1739] « Les risques associés aux approches fondées sur les données massives ne peuvent pas toujours être connus à l'avance, et les communautés touchées par un désastre ne devraient pas être exposées à des dommages potentiels sans leur consentement. Nous devons nous demander : qui décide quand les avantages l'emportent sur les risques ? Qui assume la légitimité d'un traitement de données ? Si la réponse à cette question n'est pas donnée par la communauté locale, mais par des individus résidant loin de la région, cela soulève des problèmes éthiques significatifs. »

«The risks of big data approaches cannot always be known in advance, and communities experiencing a disaster should not be further exposed to potential harm without their consent. We could ask: who gets to decide when the benefits outweigh the risks? Who "assumes the legitimacy of processing"? When the answer to this question is not the community itself, but parties far from the affected region, this raises significant ethical problems. » CRAWFORD, Kate, MEGAN, Finn, "The Limits of Crisis Data: Analytical and Ethical Challenges of Using Social and Mobile Data to Understand Disasters." *GeoJournal*, vol. 80, no. 4, 2015, p. 491–502. http://www.jstor.org/stable/44076312.

GAZI, Theodora, GAZI, Alexandros," Humanitarian aid in the age of COVID-19: A review of big data crisis analytics and the General Data Protection Regulation."*International review of red cross,* n°913, March 2021

https://international-review.icrc.org/sites/default/files/reviews-pdf/2021-03/humanitarian-aid-covid-19-big-data-crisis-analytics-gdpr-913.pdf

[1740] MAIER, Patrick, « Humanitarian UAV/Drones in Conflict Zones: Fears, Concerns and Opportunities »,*IRevolutions*, 03/11/2014, https://irevolutions.org/2014/11/03/humanitarian-uavs-conflict-zones/

[1741] **«** Collect, store, share and discard data ethically using a needs-based approach, applying informed consent where possible and employing mitigation measures where it is not. » Uav code of conduct, https://uavcode.org/code-of-conduct/

JEYABALAN, V., DONNELLE, L., MEIER, P., NOUVET, E." To Obtain Informed Consent or Not to Obtain Informed Consent? Drones for Health Programs in the Grey Zone between Research and Public Health", *Drones, 7*, 2023, p. 247. https://doi.org/10.3390/drones7040247

Enfin, il nous reste un dernier point à examiner : le caractère libre du consentement dans un contexte de fortes inégalités de pouvoirs entre bénéficiaires et humanitaires. Il est indéniable qu'il existe une importante dépendance des bénéficiaires à l'égard des ONG. Ces dernières tentent d'assurer leur survie et remplir des besoins essentiels (nourriture, santé, éducation, etc.). En comparaison, le respect de la vie privée parait être un sujet secondaire. La survie peut passer avant la confidentialité. L'échange de mail suivant — lu sur une liste de diffusion — résume la situation : « Mon équipe est en train de conduire une enquête sur la conscience que les plus vulnérables réfugiés syriens ont des risques et des droits associés à la collecte de données. Dans tous les groupes de discussion, les réfugiés s'accordent tous à dire qu'ils seraient prêts à accepter absolument tout ce qu'on peut leur demander ou proposer pour trois raisons :

1. Ils ne sont pas au courant de ce que pourraient être les risques et ils ne sont pas au courant qu'ils peuvent bénéficier de droits concernant leurs données personnelles (la plupart sont illettrés, dans ce contexte).

2. Leur confiance aveugle comme nous sommes des ONG humanitaires venant à leur secours. Ils ne se figurent pas qu'on pourrait leur causer du tort.

3. Même si l'on insiste sur le fait que répondre à notre enquête n'est absolument pas lié à une future assistance, la simple idée qu'il puisse avoir la moindre chance qu'il existe un simple lien à ce sujet, dans le cas où l'on parlerait d'eux à quelqu'un, justifie le fait qu'ils pourraient consentir à la moindre chose pouvant leur donner une chance minime d'obtenir une forme minimale d'aide, comme leur situation est réellement insupportable. »[1742]

Autre point, les inégalités de pouvoir peuvent être internes aux sociétés locales. Il est important de prendre en compte les rapports de pouvoir au sein des groupes sociaux que forment les bénéficiaires, et notamment l'influence de ceux que les humanitaires qualifient de « leader communautaire ». En effet, les ONG peuvent avoir recours à des formes collectives de consentement, plus facile à recueillir que le consentement individuel[1743]. Dans ce cas, le recueil du consentement se ferait donc auprès du « leader communautaire », à condition de s'assurer qu'il est bien représentatif des intérêts et des sensibilités individuelles du groupe. Or, il est possible que peu de personnes souhaitent se démarquer des dynamiques de groupe en refusant de consentir. Il faut donc aussi être attentif aux personnes exclues des processus de décisions communautaires, comme peuvent l'être les femmes dans certains contextes.

---

[1742] « My team is running a study on the awareness of data-related risks and rights of the most vulnerable Syrian refugees in Lebanon. In all the focus group discussions, all the refugees agreed that they would agree to absolutely anything we ask/propose them for three reasons:
1. They are not aware there might be any risk and they are even less aware that there exists a notion of rights about personal data (most are illiterate, in this context).
2. They blindly trust us as we are humanitarian NGOs here to help and they don't picture why we would do something harmful to them.
3. Even if we insist on the fact that answering our surveys is absolutely not connected to any future assistance, the mere idea that there could be a zillionth percent chance that there is actually a small connection, in case for example we speak of them to "someone", makes it worth for them to consent to anything, as they would take the slightest chance to obtain the slightest additional assistance, as their situation is really unbearable. » Consent' Examples for Mobile Data Collection?, Responsible data mailing list, 07/04/22. https://lists.theengineroom.org/lists/arc/responsible_data/2022-04/msg00013.html

[1743] VARELIUS , J. "On the Prospects of Collective Informed Consent: On the Prospects of Collective Informed Consent." *Journal of Applied Philosophie*, 2008, n° 25, p.35–44.
HUDSON, M., "Think Globally, Act Locally: Collective Consent and the Ethics of Knowledge Production", *Int. Soc. Sci. J.*, 60, 2009, p. 125–133

Enfin, rappelons que les ONG peuvent influer sur les structures sociales locales. Les dynamiques de pouvoirs perçues comme internes aux « communautés » peuvent, dans certains cas, être associées directement à la présence des ONG, comme le pointe Alice Corbet[1744].

Autre point, l'action humanitaire s'adresse à des personnes fragilisées, traversant des situations parfois périlleuses. D'où la question suivante : qu'en est-il du consentement de personnes vulnérables dans le RGPD ?

Si l'on s'intéresse au droit à la protection des données, la catégorie de « vulnérable » semble a priori absente. On dispose de peu d'éléments pour déterminer comment est envisagée la possibilité pour un sujet qualifié de vulnérable d'exercer ses droits. La définition de la personne concernée dans le RGPD est soit neutre, soit calquée sur une représentation d'un « homme moyen ». Le règlement ne contient donc pas de définition explicite des personnes concernées comme vulnérable, à l'exception faite du considérant 75. Ce dernier porte sur les atteintes pouvant résulter de traitement de données sur les droits et libertés des personnes. Il fait l'inventaire d'une série de situations ne se restreignant pas à des causes de vulnérabilité. Ce terme n'apparait de manière explicite que lorsqu'il est question du cas de traitements concernant des enfants. Certes, le RGPD ne réduit pas la catégorie de vulnérabilité à ces derniers. Cependant, il s'agit du seul exemple cité, puisque l'article est formulé comme suit et évoque de façon générale des cas où un traitement porte « sur des données à caractère personnel relatives à des personnes physiques vulnérables, en particulier les enfants. » [1745] La nature de leur vulnérabilité est décrite de manière plus extensive dans les considérants 38 et 65. Il y est expliqué que les enfants bénéficient d'une forme spéciale de protection en raison d'une moindre compréhension des potentielles conséquences des traitements de données. Leur vulnérabilité est par conséquent décisionnelle. L'accent est donc mis sur le type d'information à leur communiquer dans le cadre d'un traitement de données. Par ailleurs, les enfants sont vulnérables de façon inhérente, ce trait n'est pas lié à la nature des traitements de données.

Au-delà du RGPD, le G29 considère que les vulnérabilités des personnes concernées relèvent d'un « rapport de pouvoir » déséquilibré entre la personne et le responsable de traitement. Cette situation concerne le cas d'employés, de personnes bénéficiant de protections sociales,

---

[1744] CORBET, Alice, « Dynamiques d'encampement : comparaison entre un camp formel et un camp informel en Haïti », *Cultures & Conflits*, 93, 2014,http://journals.openedition.org/conflits/18857
« Certains *leaders* se sont donc imposés grâce à leur capacité à interagir avec les ONG et le monde *blan* (« étranger » en créole), notamment parce qu'ils parlaient anglais ou français et qu'ils avaient appréhendé le fonctionnement des organismes de solidarité. Même si, parfois, ils ne reflétaient pas réellement les aspirations de la population, ces *leaders* étaient acceptés par cette dernière qui voyait en eux leur unique moyen d'être représentés. Qualifiés de « *leaders* communautaires » dans le jargon humanitaire, mais n'ayant aucun pouvoir décisionnel sur le camp, ces intermédiaires étaient aussi épiés par les déplacés, car leurs interactions avec le monde *blan* faisaient suspecter qu'ils tiraient de leur coopération des bénéfices personnels plus que collectifs, notamment en détournant de l'argent et des biens. «

[1745] RGPD, règlement UE 2016/679 Considérant 75, « lorsque le traitement peut donner lieu à une discrimination, à un vol ou une usurpation d'identité, à une perte financière, à une atteinte à la réputation, à une perte de confidentialité de données protégées par le secret professionnel, à un renversement non autorisé du processus de pseudonymisation ou à tout autre dommage économique ou social important; lorsque les personnes concernées pourraient être privées de leurs droits et libertés ou empêchées d'exercer le contrôle sur leurs données à caractère personnel; lorsque le traitement concerne des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, la religion ou les convictions philosophiques, l'appartenance syndicale, ainsi que des données génétiques, des données concernant la santé ou des données concernant la vie sexuelle ou des données relatives à des condamnations pénales et à des infractions, ou encore à des mesures de sûreté connexes; lorsque des aspects personnels sont évalués, notamment dans le cadre de l'analyse ou de la prédiction d'éléments concernant le rendement au travail, la situation économique, la santé, les préférences ou centres d'intérêt personnels, la fiabilité ou le comportement, la localisation ou les déplacements, en vue de créer ou d'utiliser des profils individuels; lorsque le traitement porte sur des données à caractère personnel relatives à des personnes physiques vulnérables, en particulier les enfants; ou lorsque le traitement porte sur un volume important de données à caractère personnel et touche un nombre important de personnes concernées. »

des personnes souffrant de troubles psychiques, des demandeurs d'asile, des personnes âgées, des patients, etc. Les lignes directrices n'évoquent pas la nature du traitement de données, puisqu'« un traitement qui pourrait avoir peu d'impact sur les individus en général peut en fait avoir un effet significatif sur certains groupes de la société, tels que les groupes minoritaires ou les adultes vulnérables. » Curieusement, à notre connaissance, ni le RGPD ni le G29 ne mentionnent la notion de fracture numérique et son lien avec des formes de vulnérabilité. Pourtant, l'exercice de différents droits propres à la protection des données (consentement, autodétermination informationnelle, etc.) dépend fortement de sa littératie numérique.

Les chercheurs en protection des données Gianclaudio Malgieri et Niklas Jędrzej nuancent toutefois quelque peu l'idée que le consentement ne serait pas la base légale appropriée en cas de sujets « vulnérables »[1746]. Pour eux, il est possible d'avoir recours au consentement, notamment lorsque le vecteur de vulnérabilité est relative à la faculté de compréhension de la personne concernée. Selon Gianclaudio Malgieri et Niklas Jędrzej, les difficultés de compréhension peuvent être dans certains cas atténuées, en attachant une plus grande importance à la qualité de l'information délivrée au sujet, comme le suggèrent aussi les lignes directrices du G29 concernant la transparence du traitement de données[1747]. Pour tout dire, Gianclaudio Magliari est plutôt critique vis-à-vis de la notion de « vulnérabilité ». Il considère que cette dernière est soit trop stigmatisante soit trop large. Pour le moment, le droit à la protection des données oscillerait entre une définition neutre de la personne concernée et une stigmatisation de certains sujets. C'est en tout cas la thèse de Gianclaudio Malgieri et Gloria González Fust. Ils se sont en effet intéressés aux présupposés relatifs aux vulnérabilités touchant les femmes sur lesquels repose le droit à la protection des données. Ils font d'abord remarquer que la définition classique de la personnalité juridique est construite à partir de catégories dominantes (blanc, masculin, hétérosexuel, de classe sociale supérieure) [1748]. Ainsi, le RGPD serait fondé sur une définition de la personne concernée a priori neutre, mais la personne concernée semble être « masculin par défaut ». Quant aux femmes, elles seraient d'après les chercheurs considérées comme étant de facto vulnérables : « la "personne concernée" n'était formellement pas sexuée, mais dans de nombreuses situations, cette notion renvoyait implicitement à un individu "moyen" (rationnel, circonspect, raisonnable), silencieusement considéré comme un homme, tandis que les femmes concernées étaient considérées comme autres, différentes de la moyenne, et ayant besoin d'une protection de la vie privée pour compenser leur vulnérabilité inhérente présumée. »[1749]

Pour prendre en compte différents facteurs de vulnérabilité sans stigmatiser la personne concernée, Gianclaudio Malgieri propose de s'appuyer sur le travail Federica Luna. Pour cette dernière, la vulnérabilité n'est pas un attribut fixe d'un individu, mais constitue différents faisceaux de fragilité se cristallisant en fonction du statut, du temps et du lieu. Cette approche permettrait de prendre une troisième voie entre vulnérabilité universelle et vulnérabilité individuelle (et potentiellement stigmatisante). Le caractère vulnérable d'une personne

---

[1746] MALGIERI Gianclaudio, JĘDRZEJ Niklas, "Vulnerable data subjects", *Computer Law & Security Review*, Volume 37, 2020.

[1747] Groupe de travail « Article 29 », « Lignes directrices sur la transparence au sens du règlement (UE) 2016/679 »

[1748] MALGIERI, Gian Claudio, GONZALEZ FUSTER, Gloria, "The Vulnerable data subject: a gendered data subject?", *European Journal of Law and Technology*, Vol 13 No. 2, 2022

D'IGNA, C., KLEIN, L., *Data Feminism*, MIT Press, 2020, 328 p.

[1749] « the 'data subject' was formally non-gendered, in many situations this notion implicitly referred to an 'average' (rational, circumspect, reasonable) individual silently envisaged as male, while female data subjects were seen as other, different than average, and needing privacy as a tool to balance their presumed inherent vulnerability. »

MALGIERI, Gianclaudio, GONZALEZ FUSTER, Gloria, ibid.

pourrait être déterminé lors de la réalisation d'une analyse d'impact, qui permettrait d'inclure dans l'évaluation d'un traitement de données différents vecteurs de vulnérabilité.

Qu'en est-il des humanitaires ? Comment ces derniers prennent-ils ou non en compte la vulnérabilité des bénéficiaires dans le recueil de leur consentement ? Pour répondre à cette question, on peut s'appuyer sur un cas d'étude spécifique tiré d'un document publié par l'International Rescue Committee centralisant différentes recommandations sur le recueil du consentement. On peut y lire que « des précautions supplémentaires sont à prendre dans les cas où il s'agit de travailler avec des populations vulnérables, incluant des femmes, des enfants, des réfugiés et des personnes avec des troubles mentaux. »[1750] Prise isolément, cette énumération semble mettre sur le même plan des personnes étant dans des situations très différentes, notamment les femmes. A vrai dire, si les méthodes de construction des catégories de vulnérabilité par les ONG font l'objet de débat, cela l'est d'autant plus le cas pour les femmes[1751]. Les considérer comme « vulnérables » tend à réifier des rapports de pouvoir et à les réduire à un statut de victime. Ainsi, la politique de protection des données de l'International Rescue recommande d'avoir conscience de leur vulnérabilité, mais dans une logique « d'empowerment ». Il faut s'assurer que leur volonté s'exprime pleinement, et qu'elles ne sont pas réduites au silence par les différents acteurs du groupe local. L'IRC conseille alors de s'adresser à elles dans des situations de non-mixité et d'échanger avec les « leaders locaux » pour connaitre les coutumes des femmes dans la communauté. Dans le cas où une femme est accompagnée par un homme, il est recommandé de vérifier que le consentement est exprimé par cette dernière sans être influé par une présence masculine. Ceci est aussi valable dans les cas où elle est accompagnée par d'autres proches, et dans les cas où sont abordés des sujets sensibles (violences familiales ou sexuelles).

En outre, les femmes sont — comme le rappelle le document de l'International Rescue Committee — également touchées par un moindre accès à l'éducation générale. Elles sont ainsi plus durement affectées par des formes de fractures numériques. La politique de données conseille alors de « simplifier » les explications délivrées aux femmes. D'où un risque d'infantilisation. Dernier point, les femmes tendent à être concernées par des sujets relevant de l'intime (agressions sexuelles, viols, grossesses non souhaitées, santé sexuelle, avortement, etc.), sachant qu'elles sont également vulnérables aux formes de violence en ligne et par des formes de cyberharcélements[1752]. Le recueil de ce type de données est délicat. Ce sont des données sensibles au sens juridique du terme. Et elles peuvent relever de tabou. Une enquêté nous confie donc que « *sur les violences de genre, quand on travaille sur des cas de viol, le consentement est très important, mais ça demande beaucoup de temps souvent pour avoir*

[1750] « Special requirements may apply when working with vulnerable populations including women, children, refugees, and persons with mentally impairments. » MASKET, K, "Research toolkit: obtaining meaningful informed consent", International Rescue Committee,2018 https://sohs.alnap.org/help-library/irc-research-toolkit-obtaining-meaningful-informed-consent

[1751] NI AOLAIN, Fionnuala, "Women, Vulnerability, and Humanitarian Emergencies", *Michigan Journal of Gender&Law*, Vol.18-Issue 1, 2011
SANDVIK, Kristin Bergtora, "Technology, Dead Male Bodies, and Feminist Recognition: Gendering ICT Harm Theory", *Australian Feminist Law Journal*, 44:1, 2018, p.49-69, 10.1080/13200968.2018.1465371
SANDVIK, K.B., BJORHAUG, I., ESPEGREN, A. GARNIER, A. "Protecting skilled Afghan women: Brain save and the politics of vulnerability", *Global Policy*, 2023, 14, 5– 15. https://doi.org/10.1111/1758-5899.13166

[1752] O'BRIEN, Megan, « Online violence : real life impacts on women and girls in humanitarian setting », Humanitarian law &Policy, ICRC, 04/01/2024https://blogs.icrc.org/law-and-policy/2024/01/04/online-violence-real-life-impacts-women-girls-humanitarian-settings/

*des informations, et ça demande d'éviter d'être un groupe de 25, y a vraiment un cadre pour pouvoir recueillir des informations. Y a donc des fois où ça marche très bien, et d'autres moments où c'est pas toujours parfait… ça peut être lié à plein de raisons différentes*. « [1753] En outre, sans nier la prise en compte de contextes culturels, les différentes politiques de protection de données tendent à attribuer aux femmes une forme de « pudeur ». Elles tendent à « essentialiser » leur rapport à l'intime et à la sexualité, de psychologiser des dynamiques sociales. En somme, dans ce cas, il est recommandé d'être attentif aux rapports de pouvoir contextuels, propres à un groupe social donné, mais cette démarche n'est pas exempte d'une essentialisation des vulnérabilités féminines. Le risque est d'adopter en fin de compte une démarche paternaliste en ayant une conception réductrice des vulnérabilités pouvant les toucher. Enfin, le document ne fait pas référence à un enjeu faisant également l'objet de débats : la prise en compte des formes de vulnérabilité liées à la condition masculine[1754].

On a donc esquissé un panorama des différentes difficultés associées à la collecte du consentement. Mais une question reste ouverte : comment les ONG prennent-elles en compte les cas d'opposition à un traitement de données ? Une absence de consentement entraine-t-il ou non la suspension de l'aide ? Il est tout à fait clair dans le RGPD qu'une absence de consentement ne doit pas être associé à un retrait du service, et donc en l'occurrence à un retrait de l'aide humanitaire. Et surtout, la politique de protection de données du CICR suggère clairement de ne pas avoir recours à cette base légale s'il n'est pas possible de retirer ce dernier sans conséquence : « Si les personnes concernées refusent expressément leur consentement, elles doivent être informées des conséquences de ce refus, y compris de l'effet que cela peut avoir sur l'assistance qui pourrait ou pourrait être apportée aux personnes concernées par les organisations humanitaires et/ou les organisations tierces. Si, toutefois, l'assistance ne pouvait être fournie en l'absence de consentement, il convient de noter que le consentement ne peut être considéré comme une base juridique pour le traitement. »[1755]

Cependant, ce point est difficilement mis en œuvre, comme nous le confient des DPO : « *Je pense qu'il a un gros problème concernant le fait de retirer son consentement, je pense qu'il n'y a pas toujours de moyens d'être facilement joignable.* » [1756] Et surtout, les ONG ne disposent pas toujours de solution pour continuer à allouer de l'aide dans ce type de situation. On a en effet eu de nombreux retours de ce type en entretien : « *Je ne sais pas quoi faire si des personnes disent non, mais il faut trouver un moyen d'allouer le service malgré tout*. » [1757]

---

[1753] Entretien n°10, OI3, information manager officer, 06/01/2020

[1754]TURNER, Lewis, "The Politics of Labeling Refugee Men as "Vulnerable"", *Social Politics: International Studies in Gender, State & Society*, Volume 28, Issue 1, Spring 2021,p. 1–23, https://doi.org/10.1093/sp/jxz033
BRUN, Delphine,"A failure to address the vulnerability of men and boys", Norwegian Refugee council, 30/03/2021 https://www.nrc.no/expert-deployment/2016/2021/a-failure-to-adress-the-vulnerability-of-men-and-boys/

[1755] « if Data Subjects expressly withhold Consent, they should be advised about the implications, including the effect this may have on assistance that might or might not be rendered by Humanitarian Organizations and/or Third Party organizations. If, however, assistance could not be provided in the absence of Consent, note that Consent could not be considered as a legal basis for the Processing. » KUNER Christopher, MARELLI Massimo, "Handbook on data protection in humanitarian action", second edition, 2020

[1756] « I think there is a big problem about revoking consent, I think there is not always straighfull ways to be contactable. » Entretien ONG1, DPO, 08/11/2019

[1757] Entretien n°83, ONG1, DPO, 14/10/2022.

« *On devrait pouvoir proposer une forme d'alternative, en théorie on devrait toujours avoir une aide qui se passe des données, mais dans le cas… c'est rarement le cas.* »[1758]

À vrai dire, la plupart des enquêtes insistent sur le fait qu'il existe peu de cas d'opposition aux collectes des données. Tout d'abord, les bénéficiaires ne connaitraient pas leurs droits. D'après eux, il semble exister une croyance persistante (mais souvent fondée) d'une conditionnalité de l'aide à la collecte de données. Ensuite, le fait de pouvoir ou non s'opposer à un traitement de données pourrait également être dû à l'absence d'un espace dédié de communication. Les ONG elles-mêmes font face à une obligation (plus ou moins informelle) de collecter des données, afin de pouvoir remplir des audits et documenter les cas de fraudes. Elles sont donc d'autant moins incitées à prendre en compte la possibilité de s'opposer à la collecte de données. Par conséquent, le consentement est dans certains cas formel, sans prise en compte de potentielles objections. Il serait réduit à un acte automatique de validation : *« C'est pas que les organisations veulent mal faire, au contraire les organisations veulent bien faire, et donc elles disent, bah, attend, avant de recueillir des données d'une personne, il faut quand même lui recueillir son consentement, son autorisation, mais en fait là y a une confusion, entre informer une personne, qui est une obligation dans tous les cas, qu'on soit sur le consentement ou l'intérêt vital, informer une personne et prendre ses objections, donc rechercher un non, et rechercher un consentement, il y a une confusion en fait entre aller chercher un oui ou aller chercher un non.* »[1759]

Bien plus, dans de rares cas, l'information aux bénéficiaires sur les finalités du traitement semble être considérée comme un moyen de « chercher » le consentement et de prévenir tout refus. Ainsi, on peut lire dans la politique de protection de données de 2016 du WFP que : « Dans un camp où les réfugiés résidaient depuis de nombreuses années, l'introduction d'un nouveau système d'identification des personnes éligibles aux prestations s'est heurtée à une forte résistance. Auparavant, les réfugiés devaient présenter une pièce d'identité sur papier pour recevoir leurs allocations. Le nouveau système comprend des cartes à puce avec la photo et les empreintes digitales du réfugié. Les réfugiés ont compris que la prise d'empreintes digitales était une forme de consentement, et ils appréhendaient de donner leurs empreintes digitales pour la base de données des bénéficiaires, de peur qu'elles ne soient utilisées à d'autres fins, par exemple pour prouver qu'ils acceptent d'être rapatriés. Le personnel du WFP a organisé un certain nombre de distributions fictives pour montrer aux réfugiés comment le nouveau système fonctionnerait — en particulier, comment les empreintes digitales seraient utilisées pour vérifier les identités aux fins de la distribution des vivres. Le WFP a également mené une campagne intensive de sensibilisation au programme de cartes à puce. Cette campagne comprenait des réunions avec les chefs des réfugiés, des réunions communautaires, des séances de sensibilisation au niveau des ménages et la distribution de dépliants. Il était très important pour le WFP de se coordonner étroitement avec le HCR et le gouvernement. Les trois parties ont participé aux réunions avec les réfugiés et étaient présentes lors de la prise des empreintes digitales. Cela a également contribué à renforcer la confiance des réfugiés. Une fois que les réfugiés ont compris exactement pourquoi les

[1758] Entretien n°91, OI2, DPO, 26/05/2023
[1759] Ibid.

empreintes digitales étaient nécessaires et comment elles allaient être utilisées, leurs craintes ont été apaisées et le projet a été mis en œuvre avec seulement un petit pourcentage de la population qui a refusé de participer en refusant de donner son consentement. Il s'agit là d'un excellent exemple de garantie d'un consentement véritablement éclairé. »[1760] Ce type de campagne va à l'encontre des recommandation du rapporteur onusien sur la pauvreté et les droits de l'homme selon qui une alternative aux solutions numériques doit toujours exister afin d'assurer un consentement réellement libre[1761].

Pour illustrer cette problématique, on peut évoquer l'opposition des Houthi à la récolte de données biométriques, au Yémen. Le WFP a mis en avant la nécessité de contrôler l'allocation de l'aide auprès de la population yéménite via le recueil de données biométriques. Le recours à ce type de dispositif est justifié par l'argument usuel d'une nécessité de contrôler l'allocation de l'aide et empêcher des « fraudes ». Or des groupes Houthi s'y sont opposés, considérant que cela constituait une opération de renseignement. Par voie de conséquence le WFP a commencé à suspendre partiellement ses opérations d'aide alimentaires. L'organisation humanitaire explique que : «  Cette décision a été prise en dernier ressort, après que de longues négociations ont achoppé sur un accord visant à introduire des contrôles pour empêcher le détournement des denrées alimentaires au détriment de certaines des personnes les plus vulnérables du Yémen. »[1762] Le WFP confirme que «  la priorité du WFP reste de nourrir les enfants, les femmes et les hommes les plus affamés du Yémen. Mais comme dans toute zone de conflit, certains individus cherchent à tirer profit en s'attaquant aux personnes vulnérables et en détournant les denrées alimentaires des endroits où elles sont le plus nécessaires. Le WFP cherche à obtenir le soutien des autorités de Sanaa pour mettre en place un système d'enregistrement biométrique qui empêcherait les détournements et protégerait les familles yéménites que nous servons, en veillant à ce que la nourriture parvienne à ceux qui en ont le plus besoin. »[1763]

---

[1760] « At a camp where refugees had been resident for many years, the introduction of a new system of identifying eligible persons for benefits was met with strong resistance. Previously, refugees had to present a paper identification document to receive their benefits. The new system involved smart cards with the refugee's picture and fingerprints. The refugees understood fingerprinting as a form of giving consent, and they were apprehensive about giving a fingerprint for the beneficiary database lest their print be misused for other purposes, such as evidence of their agreement to repatriation. WFP personnel held a number of mock distributions to demonstrate to the refugees how the new system would work — specifically, how fingerprints would be used to verify identities for the purpose of food distribution. WFP also conducted an intensive sensitisation campaign for the smart card programme. This included meetings with refugee leaders, community meetings, household-level awareness sessions and distribution of flyers. It was very important for WFP to coordinate closely with UNHCR and the Government. All three parties participated in meetings with the refugees and were present during the fingerprinting exercise. This also helped increase the trust of refugees. Once the refugees understood exactly why fingerprints were required and how they were going to be used, their fears were allayed and the project was implemented with only a small percentage of the population declining to participate by withholding consent. This is an excellent example of ensuring that consent is truly informed. » WFP Guide to Personal Data Protection and Privacy, 2016 https://docs.wfp.org/api/documents/e8d24e70cc11448383495caca154cb97/download/

[1761] ALSTON, Philip, United Nations, Human Rights Council," Report of the Special Rapporteur on extreme poverty and human rights", A/74/48037,11/10/ 2019.

[1762]WFP, "World Food program begins partial suspension of aid in Yemen", 2019 *https://reliefweb.int/report/yemen/world-food-programme-begins-partial-suspension-aid-yemen*

[1763] « The United Nations World Food Program has started a partial suspension of food assistance operations in areas of Yemen under the control of the Sana'a-based authorities. The decision was taken as a last resort after lengthy negotiations stalled on an agreement to introduce controls to prevent the diversion of food away from some of the most vulnerable people in Yemen. WFP's priority remains to feed the hungriest children, women and men of Yemen. But as in any conflict zone, some individuals seek to profit by preying on the vulnerable and diverting food away from where it is most needed. WFP has been seeking the support of the Sana'a-based authorities to introduce a biometric registration system that would prevent diversion and protect the Yemeni families we serve, ensuring food reaches those who need it most. » WFP, "World Food program begins partial suspension of aid in Yemen", 2019 https://reliefweb.int/report/yemen/world-food-programme-begins-partial-suspension-aid-yemen
https://twitter.com/BenParker140/status/1141810181849976834

Dans cet extrait, on voit bien que les houthis sont binairement opposés à des populations vulnérables. Ces dernières sont réduites à être des victimes « sans voix ». Et de fait, dans les prises de paroles publiques du WFP leur avis sur les dispositifs biométriques n'est pas évoqué. Notons que l'opposition des groupes houthis est désignée comme mettant en danger les populations,

Cette affaire a été interprétée comme un exemple de non-respect du droit d'opposition au traitement aux données. La chercheuse Mirca Madianou déclare par exemple que : « Cet épisode a fait couler beaucoup d'encre, notamment parce qu'il a révélé en termes crus l'absence de consentement valable dans les enregistrements biométriques des sujets humanitaires. »[1764] En plus de strictes problématiques de vie privée individuelle, l'affaire traduit aussi des enjeux de souveraineté et des tensions relatives au contrôle de données entre une organisation internationale et un groupe d'acteurs locaux. Cela dit, l'affaire ne s'est pas simplement jouée qu'entre le WFP et les houthis. A priori, le fait de collecter des données biométrique est dans une certaine mesure dû à la crainte d'un possible retrait de financement par un bailleur, l'USAID, comme le révèle l'organisation Human Right watch : « Un responsable des donateurs a déclaré qu'il était peu probable que les États-Unis financent des rations alimentaires complètes tant que la question de la collecte des données biométriques n'aurait pas été résolue. » [1765] Cette exigence s'inscrit dans une tendance plus générale de restriction par les USA de l'aide au Yémen dans les zones « contrôlées » par les houthis[1766]. Il se trouve en effet qu'en février 2021, Mike Pompeo a désigné les groupes houthis comme « terroristes ». Il les a placés sous liste rouge, alors que le secrétaire d'État Anthony Bliken s'était opposé à le faire. Il a pourtant dénoncé (notamment en 2022) publiquement le financement de groupes houthis par différents acteurs. Le terme de « terroriste » est utilisé pour les désigner : « Les attaques des Houthis à l'intérieur du Yémen et contre les voisins du Yémen, y compris les récents attentats terroristes visant explicitement des sites civils en Arabie saoudite et aux Émirats arabes unis, ont fait de nombreuses victimes civiles. »[1767] Il reste difficile d'objectiver un lien direct entre l'action du WFP et les prises de positions américaines. Mais on peut faire l'hypothèse qu'elles ont pu jouer dans le choix de mettre en place des dispositifs biométriques, d'autant que l'USAID participe au financement des programmes du WFP[1768]. Enfin, on doit aussi prendre en compte le contexte fortement dégradé dans les zones contrôlées par les houthis ( enlèvements de personnes de la société civile, dont du personnel de l'ONU et d'ONG humanitaires, détournement de l'aide)[1769].

---

[1764] « This episode received much attention not least because it revealed in stark terms the lack of meaningful consent in the biometric registrations of humanitarian subjects. »MADIANOU, Mirca, "Contribution to the Expert Workshop on Race, Technology and Borders convened by the UN Special Rapporteur*", E. Tendayi Achiume,* juin 2020.

[1765] « A donor official said the US would be unlikely to fund full food rations until the issue around biometric data collection had been resolved « Human Right Watch, "Obstruction of Aid in Yemen During Covid-19", 14/09/ 2020

[1766] SCOTT, Paul, " USAID has suspended aid to 80 percent of Yemenis: an appalling abuse of humanitarian principles," *Just security*, 22/07/2020 https://www.justsecurity.org/71576/usaid-has-suspended-aid-to-80-percent-of-yemenis-an-appalling-abuse-of-humanitarian-principles/

[1767] BLINKEN J Antony," United States Designates Houthi Finance Network in Coordination with Gulf Partners", 23/02/2022. https://www.state.gov/united-states-designates-houthi-finance-network-in-coordination-with-gulf-partners/

[1768] https://www.wfp.org/funding/2022

[1769] Yemen : Houthis disappear dozens of UN, Civil Society Staff, release detainees, end arbitrary arrests and enforced disappearances", *Human RIghts Watch,* 26/06/2024 https://www.hrw.org/news/2024/06/26/yemen-houthis-disappear-dozens-un-civil-society-staff

Cet exemple nous a donc paru une illustration des différentes dynamiques de pouvoir pesant dans le recueil du consentement, qui s'inscrit dans un contexte hautement politisé. Mais de façon générale, le tableau est contrasté : il existe certes des effets de dominations assez forts, dans certains cas les choix des ONG les renforcent, et passent outre le respect de l'autonomie des bénéficiaires. Le recueil du consentement pourrait être strictement formel, être une pure performance sans qu'un véritable choix soit laissé aux bénéficiaires. Mais dans le même temps, on note une tendance de fond actant une prise de conscience des limites liées au consentement, qui se traduit d'abord par la volonté d'« améliorer » le recueil de ce dernier dans l'aide.

Car de façon générale, il semblerait que, pour le moment, se détacher du consentement reste difficile. Ainsi, dans un webinaire, un participant avoue que le consentement n'est pas encore effectif, mais qu'au moins il est demandé aux bénéficiaires d'effectuer un choix minimal. Mais le même participant reconnait que dire qu'ils ont un choix totalement libre serait exagéré[1770]. Toujours dans ce même webinaire, un autre participant renchérit qu'il aimerait bien utiliser le consentement éclairé, que cela est fondamental pour préserver la dignité des personnes. Mais, il ajoute que cela est impossible s'il se fonde sur le texte actuel de loi. Il attend par conséquent des juristes qu'ils écrivent une loi plus adaptée au contexte humanitaire, notamment en ce qui concerne le consentement[1771]. Sans en venir à ce type d'extrémité, certains DPO tentent d'« améliorer » le consentement, d'atténuer les rapports de pouvoir, de rendre plus lisible l'information délivrée. Certains délégués à la protection des données recommandent en revanche de limiter le consentement au fait d'informer la personne concernée : « Si le recueil du consentement n'est pas possible « on considère que les bénéficiaires doivent être au moins informés individuellement ou collectivement de la nature du programme leur étant délivré, et sur la nature des informations collectées, et sur l'identité des personnes les collectant ainsi que les raisons du traitement. »[1772]

Bien plus, au fil du temps, on a observé que certaines politiques de protection de données mentionnent le fait que le consentement n'est pas approprié au contexte humanitaire. Cette précision est souvent accompagnée de regret. Et dans la plupart des cas, on peut lire que cette base légale doit être malgré tout employée dans la mesure du possible. Les autres bases légales sont alors à employer qu'en dernier recours.

Seule une minorité d'humanitaires revendique d'envisager des alternatives au consentement. Raymond Nathaniel déclare ainsi que : « les organisations — qui ont cherché à se conformer à l'éthique fondée sur le principe "ne pas nuire" via la protection des données personnelles et un attachement au consentement éclairé individuel — s'accrochent à un modèle éthique qui est — dans un nombre grandissant de cas — anachronique. L'évolution des méthodologies de collecte, d'utilisation et des contextes opérationnels a rendu l'éthique centrée sur les données personnelles et sur le consentement individuel insuffisant dans un monde complexe en réseau

[1770] CARTONG, « How Can you truly manage informed consent in practice? », November 2020. https://www.youtube.com/watch?v=jIeB-i5fWR0&list=PLDuxmnTc4fTroeNltntD8HaYrs6xHiuBG&index=6

[1771] Ibid.

[1772] « If this is not possible then we consider that beneficiaries should at least be informed individually or collectively or both as to the nature of the program being provided, what information is being collected, by whom and why. » CALPNETWORK, "Protecting beneficiary privacy, Principles and operational standards for the secure use of personal data in cash and e-transfer programmes", *The Cash learning Partnership*, 2020

en évolution croissante — un monde qui remplace rapidement les cadres normatifs dont disposent ces acteurs. » [1773]

Pour résumer la situation, nous avons construit le tableau suivant, fait à partir de politiques de protection de données. Il donne un aperçu de l'absence de consensus sur la réponse à apporter au « paradoxe du consentement ».

| Consentement | CICR | UNHCR (version2018) | Unhcr (version 2015) | OIM (2010) | IFRC | UNICEF | WFP | Médecins du monde (2010) |
|---|---|---|---|---|---|---|---|---|
| Libre | | | | | | | | |
| Eclairé | | | | | | | | |
| Univoque | | | | | | | | |
| Spécifique | | | | | | | | |
| Nécessité de redemander le consentement en cas de changement de finalité | | | | | | | | |
| Possibilité de retirer son consentement | | | | | | | | |
| Possibilité de ne pas donner d'informations (ou retirer son consentement ) sans avoir à en supporter les conséquences | | | | | | | | |
| Intérêt légitime | | | | | | | | |

[1773]« Thus organizations seeking to embody the ethic of non-maleficence primarily through the protection of PII and a reliance on individual informed consent models are pursuing an ethical paradigm that is, in an increasing number of cases, anachronistic. Evolving collection approaches, uses, and operational contexts have rendered a PII and individual consent-focused ethics alone insufficient in an increasingly evolving and complex networked world - a world that is quickly superseding the traditional normative frameworks available to these actors. » RAYMOND, Nathaniel, « Beyond "Do No Harm" and Individual Consent: Reckoning with the Emerging Ethical Challenges of Civil Society's Use of Data ». In: VAN DER SLOOT, Bart, FLORIDI, Luciano, TAYLOR, Linnet (eds.), *Group Privacy*, Springer Verlag,2017.

| Consentement | Oxfam (2015) | Oxfam (2021, biométrie) | Terre des Hommes | Mercy Corps | International rescue committee | 510 Red Cross netherland |
|---|---|---|---|---|---|---|
| Libre | | | | | | |
| Eclairé | | | | | | |
| Univoque | | | | | | |
| Spécifique | | | | | | |
| Possibilité de redemander le consentement en cas de changement de finalité | | | | | | |
| Possibilité de retirer son consentement | | | | | | |
| Possibilité de ne pas donner d'information (ou retirer consentement) sans avoir à en supporter les conséquences | | | | | | |
| Intérêt légitime | | | | | | |
| Intérêt vital | | | | | | |

On peut observer que le consentement est la base légale la plus mentionnée. Ceci pourrait avoir plusieurs explications. Cela pourrait être dû à une méconnaissance du droit, à une méconnaissance des autres bases légales, comme l'avance une enquêtée : *« la plupart des ONG ne savent pas que l'intérêt légitime existe et se démènent avec le consentement. »* [1774]

[1774] Entretien n°4, DPO, 18/11/2019

Ou ceci pourrait aussi découler d'un attachement au consentement plutôt qu'un manque de culture juridique.

## §2 — L'intérêt légitime

Et pourtant, dans les situations de crise, il semble cohérent d'avoir recours à l'intérêt vital. Ce dernier est défini comme suit par le considérant 46 du RGPD : « Le traitement de données à caractère personnel devrait être également considéré comme licite lorsqu'il est nécessaire pour protéger un intérêt essentiel à la vie de la personne concernée ou à celle d'une autre personne physique. Le traitement de données à caractère personnel fondé sur l'intérêt vital d'une autre personne physique ne devrait en principe avoir lieu que lorsque le traitement ne peut manifestement pas être fondé sur une autre base juridique. Certains types de traitement peuvent être justifiés à la fois par des motifs importants d'intérêt public et par les intérêts vitaux de la personne concernée, par exemple lorsque le traitement est nécessaire à des fins humanitaires, y compris pour suivre des épidémies et leur propagation, ou dans les cas d'urgence humanitaire, notamment les situations de catastrophe naturelle et d'origine humaine. »[1775]

Il s'agit donc a priori de la base légale la plus appropriée à l'humanitaire. Cependant, telle qu'elle est définie dans le droit, elle ne correspond pas à l'ensemble des pratiques du secteur. Et de fait, en entretien, peu de DPO y font référence. Ils la citent simplement pour des situations spécifiques, comme la vaccination de masse ; ou bien lorsque la personne ne peut exprimer sa volonté, en cas de blessure grave. Plus communément, l'intérêt vital est limité aux situations d'urgence : « c'est commun dans des situations humanitaires, qui nécessitent d'avoir recours à d'autres bases légales, comme l'intérêt vital ou l'intérêt public. Quoiqu'il en soit, ces bases légales alternatives ont peu de chance de pouvoir être appliquées dans de futur cas d'usage des données, allant au-delà de l'assistance vitale du moment. »[1776] Cela dit, on a aussi pu lire qu'il était possible d'avoir recours à l'intérêt vital pour tout traitement relatif « à la délivrance de biens essentiels à un individu ou à une communauté, pendant ou après une urgence humanitaire.» [1777] Cette interprétation très large de l'intérêt vital semble être minoritaire, en tout cas nos enquêtés n'y ont pas fait mention.

Une deuxième option consiste à avoir recours à la base légale de l'intérêt légitime. Cette base légale était déjà existante dans la directive de 1995. Dans le RGPD, elle est définie comme suit : Article 6.1.f : « [le] traitement n'est licite que si, et dans la mesure où (…) le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou

---

[1775]Raison 46, Règlement UE 2016/679 https://www.privacy-regulation.eu/fr/r46.htm

[1776] GOODMAN Ric, SCHOEMAKER Emrys,MESSENGER Chloe,STELLER Rachael, "Review and analysis of identification and registration systems in protracted and recurrent crises, Development alternative incorporated", *Caribou Digital*, May 2020. https://assetify-dai.com/pdfs/BASIC%20MIS%20in%20Crises%20Full%20Report%20External%20Version.pdf

« Most importantly, a person who has no other option cannot provide valid consent. Nonetheless, the inability to provide consent does not mean that services cannot be provided. This is common in humanitarian settings, and requires relying on another lawful basis, such as vital or public interest. However, these alternative legal bases are unlikely to apply to future uses of this data, beyond immediate, life-saving support. »

[1777] Ibid, « The processing is necessary to provide for the essential needs of an individual or a community during, or in the aftermath of, a humanitarian emergency. »

par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant. »

L'intérêt légitime permet donc de se passer du consentement de la personne concernée. Son caractère « glissant » a été dénoncé par plusieurs activistes de défense des droits de l'homme en ligne, notamment Jann Philipp Albrecht, député européen ayant pris part à la rédaction du RGPD. Il considère que l'intérêt légitime tel qu'il est formulé dans la proposition de loi introduirait le risque « de rendre l'ensemble du règlement inefficace. »[1778] Le juriste Federico Ferreti va dans ce sens en avertissant sur le fait que l'intérêt légitime pourrait être un outil pour contourner les protections légales portées par le RGPD[1779].

Le WG29 adopte une position plus modérée sur l'intérêt légitime. Selon lui, il ne doit pas être une solution clef en main, à laquelle on aurait systématiquement recours. Il ne faut pas pour autant que le responsable de traitement soit trop restrictif sur son usage. En bref, y recourir doit être fait selon une logique « au cas par cas », en se fondant sur différentes conditions que précise le WG29[1780].

Premièrement, l'usage de l'intérêt légitime doit reposer sur un critère de nécessité, qui limite strictement les contextes dans lesquels cette base légale peut être appliquée. On ne pourrait s'y référer qu'en dernier recours.

En outre, l'intérêt du responsable de données doit être formulé de façon claire. Cela permet d'établir une balance entre les intérêts de ce dernier et les droits fondamentaux de la personne concernée. Les intérêts du responsable de traitement doivent concerner des activités présentes, et non pas des intérêts vagues ou hypothétiques. L'intérêt légitime est défini par son caractère à la fois impérieux et profitable à la société. Un intérêt commercial n'est par exemple pour le G29 pas considéré comme un « intérêt légitime ». Et évidemment, il est indiqué que l'intérêt légitime doit rester dans le cadre de la légalité.

Deuxièmement, le WG29 souligne qu'il ne faut pas tromper les attentes raisonnables des personnes concernées. Et le considérant 47 du RGPD précise que : « l'existence d'un intérêt légitime devrait faire l'objet d'une évaluation attentive, notamment afin de déterminer si une personne concernée peut raisonnablement s'attendre, au moment et dans le cadre de la collecte des données à caractère personnel, à ce que celles-ci fassent l'objet d'un traitement à une fin donnée ».

Ajoutons que le RGPD précise que l'intérêt et les droits des personnes concernées doivent être pris en compte, comme le spécifie dans un avis le G29 : « La liberté d'expression et d'information, la liberté des arts et des sciences, le droit d'accès aux documents, par exemple,

---

[1778] La quadrature du net, « Major Loopholes in Privacy Regulation – EU Parliament Must Stand For Citizens », 21/10/2013https://www.laquadrature.net/en/2013/10/21/data-protection-regulation-today-progress-can-be-reversed-by-opaque-negotiations/

[1779] FERRETTI, Federico, « Data protection and the legitimate interest of data controllers: Much ado about nothing or the winter of rights? » *Common Market Law Review*, Issue 3, 2014, p. 843-868, https://kluwerlawonline.com/journalarticle/Common+Market+Law+Review/51.3/COLA2014063

[1780] The Future of Privacy Forum, "Processing Personal Data on the Basis of Legitimate Interests under the GDPR PRACTICAL CASES",2018, https://fpf.org/wp-content/uploads/2018/04/20180413-Legitimate-Interest_FPF_Nymity-2018.pdf

que le droit à la liberté et à la sûreté, la liberté de pensée, de conscience et de religion, la liberté d'entreprise, le droit de propriété, le droit à un recours effectif et à accéder à un tribunal impartial, ou la présomption d'innocence et les droits de la défense, etc. L'intérêt individuel peut également recouper l'intérêt collectif, tel l'avantage pour le public de pouvoir accéder à l'article d'un journaliste révélant des faits de corruption dans l'administration de l'État ou l'avantage de bénéficier du progrès des recherches médicales. »[1781]

Troisièmement, avoir recours à l'intérêt légitime nécessite de pondérer l'intérêt du contrôleur et de la personne concernée. Il faut prendre en compte dans l'exercice de pondération la nature de l'information (des données sensibles, des données publiques ou non). Il ne faut pas oublier de tenir compte de l'existence de mesure d'atténuation de risques, de minimisation de la collecte de données, d'autres mesures de protection des données[1782].

Les données collectées doivent l'être de façon proportionnelle, en respectant le principe de minimisation. Par exemple, il peut s'avérer essentiel et proportionné qu'un journal publie certains éléments incriminants à propos du train de vie d'un haut fonctionnaire impliqué dans un scandale de corruption présumé. Mais il ne s'agit pas pour le journal de publier l'intégralité des détails de la vie privée des personnalités publiques.

En général, le fait qu'un responsable du traitement agisse non seulement dans son propre intérêt légitime (commercial), mais aussi dans l'intérêt de la collectivité peut donner plus de « poids » à cet intérêt. On peut citer certains cas limites : pour le G29 l'utilisation de la biométrie peut grandement contrevenir à la vie privée des personnes, tout en étant nécessaire au fait d'assurer la sécurité publique. L'exercice de cette pondération est donc hautement contextualisé, voire subjectif, comme le craint également le chercheur Paolo Balboni[1783].

Mais le WG29 met en garde : plus les informations sont sensibles, plus les conséquences qu'elles peuvent avoir pour la personne concernée sont importantes, et plus la balance peut pencher en sa faveur. Le responsable de traitement doit donc également être attentif aux inégalités de pouvoir et les rapports de force. Ces derniers peuvent être tempérés de deux manières. Tout d'abord, pour permettre aux personnes concernées de faire valoir leurs droits, le WG29 recommande que les responsables de traitement expliquent aux personnes concernées d'une manière claire la finalité de la collecte de données. Enfin, il est conseillé de ménager la possibilité pour les personnes concernées de s'opposer au traitement de données. À noter que l'intérêt légitime ne vaut pas nécessairement une acceptation totale et de facto des traitements. L'intérêt légitime contredit l'autonomie informationnelle du sujet, et va à l'encontre de tout contrôle a priori sur l'usage de ses données. Mais il est accordé au sujet un droit d'opposition et la personne doit démontrer que le responsable de traitement s'est

[1781] G29, Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE, 09/04/2014.
[1782] KAMARA I., DE HERT, P., « Understanding the balancing act behind the legitimate interest of the controller ground: A pragmatic approach », In : SELINGER E, POLONETSKY J., TENE, O. (eds.), *Cambridge handbook of consumer privacy*, 2018, p. 321-352
[1783] BALBONI, P., COOPER, D., IMPERIALI, R. & MACENEITE, M. , « Legitimate interest of the data controller New data protection paradigm: legitimacy grounded on appropriate protection », *International Data Privacy Law,* 2013, 3 (4), p. 244-261

trompé dans la pondération, que la balance penche en sa faveur. Le responsable de traitement ne peut s'y opposer que s'il invoque des « motifs légitimes et impérieux »[1784].

Ces derniers points nous laissent penser que l'intérêt légitime pourrait peut-être pencher en faveur des bénéficiaires (ces derniers étant vulnérables, la possibilité de refuser la collecte est mince, il s'agit souvent de données sensibles, etc.) Mais notons que l'intérêt légitime du responsable de traitement peut être considéré comme impérieux. Déterminer de façon générale dans quel sens penche la balance en contexte humanitaire nous parait a priori difficile.

Or, dans le guide relatif à la protection des données du CICR, l'usage de l'intérêt légitime est très large. Il ne semble pas constituer une base légale de « dernier recours ». On peut y lire que : « l'intérêt légitime peut inclure des situations comme les suivantes :

— Le traitement est nécessaire afin de remplir la mission de l'organisation humanitaire, dans les cas où des motifs importants d'intérêt public ne sont pas invoqués.

— Le traitement est nécessaire pour assurer la sécurité des systèmes d'information et la sécurité de l'information, ainsi que la sécurité des services connexes accessibles via ces systèmes d'information, par les autorités publiques, les Computer Computer Emergency Response Teams (CERT), Computer Security Incident Response Teams (CSIRT), les fournisseurs de services d'information et de communication (CSIRT), les fournisseurs de réseaux et de services de communications électroniques et les fournisseurs de technologies et de services de sécurité et par les fournisseurs de technologies et de services de sécurité. Il peut s'agir, par exemple, d'empêcher l'accès non autorisé aux réseaux de communications électroniques et la distribution de codes malveillants, et de mettre un terme à la diffusion de codes malveillants, ainsi que l'arrêt des attaques par "déni de service" et des dommages causés aux systèmes informatiques et de communication électronique.

— Le traitement est nécessaire à des fins de prévention, de preuve et d'arrêt de la fraude ou du vol.

— Le traitement des données à caractère personnel est nécessaire aux fins d'anonymisation ou de pseudonymisation des données à caractère personnel.

— Le traitement est nécessaire à la constatation, à l'exercice ou à la défense de droits d'une action en justice, que ce soit dans le cadre d'une procédure judiciaire, administrative ou extrajudiciaire. »[1785]

Le fait de se concentrer sur base légale d'intérêt légitime est alors présenté comme une forme de pragmatisme, mais elle renforce la responsabilisation des personnes dont la tâche concerne la gestion de l'information. Ainsi, une humanitaire fait remarquer que « le concept de "duty of care" est particulièrement utile, et permet de transférer le fardeau de la

[1784] L'article 21, 1 du RGPD prévoit ainsi que : « la personne concernée a le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à un traitement des données à caractère personnel la concernant fondé sur [les intérêts légitimes du responsable du traitement, y compris un profilage fondé sur ces dispositions. » Dans ce cas, « [le] responsable du traitement ne traite plus les données à caractère personnel, à moins qu'il ne démontre qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée».

[1785] KUNER, Christopher, MARELLI, Massimo," *Handbook on data protection in humanitarian action"*, second edition, 2020.

responsabilité sur l'institution plutôt que sur l'individu, qui est en fin de compte responsable de la façon et dans quels cas est utilisé des données sur des individus vulnérables. »[1786] On voit bien au regard de cette liste de cas que cette base légale pourrait être utilisée dans de nombreuses situations. Cela inquiète certains DPO qui pointent le fait que cette base légale est « glissante » : « *le passage du cadre du consentement à l'intérêt public, est-ce un garde-fou éthique suffisant ? Cela ne fait qu'entériner une pratique au sein du champ humanitaire. Mais est-ce en soi critiquable ou bien est-ce faire preuve de réalisme* ? »[1787]

Les humanitaires sont donc partagés entre un idéal d'autonomie informationnelle et un risque de paternalisme[1788]. Pour Alexandre Jaunet, chercheur spécialisé en éthique médicale, Cela impliquerait de dépasser cette opposition en substituant un modèle du consentement fondé sur l'autonomie exclusive de l'individu à un modèle fondé sur celui de la confiance. Il fait référence à Annette Baier, philosophe spécialiste de Hume, ayant mené une réflexion critique sur le libéralisme moral et pouvant être rattachée aux théories du care[1789]. L'objet des réflexions d'Annette Baier consiste en effet à réfléchir sur la forme que pourrait prendre un cadre éthique d'une relation entre personnes inégales en sortant du modèle de l'autonomie. Afin de se préserver des abus de confiance, cette interaction ne doit pas reposer sur de la peur, de l'exploitation ou de la manipulation. Pour Alexandre Jaunet, le professionnalisme est un critère garantissant le caractère moral de la relation thérapeutique. Acceptant sa propre vulnérabilité, il fait le choix d'une remise de soi en faisant confiance à son médecin[1790]. Or, la confiance est un élément essentiel de la relation humanitaire, aussi bien sur le terrain physique que numérique[1791]. Le DPO Massimo Marelli surligne régulièrement l'importance de s'assurer la sécurité de l'information afin de conserver la confiance des bénéficiaires.

On a donc esquissé un panorama des différentes difficultés associées à la collecte du consentement. Ce difficile renoncement au consentement est dû à son profond ancrage dans le cadrage éthique des humanitaires. Et ceci pourrait expliquer pourquoi il n'est pas évident pour eux de ne plus s'y référer, alors qu'ils sont aux prises avec de nombreux obstacles dans

---

[1786] « the concept of 'duty of care' is particularly useful, shifting the burden of responsibility back to the institutional entity rather than the individual, which is ultimately responsible for how and if data about vulnerable constituencies is used. » RAFTREE, Linda, "Rethinking informed consent in the digital age", *Wait… What ?, 02*/11/2016. https://lindaraftree.com/2016/11/02/rethinking-informed-consent-in-the-digital-age/ (commentaire d'un article du blog).

[1787] Entretien n°6, OI3, Information manager officer, 22/11/2019.

[1788]SOLOVE, Daniel J., "Privacy Self-Management and the Consent Dilemma", *Harvard Law Review 1880*, 2013, GWU Law School Public Law

[1789] BAIER, Annette, *Moral Prejudices : essays on ethics*, Harvard University press, 1995, 369 p.

[1790] JAUNAIT Alexandre, « Comment peut-on être paternaliste ? Confiance et consentement dans la relation médecin-patient », *Raisons politiques*, 2003/3 (n° 11), p. 59-79. https://www.cairn.info/revue-raisons-politiques-2003-3-page-59.htm

[1791]"La confiance est une condition préalable essentielle à l'accès. Il s'agit de la confiance à la fois (1) des populations affectées et (2) des parties au conflit armé et des acteurs dans d'autres situations de violence. En ce qui concerne les populations affectées, la confiance est établie par la garantie que tout engagement entre elles et le CICR sera exclusivement humanitaire". "An essential precondition for access is trust. This relates to the trust of both (1) affected populations and (2) parties to the armed conflict and actors in other situations of violence. As far as affected populations are concerned, trust is established by the guarantee that any engagement between them and the ICRC will be exclusively humanitarian." MARELLI, Massimo, "Hacking Humanitarians: Defining the Cyber Perimeter and Developing a Cyber Security Strategy for International Humanitarian Organizations in Digital Transformation", *International Review of the Red Cross,* 2020, 102 (913), p. 367–387, https://ssrn.com/abstract=3969883

FAST, Larissa, " Governing Data: Relationships, Trust & Ethics in Leveraging Data & Technology in Service of Humanitarian Health Delivery", *Daedalus* 2023, (2), 2023, p. 125–140

sa mise en œuvre. Le fait de se concentrer sur base légale d'intérêt légitime est alors présenté comme une forme de pragmatisme. Mais cela implique d'accorder une plus grande responsabilité dans la gestion de l'information, surtout s'il s'agit de données sensibles, et ce alors qu'on a pu faire le constat dans le chapitre 2 d'une professionnalisation inachevée des usages du numérique.

## Chapitre 07 — Blockchains humanitaires et autodétermination informationnelle des bénéficiaires

### Introduction de chapitre

Ce nouveau chapitre poursuit notre questionnement sur les modalités de préservation de la dignité des personnes dans l'espace numérique humanitaire. Cette fois-ci, on explorera les différentes manières d'outiller technologiquement le consentement et l'autodétermination informationnelle des bénéficiaires.

En sommes, la partie précédente était consacrée au contrôle des individus sur leurs données sous un angle juridique. On y a examiné les nombreuses interrogations liées au respect du consentement, tel qu'il est défini par le RGPD, dans l'humanitaire. Le point de vue adopté sera maintenant plus technique puisqu'il sera question de dispositifs technologiques décentralisés et distribués et de la façon dont ils peuvent assurer une forme d'autodétermination informationnelle. Cela dit, n'oublions pas que les deux approches ne sont pas contradictoires. La relation entre architecture technique et droit a été explorée par des auteurs comme Lawrence Lessig[1792] ou Joël Reidenberg[1793]. On peut aussi citer les travaux de Francesca Musiani ou encore Primavera de Filippi sur les liens entre la gouvernance politique et la conception technique des infrastructures. Ces dernières influent sur les usages des internautes, leurs marges de liberté et d'action. Les choix d'architecture des réseaux impliquent une certaine répartition des compétences et des responsabilités entre les acteurs concernés, les utilisateurs, les opérateurs de réseaux, etc. [1794] . Ainsi, l'autodétermination informationnelle peut s'incarner dans différents objets techniques, comme les « personal Information Management Systems » (PIMS)[1795] ou les blockchains, soit une architecture différant d'une gestion centralisée d'un réseau, où un acteur unique contrôle la finalité d'usage des données. Cette décentralisation peut être plus ou moins grande, et prend plusieurs formes, notamment fédérées ou distribuées. Dans des réseaux fédérés, il existe une multitude de centres, gérés par un acteur autour duquel s'agrègent des utilisateurs. Dans des réseaux distribués, chaque point est connecté à un autre et ne communique pas avec un centre. L'information peut transiter de pair en pair. Et l'ensemble des ressources du système ne se trouve pas dans un même endroit physique, il est réparti au contraire entre plusieurs machines[1796]. Les blockchains sont caractérisées par ce type d'architecture.

---

[1792] LESSIG, Lawrence, « code is law, on liberty in cyberspace », Harvard Magazine, January 2000.

[1793] REIDENBERG, Joel, " Lex Informatica: The Formulation of Information Policy Rules through Technology ", 76 *Tex. L. Rev*., 553, p.1997-1998

[1794] MUSIANI, Francesca**,** « L'invisible qui façonne. Études d'infrastructure et gouvernance d'Internet », *Tracés. Revue de Sciences humaines*, 35, 2018, http://journals.openedition.org/traces/8419
MUSIANI, F., « Network architecture as internet governance », *Internet Policy Review*, 2(4), 2013 https://doi.org/10.14763/2013.4.208
DE FILIPPI, Primavera, BOURCIER, Danièle, « Réseaux et gouvernance. Le cas des architectures distribuées sur internet », *Pensée plurielle*, 2014/2 (n° 36), p. 37-53. https://www.cairn.info/revue-pensee-plurielle-2014-2-page-37.htm

[1795] JANSSEN, H., SINGH, J, "Personal Information Management Systems", *Internet Policy Review*, *11*(2), 2022 https://doi.org/10.14763/2022.2.1659

[1796] MUSIANI, Francesca. « Architecture distribuée/répartie/décentralisée/P2P », In : MÉADEL, Cécile, MUSIANI, Francesca, *Abécédaire des architectures distribuées*,Paris : Presses des Mines, 2015, <http://books.openedition.org/pressesmines/2106>.

Or vers la fin des années 2010, une vague d'enthousiasme pour les blockchains aurait touché l'humanitaire[1797]. L'usage de blockchains est entouré de nombreux espoirs contrastant avec le caractère éphémère des projets[1798], dû à un manque de financement suivi sur le long terme. Quoi qu'il en soit, les blockchains ont pu apparaitre comme autant de « solutions » pour toute une série de problèmes concernant l'humanitaire. Elles permettraient d'améliorer la transparence des chaines logistiques, des donations, et contribuer aux exigences de redevabilité des bailleurs. Les dossiers médicaux à base de blockchain permettraient d'assurer une continuité de stockage des données de santé. Ils ambitionnent, toujours grâce aux blockchains, à mettre l'usager au centre du dispositif en laissant au patient une certaine autonomie de gestion de ses informations. En outre, des programmes de transferts monétaires recourent à de la cryptomonnaie afin de contourner (avec plus ou moins de succès) les mesures de conformité bancaire (cf. chapitre 4). Autre point, les programmes de transfert monétaire nécessitent que les individus disposent de papiers d'identification officiels. On verra que des dispositifs décentralisés d'identité fondés sur des blockchains se proposent de pallier ce problème, tout en laissant aux usagers une plus grande maitrise de ces données[1799]. C'est ce dernier sujet qui va nous occuper dans les lignes qui suivent. Notre axe majeur concernera la possibilité qu'offrent ces outils techniques de reconfigurer les relations de pouvoir entre ONG et bénéficiaires. D'emblée, on peut se demander s'il est possible d'assurer un meilleur contrôle de données grâce à des dispositifs technologiques complexes, des blockchains, pour des personnes qualifiées de « vulnérables », parfois dotés d'une culture numérique faible. En outre, les ONG sont prises entre plusieurs objectifs contradictoires. Elles peuvent défendre l'idée d'une technologie émancipatrice, permettant aux utilisateurs de mieux contrôler leurs données, mais elles doivent aussi rendre compte de leurs activités aux bailleurs. Et ces tensions entre transparence et autodétermination informationnelle se traduisent dans l'architecture des blockchains. Ajoutons que plus généralement, ces projets malgré leur idéal émancipateur n'échappent pas à des dynamiques de pouvoir plus verticales, et au contrôle des États, surtout lorsqu'il est question de programmes à destination de réfugiés. Un contexte politique que, comme le rappelle Margie Chessman, les concepteurs de

[1797] ZUCCHINI, Giulio, LOISEAU, Camille, CAPATAZ GORDILO, Carlos, ANDUJAR PEREZ, Julian, BLANCO PENALVER, Ana, SCRUBY, Celia, "How blockchain can possibly improve humanitarian action, community engagement, cash transfer & traceability », *Red Social Innovation*, March 2023 https://red-social-innovation.com/wp-content/uploads/2023/06/Blockchain_EN.pdf
JOHNSON, Simon, "Humanitarian technology hype 2018", 19/03/2018 https://medium.com/hetco-zine/humanitarian-technology-hype-2018-96f0ed993140

[1798] « While there have been a number of projects in this space, they are largely one-off pilots which receive some media coverage at their launch – particularly when new technologies are involved, such as Self Sovereign Identity (which is discussed below)– but which then disappear from public view without even any indication of whether they succeeded or failed (DIGID is a notable exception in this case). As a result there is little coherence or continuity when compared to UN-led projects; the latter, while opaque, usually fit into longer-term strategic plans and/ business processes. For NGOs to match this will require their own multi-year funding. »

[1799] COPPI, Giulio, FAST, Larissa, "Blockchain and distributed ledger technologies in the humanitarian sector", HPG Commissioned Report, Overseas Development Institute (ODI), 2019,
https://odi.org/en/publications/blockchain-and-distributed-ledger-technologies-in-the-humanitarian-sector/
THYLIN, Theresia, NOVELO DUARTE, María Fernanda, " Leveraging blockchain technology in humanitarian settings – opportunities and risks for women and girls", *Gender & Development*, 27:2, 2019, p. 317-336.
Danish Red Cross, Mercy Corps, Hiveonline, « The Next generation humanitarian distributed platform », 2020, https://www.mercycorps.org/sites/default/files/2020-11/The-Next-Generation-Humanitarian-Distributed-Platform-v3.pdf
WANG, Fennie, DE FILIPPI, Primavera, « Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion », *Frontiers in Blockchain*, 2020. https://www.frontiersin.org/articles/10.3389/fbloc.2019.00028/full
CHRISTOPHER, Allen, "The Path to Self-Sovereign Identity"**,** April 25 2016
http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

blockchain ne prennent pas nécessairement en compte[1800]. Et on gardera en tête que, comme l'avertit Andrej Zwitter, : « certaines caractéristiques de la technologie Blockchain sont souvent considérées comme essentialisé et intrinsèques, nous avons indiqué qu'il est indispensable de comprendre que des caractéristiques telles que la décentralisation, la transparence et l'immutabilité doivent être considérées comme le résultat de choix intentionnels dans le développement de ces architectures technologiques. Ces caractéristiques ne sont en aucun cas nécessaires ou intrinsèquement bonnes. »[1801] Notre premier cas d'étude concernera un projet de transfert monétaire du World Food Program intitulé « Building Blocks ». On verra que, d'emblée, il apparait que Building Block accorde aux bénéficiaires peu de contrôle sur leurs données, et ce en dépit du fait qu'un des objectifs affichés des programmes de « cash transfert » est l'émancipation (l'empowerment) des bénéficiaires. Le projet se concentre sur des objectifs d'efficacité et de redevabilité, et son architecture est très centralisée, et repose en outre sur des choix questionnables d'un point de vue de la protection des données. Ensuite, on se penchera sur un autre exemple intéressant : Iryo, un archétype de blockchain médicale, souhaitant rendre l'utilisateur maitre de ses données. Or la version de la blockchain destinée aux réfugiés ne laisse pas la même marge de contrôle, point qu'on interrogera. Enfin, notre dernier cas d'étude concerne un projet de l'IFRC et du consortium Dignified identity for cash delivery (DIGID). Comme le nom du projet l'indique, les ONG accordent une grande importance à la dignité des bénéficiaires et à leur autonomie, tout en faisant face à des rapports de pouvoir qu'un dispositif technique ne permette pas totalement d'atténuer.

Pour résumer, notre chapitre sera donc organisé en deux temps. Une première partie se veut plus générale. Les blockchains étant des objets relativement techniques, il nous a paru nécessaire de prendre un moment pour les décrire. On en profitera pour préciser les liens entre blockchains et autodétermination informationnelle. Ensuite, une fois notre cadre posé, on en viendra à nos cas d'étude et à des blockchains humanitaires. On prendra évidemment soin de ne pas se limiter à l'échelle technique, on inclura évidemment dans notre analyse des éléments contextuels et sociopolitiques propres au secteur humanitaire.

---

[1800] « Rather than social and political agency, with blockchain refugees gain the authority to only manage what UNHCR acknowledges about them for the purposes of interest to UNHCR management of refugee populations overall, in their ultimate objective of knowing refugees in the presumed governable "world of refugees." By attempting to "liberate" refugees through integration of their data within a biometrically driven blockchain network, UNHCR seeks to render an immutable physical feature of refugees' bodies the source and representative of their identities. Thus, rather than gaining liberty in assistance and protection, refugees become dictated to in their movements and claims to whatever UNHCR permits persons to represent as coded data in relation to the UNHCR's organizational objectives of assistance and protection and not in relation to the refugees as social and political beings interested in self-determination beyond UNHCR-centered functions. »
FRANKE, Mark, "Refugees' loss of self-determination in UNHCR operations through the gaining of identity in blockchain technology", *Politics, Groups, and Identities*, 10:1, 2020, p.21-40, DOI: 10.1080/21565503.2020.1748069
"The emancipatory potential of decentralized, user-owned modes of identification came into tension with the geopolitical reality of the nation-state system in which states' prerogative is to control the legitimate means of movement – or, indeed, identification (Torpey 2000). In this reality, technologies of identification have since 9/11 intensified regimes of surveillance, securitisation and control (Bennett and Lyon 2008). "
CHEESMAN, Margie, " Self-Sovereignty for Refugees? The Contested Horizons of Digital Identity", *Geopolitics,* 27:1, 2022, p.134-159,
SLAVIN, Aiden, "Distributed Ledger Identification Systems in the Humanitarian Sector." Sovrin Foundation,2019 https://sovrin.org/wp-content/uploads/14A-Report.pdf

[1801] "While certain features of Blockchain technology are often considered to be absolute and intrinsic, we indicated that it is critical to realize that characteristics such as decentralization, transparency, and immutability should be understood as outcomes of intentional choices in developing these technological architectures. These features are by no means necessary or intrinsically good."
ZWITTER, Andrej, BOISSE-DESPIAUX, Mathilde, « Blockchain for humanitarian action and development aid », *Journal of international humanitarian action,* 3:16, 2018

## Section 1 — Réseaux décentralisés, distribués et autodétermination informationnelle

Avant toute chose, il est nécessaire de préciser en quoi des dispositifs technologiques décentralisés et distribués — et notamment des blockchains — offriraient aux usagers une plus grande maitrise de leurs données.

L'idée est loin d'être nouvelle. À la fin des années 1990 se sont développés des dispositifs décentralisés permettant de négocier sa vie privée en ligne, baptisés les « Personal Information Management Systems » (PIMS)[1802] . Les chercheurs Arvind Narayanan et Helen Nissenbaum ont retracé une partie de leur histoire et les décrivent comme : « un écosystème, qui comprend le plus souvent une plateforme fournissant l'infrastructure du PIMS. La plateforme propose aux utilisateurs certains composants pour le traitement de leurs données personnelles. Au sein de cet écosystème, des tiers cherchent à traiter les données des utilisateurs (…). Les PIMS utilisent des mesures techniques, juridiques et organisationnelles qui permettent aux utilisateurs de gérer et de contrôler leurs données, et de garantir et de valider que les comportements des tiers sont conformes aux exigences de l'utilisateur et de la plateforme. » [1803] Mais les PIMS ont périclité ou sont restés marginaux face au rôle grandissant des GAFAM et à leur contrôle croissant d'Internet. Cet idéal technologique aurait connu néanmoins un récent sursaut avec ce qui aurait été nommé le « Web.3 », ou encore « DWEB »[1804]. Ce dernier engloberait une série de dispositifs techniques, NFT, crypto, etc., dont les blockchains font aussi partie, mais dont la portée et le développement resteraient pour le moment incertain au sein de l'écosystème numérique plus global.

À ce stade, il est nécessaire, au regard de la complexité technique du sujet, d'apporter quelques éléments de définition. En simplifiant à l'extrême, on pourrait dire qu'une blockchain est une base de données distribuée, infalsifiable, sur laquelle les informations enregistrées sont soumises au contrôle des acteurs d'un réseau.

Aucune autorité unique n'est responsable de la maintenance d'une blockchain. Chaque ordinateur d'un réseau pair à pair stocke une copie du registre, et les transactions sont vérifiées au moyen d'un mécanisme de consensus décentralisé. En clair, les transactions sont enregistrées dans des unités permanentes et horodatées, soit des blocs. Ces derniers sont reliés (chaînés) entre eux par un hachage cryptographique créé en utilisant le contenu du bloc

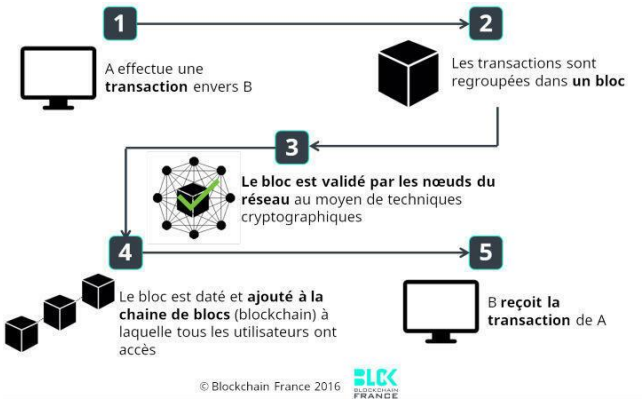
---

[1802] NARAYANAN, Arvind, NISSENBAUM, Helen, BAROCAS, Solon, TOUBIANA, Vincent, BONEH Dan, "A critical look at decentralized personal data architectures", https://ar5iv.labs.arxiv.org/html/1202.4503

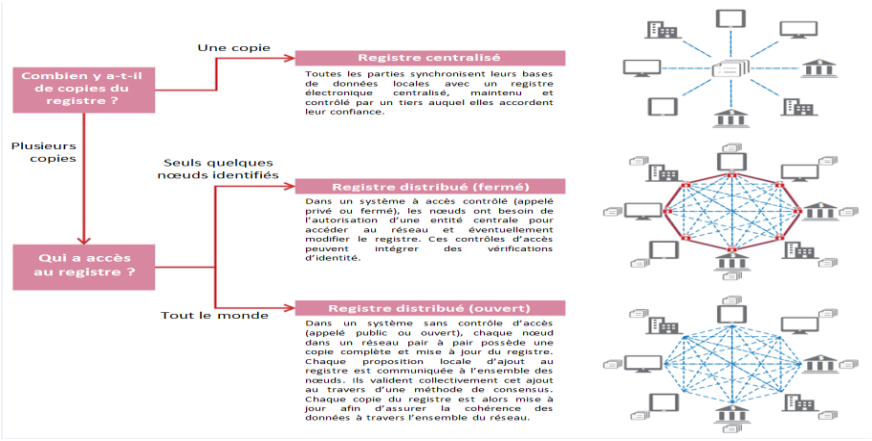
[1803]" PIMS typically involve an ecosystem, which generally entails a *platform* providing the PIMS infrastructure. The platform provides *users with some* components for handling their personal data. Within this ecosystem, *third parties* seek to process user data (Janssen et al., 2020b). PIMS employ technical, legal and organizational measures that enable users to manage and control their data, and to ensure and validate that the behaviours of third-parties accord with user and platform requirements", JANSSEN, H. SINGH, J. "Personal Information Management Systems", *Internet Policy Review*, *11*(2), 2022 https://doi.org/10.14763/2022.2.1659

[1804]« Le DWeb consiste donc à la "redécentralisation" des contenus et des interactions, afin que les utilisateurs gardent le contrôle de leurs données, se connectent, interagissent et échangent des messages, sans intermédiaire. »
FINES SCHLUMBERGER, Jacques-André, « DWEB », *La Revue européenne des médias et du numérique*, 2018
https://la-rem.eu/2018/11/dweb/

précédent[1805]. Les liens de hachage font qu'il est impossible de modifier les données d'un bloc sans apporter des modifications à chaque bloc suivant de la chaîne. Ceci explique le caractère immuable d'une blockchain : toute tentative de modification ou de suppression d'informations brisera la chaîne cryptographique. Ajoutons que théoriquement, du fait de cette architecture décentralisée, chacun peut assurer l'authenticité d'une opération, la blockchain ayant une finalité de « désintermédiation ». Et l'authenticité d'une information — identité numérique, titre de propriété, de mariage, certificat… — n'est plus validée par un tiers de confiance (une banque, un notaire).




Point important, il existe plusieurs types de blockchain : les blockchains privées ou fermées, dans lesquelles un acteur contrôle l'accès au registre ; les blockchains publiques qui sont ouvertes à toute personne sans système de vérification.




*Source : OPECST d'après le chapitre « Cryptocurrencies : looking beyond the hype » du rapport annuel 2018 de la Banque des règlements internationaux, et la note de la Banque mondiale*

[1805] En informatique, les fonctions de « hachage » permettent de convertir n'importe quel ensemble de données numériques en un hash, c'est-à-dire en une courte suite binaire qui lui est propre. L'algorithme de compression utilisé à cet effet est appelé « fonction de hachage cryptographique ».

*« Distributed ledger technology and blockchain » par H.Natarajan, S.Krause and H.Gradstein, 2017*.[1806]

Originellement, les blockchains ont émergé au sein de groupes d'acteurs baignant dans une culture crypto-anarchiste, caractérisée par une méfiance à l'égard des institutions traditionnelles. Les blockchains illustrent cette vision. Elles permettent de passer outre une autorité centrale du fait de leur nature distribuée, qui assure une forme d'autodétermination, soit la possibilité pour les communautés de définir la nature de l'infrastructure technique utilisée.

Primavera de Filippi nuance ce propos. Des blockchains peuvent être techniquement décentralisées, mais leurs effets sociopolitiques restent centralisés du fait des compétences techniques nécessaires à la gestion des nœuds. Les usagers n'ont pas tous le même niveau de maitrise du réseau. Il peut s'en suivre d'après la chercheuse l'émergence de gouvernances technocratiques[1807], d'où le risque que la décentralisation technique, plutôt que de favoriser l'« empowerment » des acteurs, décentralise les risques et crée de nouvelles inégalités[1808].

Autre point, la nature distribuée des blockchains entraine en contrepartie une augmentation des coûts de coordination au sein des réseaux : « en l'absence d'une autorité centrale chargée de contrôler le réseau, les utilisateurs malveillants pourraient être tentés de "tricher" avec le système pour leur propre profit. La transparence peut donc être considérée comme un moyen pour le réseau de se contrôler lui-même, en octroyant la possibilité aux usagers de vérifier collectivement la légitimité de chaque transaction sur le réseau. »[1809]

Pour Primavera de Filippi, plus un réseau est décentralisé, moins il repose sur la confiance, et plus il repose sur la transparence. Elle différencie deux types de transparence : au niveau du contenu, au niveau du protocole réseau (qui limite le partage d'information au niveau des

---

[1806] ANDERSON, Allison, KANE, Seth, "Identities for opportunities, a feasibility study for overcoming the Rohingya's statelessness challenges via blockchain-based digital solutions", University of Washington, 2018, https://rohingyaproject.com/identities-for-opportunity-university-of-washington/

"The Ethereum blockchain platform has the most nodes and is the most architecturally decentralized. Ethereum is also the most distributed regarding latency.15 Ethereum's nodes are widely distributed across the world and have more homegrown entities, giving it greater political decentralization.16 In contrast, most of Bitcoin's nodes are in data centers, limiting its decentralization. Ethereum nodes are also primarily operated by individuals while Bitcoin's nodes have a higher percentage of institutions and organizations serving as operators"

[1807]DE FILIPPI, P., LOVELUCK, B. "The invisible politics of Bitcoin: governance crisis of a decentralized infrastructure", *Internet Policy Review*, 5(3),2016, https://doi.org/10.14763/2016.3.427

"Implicit in the governance structure of Bitcoin is the idea that the Bitcoin core developers (together with a small number of technical experts) are – by virtue of their technical expertise – the most likely to come up with the right decision as to the specific set of technical features that should be implemented in the platform. Such a technocratic approach to governance is problematic in that it goes counter to the original conception of the Bitcoin project. There exists, therefore, an obvious discrepancy between the libertarian vision of Bitcoin as a decentralised infrastructure that cannot be regulated by any third party institution, and the actual governance structure that dictates the technological development of Bitcoin – which, in spite of its open source nature, is highly centralised and undemocratic. While the (a)political dimension of the former has been praised or at least acknowledged by many, the latter has remained, for a long time, invisible to the public: the technical decisions to be taken by the Bitcoin developers were not presented as political decisions, and were therefore never debated as such.

[1808] DE FILIPPI, Primavera, « Ethereum « , In : MÉADEL, Cécile, MUSIANI, Francesca (dir*), Abécédaire des architectures distribuées* , Paris : Presses des Mines, 2015 http://books.openedition.org/pressesmines/2118

BODÓ, B., BREKKE, J. K., HOEPMAN, J.-H. « Decentralisation in the blockchain space », *Internet Policy Review*, *10*(2), 2021https://doi.org/10.14763/2021.2.1560

[1809] DE FILIPPI, Primavera, « The Interplay between Decentralization and Privacy: The Case of Blockchain Technologies », *Journal of Peer Production*, Issue n.7 , 2016

"in absence of a central authority in charge of policing the network, malicious users migth be tempted to "cheat" the system for their own gain. Transparency can thus be regarded as a means for the network to police itself, by enabling users to collectively verify the legitimacy of every networl transaction"

métadonnées). Il existe un jeu de bascule entre ces deux pôles de confidentialité : « Par conséquent, si la décentralisation peut contribuer à promouvoir la vie privée et la confidentialité des utilisateurs au niveau du contenu, elle peut toutefois se faire au prix d'une transparence radicale au niveau du protocole ou des métadonnées. » [1810]

Par exemple, des cryptomonnaies ayant pour support des blockchains fonctionnent grâce à la cryptographie asymétrique. Pour rappel, concernant les Bitcoins, un identifiant unique leur est attribué (une « adresse » constituée d'une série de chiffres et de lettres). Cet identifiant est a priori « anonyme ». Il n'est pas composé d'éléments directement identifiants. Il s'agit d'une clef publique, cette dernière va être stockée sur la blockchain pour assurer un minimum de transparence et elle apparaitra à chaque nouvelle transaction. L'utilisateur détient aussi une clef privée, qui lui sert de « mot de passe » et lui permet d'accéder à ses fonds et de contrôler ses transactions. Seul l'utilisateur peut connaitre, théoriquement, sa clef privée. Mais, l'anonymat d'un utilisateur de blockchain n'est pas absolu. Et plus une clef publique est utilisée, plus le risque d'être re-identifié est fort. Des entreprises comme Coinanalytics, Coinometrics ou Elliptic vendent des logiciels pour identifier des adresses connues comme étant reliées à des activités criminelles. L'intérêt est de se conformer à des régulations anti-blanchiment d'argent, comme on l'a vu dans le chapitre 4.

Cela dit, plus que le diptyque visibilité/invisibilité, anonymat/identification, le point qui nous intéresse dans ce chapitre est relatif à la possibilité de contrôler ses données. Or, il se trouve que les blockchains peuvent servir à garder la main sur les informations constitutives de l'identité d'une personne (son âge, son nom, son genre, etc.). En effet, les blockchains peuvent servir de fondement à des dispositifs d'identité souveraine (Self sovereign identity) qui promettent une gestion de l'identité par l'utilisateur lui-même. Ils incarnent donc l'idée d'autodétermination informationnelle[1811]. Christopher Allen et Jeff Garzik, informaticiens férus de techniques de chiffrement et de bitcoin, ont popularisé l'idée de systèmes d'identité souverains (self sovereign identity en anglais — soit SSI)[1812].

Tous les projets de système d'identité souverain ne recourent pas à des blockchains, cependant, leur nature décentralisée parait a priori adaptée à ces derniers. Dans des systèmes d'identification traditionnels, l'identité de la personne est définie selon la perspective d'une autorité pour une finalité spécifique. Selon les partisans des SSI, les personnes elles-mêmes peuvent choisir — dans une certaine mesure — les données les définissant.

Plus concrètement, les utilisateurs de blockchains détiennent une paire de clefs publiques et privées. L'accès aux différentes données est permis par une clef privée, détenue par la personne qui contrôle le portefeuille d'identité. Par voie de conséquence, l'utilisateur garde la main sur ses données selon des systèmes de permissions révocables, sans avoir à passer par une partie tierce. L'utilisateur peut aussi contrôler l'accès à des données stockées « hors chaine », sous forme chiffrée. Dans ce cas, les utilisateurs ont recours à leur clef privée pour

---

[1810] DE FILIPPI, Primavera, ibid. « hence if decentralisation can contribute to promoting users privacy and confidentiality at the content layer, it might, however, come at the price of radical transparency at the protocol or metadata layer. »

[1811] COUTOR, Sophie, HENNEBERT,Christine, FAHER, Mourad, "Blockchain et identification numérique", 2020 https://www.vie-publique.fr/files/rapport/pdf/280103.pdf

[1812] CHRISTOPHER, Allen, "The Path to Self-Sovereign Identity", 2016 http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

autoriser ou non l'accès à leurs données. En outre, les conditions de partage des données entre utilisateurs peuvent être prévues par des « contrats intelligents » en amont, et chaque accès demeure conditionné à l'accord de l'utilisateur[1813]. Les contrats intelligents servent alors à spécifier les droits d'accès et de lecture, la durée de validité du consentement. La révocation de ce dernier serait facilitée puisqu'il serait configurable depuis une interface et non pas via une médiation en face-à-face. Les choix des utilisateurs seraient documentés, et automatisés.

Les blockchains sont alors présentées comme des moyens de renforcer l'autonomie des usagers. Grâce à des contrats intelligents, il est possible d'enregistrer les conditions d'échange de données entre l'utilisateur et les fournisseurs de service [1814]. Cependant, la plupart des droits accordés aux personnes concernées selon le RGPD ne sont pas applicables aux blockchains. Le caractère immuable des blockchains complique le retrait du consentement, ainsi que la possibilité de rectifier ou supprimer des données.

Toutefois les SSI conservent dans une certaine mesure un fonctionnement triangulaire. Le bénéficiaire présente à autrui des « accréditations » (informations sur son âge, nom, documents administratifs, etc.) validées au préalable par un tiers de confiance. Précisons que : « la blockchain se prête bien à la conservation des attestations, des preuves sur des assertions certifiées, ainsi qu'à la gestion des certificats numériques émanant d'acteurs d'identité publique (acteurs étatiques souverains), ou encore à la traçabilité des services rendus. Elle fournit au vérificateur, de façon décentralisée, une preuve permettant de vérifier la validité, l'authenticité et l'intégrité des données. Le prestataire de service peut se passer de l'intermédiaire de vérification et peut endosser directement ce rôle en accédant à la blockchain. Tout certificateur d'attributs ou de documents authentiques a la possibilité d'enregistrer les preuves et attestations sur la blockchain. »[1815]

## Section 2 — Blockchain humanitaire

Une fois notre objet technique présenté, on peut en venir à nos cas d'usage humanitaires. On partira d'un paradoxe : les blockchains sont des dispositifs techniques relativement complexes, alors que le public cible des projets qu'on va évoquer manque dans une certaine mesure de littératie numérique. Au fil de la section qui suit, on détaillera les différentes façons dont les ONG font face à cette contradiction.

---

[1813]Les « contrats intelligents » seraient caractérisés par une absence d'ambiguïté textuelle, car leurs dispositions sont rédigées dans un langage formel qui doit être compris par une machine. Ce sont des programmes informatiques qui facilitent la négociation, la vérification et l'exécution d'un contrat, voire qui peuvent de se passer d'un accord contractuel sous-jacent entre les parties.
Les « contrats intelligents » seraient caractérisés par une absence d'ambiguïté textuelle, car leurs dispositions sont rédigées dans un langage formel qui doit être compris par une machine. Ce sont des programmes informatiques qui facilitent la négociation, la vérification et l'exécution d'un contrat, voire qui peuvent de se passer d'un accord contractuel sous-jacent entre les parties.
Primavera de Filippi, Primavera, HASSAN, Samer, " Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Code." First Monday, 2016.

[1814] European Parliament research service, "Blockchain and the General data protection regulation, can distributed ledgers be squared with European data protection law?", 2019, https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf

[1815] HENNEBERT, Christine, "Blockchain et identification numérique, restitution des ateliers du groupe de travail « blockchain et identité », octobre 2020

### *§ 1 - WFP, Building Blocks*

Notre premier exemple concerne Building Block, une blockchain développée au sein du WFP pour soutenir ses programmes de transfert monétaire, notamment en Jordanie. Sachant que le WFP recourt aux programmes de « cash transfert » depuis 2008. Actuellement, ce type d'opération représenterait environ 35 % de l'ensemble de l'assistance du WFP[1816]. Le projet de portefeuille à base de blockchain concerne une minorité des opérations, ayant lieu au Bangladesh, en Jordanie, au Liban et en Ukraine. Pour donner un ordre d'idée, en 2020, le WFP affirme avoir transféré un montant de 2,1 milliards de dollars de pouvoir d'achat aux habitants de 67 pays[1817]. Sachant que les opérations de transfert monétaire englobent différentes modalités, allant d'espèces liquides, à des cartes de retraits ATM aux portes-feuilles numériques et enfin aux blockchains. Il n'existe pas de données publiques concernant le pourcentage d'opération utilisant telle ou telle technologie. Mais il semblerait que le WFP associe les programmes de transferts monétaires avec la transformation numérique de l'organisation[1818]. Ainsi, en Jordanie l'organisation a impulsé une transition des programmes de transfert monétaire vers des portefeuilles numériques[1819].

Sachant que pour l'ensemble des programmes de transfert monétaire l'organisation humanitaire doit collaborer avec des partenaires financiers, avec les contraintes qu'on connait, notamment quant aux mesures de KYC (cf. chapitre 4). Le WFP procure une liste de bénéficiaires à une banque et se plie aux prérequis en matière de conformité bancaire. Les bénéficiaires peuvent ensuite se rendre dans un magasin autorisé pour faire leurs achats. Dans le cas du camp de Zaatari, en Jordanie, le vendeur local identifie le bénéficiaire avec un scan d'iris. Le vendeur valide ensuite la vente et reçoit un paiement de la part du WFP. La procédure nécessite néanmoins, selon le WFP, des charges administratives et financières. Les transferts monétaires nécessitent de gérer auprès d'une banque des opérations de centaines de bénéficiaires. Pour alléger la lourdeur de ce processus, Houman Haddad aurait eu l'idée

---

[1816] Ibid.

[1817] https://fr.wfp.org/transferts-monetaires

[1818] « Technological developments have opened new opportunities for many people who are underserved by traditional financial service providers to take advantage of a range of financial services and products that bring them into increasingly digitally connected societies and economies. », » les progrès technologiques ont ouvert de nouvelles perspectives à de nombreuses personnes mal desservies par les prestataires de services financiers traditionnels, leur permettant de bénéficier d'une gamme de services et de produits financiers qui les intègrent dans des sociétés et des économies de plus en plus connectées au numérique. »
GIZ, UNHCR, WFP, « Financial inclusion of refugees in Jordan, knowledge note », November2022, https://www.giz.de/en/downloads/giz2022-en-financial-inclusion-refugees-jordan.pdf

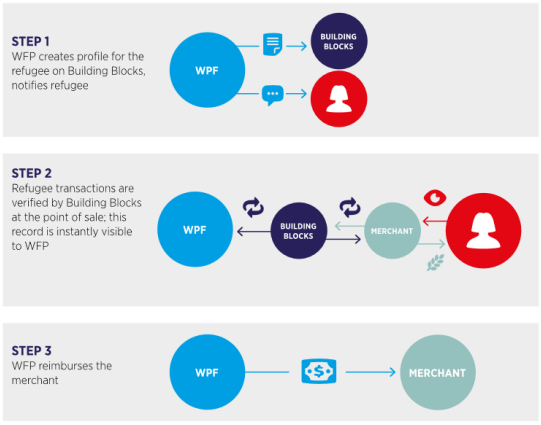
[1819] « En ce qui concerne les réfugiés vivant dans des communautés, la transition vers l'argent mobile a commencé en 2022, mais les cartes électroniques sont toujours utilisées. En 2020-21, le WFP a procédé à une évaluation technique des sept fournisseurs de portefeuilles mobiles disponibles en Jordanie et a mené diverses consultations avec les bénéficiaires sur leurs perceptions de l'argent mobile. En 2022, sur la base des résultats opérationnels positifs et des commentaires reçus des bénéficiaires, le WFP a commencé à transférer toute son assistance en espèces vers l'argent mobile, y compris l'assistance alimentaire générale, les moyens de subsistance et les activités d'alimentation scolaire. La transition du WFP vers l'argent mobile a commencé en janvier 2022 et s'achèvera à la mi-2023, avec un objectif de 93 000 portefeuilles appartenant aux bénéficiaires (plus de 440 000 personnes) dans toute la Jordanie, y compris les Syriens vivant dans les communautés et les camps. »,"As for refugees living in communities, the transition to mobile money started in 2022 but e-cards are still in use. In 2020-21, WFP conducted a technical assessment of the seven mobile wallet providers available in Jordan and led various consultations with beneficiaries on their mobile money perceptions. In 2022, based on the positive operational results and feedback received from beneficiaries, WFP started shifting all of its cash assistance to mobile money, including general food assistance, livelihood and school feeding activities. WFP's transition to mobile money started in January 2022 and will be completed by mid-2023, with a target of 93,000 beneficiary- owned wallets (over 440,000 individuals) across Jordan, including Syrians living in communities and camps."
GIZ, UNHCR, WFP, "Financial inclusion of refugees in Jordan, knowledge note", November 2022,https://www.giz.de/en/downloads/giz2022-en-financial-inclusion-refugees-jordan.pdf

courant 2016 d'utiliser une blockchain. L'idée est soumise à l'unité « Accelerator » du WFP, basée à Munich, d'où des partenariats avec des entreprises allemandes[1820]. Un premier pilote est lancé au Pakistan, ainsi qu'au Bangladesh, puis en Jordanie, au camp de Zaatari, en mai 2017. Building Blocks intègre alors le système d'identification biométrique de l'UNHCR déjà en place.

Le système de contrats intelligents de Building Blocks sert à déclencher des virements de fonds aux réfugiés, identifiés grâce à la base de données biométriques du HCR. Un système de blockchain sert à gérer les données de transaction. Plus précisément, des portefeuilles numériques sont créés par l'organisation humanitaire pour les bénéficiaires. Le WFP expédie des fonds sur le portefeuille. Les bénéficiaires effectuent ensuite leurs achats dans des magasins partenaires du programme. Puis l'identification du bénéficiaire est opérée par un scan d'iris. Ce dernier est envoyé sur la base biométrique de l'UNHCR (BIMS). Il est par la suite associé à un identifiant unique, correspondant à une unité familiale. Dans un deuxième temps, l'identifiant est envoyé au système de Building block pour retrouver les clefs de chiffrement reliées aux bénéficiaires. Les clefs permettent de vérifier si les fonds du bénéficiaire sont suffisants ou non pour exécuter une transaction (un contrat intelligent automatise le processus). En cas de réponse affirmative, une transaction est autorisée puis enregistrée sur la blockchain : « Au point de vente, le commerçant emploie un appareil connecté pour authentifier la transaction du réfugié par rapport aux informations sur les droits stockées dans Building Blocks, ce qui confirme automatiquement que le bénéficiaire dispose du "crédit" nécessaire pour effectuer son achat. Chaque transaction est enregistrée dans le profil du réfugié et le WFP utilise ces informations pour payer directement le supermarché, en utilisant la banque de l'entreprise. » [1821] La clef privée est utilisée pour signer les données de transaction, qui sont conservées ensuite sur la blockchain. Précisons qu'elles comprennent le montant, la date et le lieu du retrait, l'identité du bénéficiaire (un code l'identifiant).

[1820] CHENEY, Catherine, « A new mindset for the SDGs? Top takeaways from Singularity university global summit", *Devex*, 16/08/2017 *https://www.devex.com/news/a-new-mindset-for-the-sdgs-top-takeaways-from-singularity-university-s-global-summit-90875*

[1821] « At the point of sale, the merchant uses a connected device to authenticate the refugee's transaction against the entitlement information stored on Building Blocks, automatically confirms that the beneficiary has the 'credit' available to make their purchase. Every transaction is recorded on the refugee's profile, and WFP uses this information to pay the supermarket directly, using their corporate bank" GSMA, "blockchain for development: emerging opportunities for mobile, identity and Aid",2017, https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/12/Blockchain-for-Development.pdf




Source: GSM Association, 2017.

### FONCTIONNEMENT DE BUILDING BLOCKS[1822]

Building Blocks génère donc une certaine quantité de données et métadonnées. Mais selon la communication du WFP, son architecture technique est conçue de manière à protéger la vie privée des bénéficiaires[1823]. Le WFP met en avant le fait qu'avec Building Blocks, le rôle des intermédiaires est réduit. Les acteurs financiers n'occupent plus une place centrale dans la gestion des transferts financiers. Il ne serait plus requis d'envoyer des données sensibles et identifiantes aux banques, afin d'ouvrir un compte. En outre d'après l'organisation humanitaire, les autres parties prenantes de Building Block n'auraient accès qu'à une quantité limitée de données : « Building Block comprend les garanties nécessaires pour que le commerçant, la banque, le prestataire de services de paiement, le réseau de paiement et les autres intermédiaires ne soient pas exposés à des informations qui ne sont pas pertinentes pour leur fonction. »[1824] Par conséquent, l'organisation humanitaire se félicite de pouvoir protéger : « l'anonymat des bénéficiaires tout en permettant aux organisations humanitaires de coordonner les opérations de transfert monétaire à l'aide de leur code d'identification unique. Sans collecter ni stocker de données personnelles supplémentaires, toute organisation humanitaire peut vérifier les distributions passées et présentes de transfert monétaire pour n'importe quel code d'identification unique. »[1825]

Cela dit, l'organisation humanitaire omet de mentionner le fait que Building Blocks repose sur un dispositif très invasif, le scan d'iris, utilisé par l'UNHCR pour enregistrer les exilés. En outre, les Blockchains permettent de contourner les acteurs financiers, mais leur usage implique une

---

[1822] GSMA, « Humanitarian cash and voucher assistance in Jordan: a gateway to mobile financial services », 2020, https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/01/Jordan_Mobile_Money_CVA_Case_Study_Web_Spreads.pdf

[1823] Reports by the joint inspection unit relevant to the work of WFP, WFP, 2022 https://executiveboard.wfp.org/document_download/WFP-0000135925

[1824] « Hence, from a privacy and security standpoint, WFP's Building Blocks incorporates the necessary safeguards to ensure that the merchant, the bank, the payment processor, the payment network, and other intermediaries are not exposed to information that is not relevant to their function. »
ZWITTER, Andrej, GSTREIN, Oskar Josef, "identity and privacy governance", *Frontiers Research Topics*, 2021

[1825] "This protects recipients' anonymity while allowing humanitarian organizations to coordinate CVA using their unique identifier code. Without collecting or storing any additional personal data, any humanitarian organization could verify past and current CVA distributions to any unique identifier code."GSMA, « Humanitarian cash and voucher assistance in Jordan: a gateway to mobile financial services »,2020, https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/01/Jordan_Mobile_Money_CVA_Case_Study_Web_Spreads.pdf

plus grande dépendance à des prestataires techniques. Quel est donc l'accès aux données stockées sur les blockchains par les différentes entreprises concernées ? Nous n'avons pas trouvé d'information sur ce point. Notons simplement qu'un audit interne a été publié surlignant le fait que les mécanismes d'évaluation des partenaires techniques du WFP en matière de protection des données étaient jugés « faibles » [1826].

*Entreprises partenaires de Building Blocks*
Datarella Entreprise allemande spécialisée en données massives et en Blockchain. L'entreprise a développé la blockchain en se basant sur un nœud d'Ethereum.
Baltic Data Science : Entreprise polonaise spécialisée en « data science » et blockchain, affiliée à Datarella. Elle maintient la blockchain et participe à son développement.
Parity technologies : Entreprise développant des « contrats intelligents »
IrisGuard : Entreprise fournissant les solutions biométriques (scanners d'iris) et gérant la base de données « Irisbank » en partenariat avec l'UNHCR.
Amazon Web Services : serveurs cloud stockant les données de la blockchain. En effet, une majeure partie d'Ethereum dépend d'Amazon. AWS gère aussi les clefs privées et publiques de Building Blocks[1827].

De surcroit, les interactions entre les bénéficiaires et les vendeurs laissent également des traces. Si l'on prend le cas d'un vendeur auprès duquel un bénéficiaire vient faire un achat, le commerçant n'a pas besoin de connaitre l'identité exacte de son client. Mais il lui faut tout de même savoir si la personne a été enregistrée (d'où le scan biométrique), et si le montant sur son compte est suffisant. Le vendeur ne connait donc pas le montant exact du solde du compte. Et, il n'est pas précisé s'il a accès ou non à l'historique des transactions, contrairement au WFP, qui gère aussi les clefs de chiffrement de Building Blocks. En effet, rappelons que le WFP a accès aux données de transaction suivantes : les sommes dépensées, lieux et dates des achats. Or, ces métadonnées peuvent conduire à une réidentification du bénéficiaire. Il est en effet toujours possible de reconnaitre une personne en se fondant sur son historique et ses habitudes de consommation, comme l'a démontré le mathématicien Yves Alexandre de Montjoye, en 2015 [1828]. Nous pouvons aussi noter qu'un partenaire de Building Blocks, UNWomen projette d'exploiter ces métadonnées à des finalités d'étude statistique sur les comportements de consommation des bénéficiaires, afin d'améliorer le ciblage de l'allocation de l'aide dans les camps[1829]. Et donc comme souvent les identités des usagers ne sont pas anonymisées, mais pseudonymisées. Pour rappel, le RGPD estime qu'on parle de données pseudonymisées, dès qu'il est possible de « raisonnablement « réidentifier une personne

[1826] Internal audit of third-party access to WFP's data and system Office of the inspector general internal audit report AR/20/02
[1827] DUMITRIU, Petru, "Blockchain applications in the United Nations system: toward a state of readiness", Report of the joint inspection unit, 2020https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2020_7_english.pdf
[1828] De MONTJOYE, Yves-Alexandre et al. , « Unique in the shopping mall: On the reidentifiability of credit card metadata », *Science*, 347,2015,p.536-539
[1829] UN WOMEN JORDAN, "UN WOMEN -WFP Blockchain project for cash transfers in refugee camps", 2021 https://jordan.unwomen.org/sites/default/files/Field Office Jordan/Images/publications/2021/Blockchain pilot project/UN WOMEN-WFP BLOCKCHAIN PILOT PROJECT FOR CASH TRANSFERS IN REFUGEE CAMPS JORDAN CASE STUDY.pdf

concernée. Mais le sens du terme « raisonnablement » ne fait évidemment pas consensus[1830]. Or ce risque peut être minimisé. Pour rappel, on avait vu dans le chapitre 4 que le CICR, dans le cadre d'un projet de transfert monétaire utilisant de la blockchain, prend en compte ce risque. La conception du dispositif atténuerait la possibilité d'une réidentification, les vendeurs n'ayant accès qu'à une clef publique renouvelée régulièrement de manière à limiter la réidentification d'un utilisateur. Ajoutons que le statut des clefs publiques ne fait pas consensus, notamment concernant le fait de savoir si elles sont considérées ou non comme des données personnelles. Pour les juristes Yves Poullet et Antoine Delforge, cela dépend de la qualité de la clef utilisée et de la fréquence de son renouvellement[1831]. Tandis que Ioannis Stathakis, auteur d'un mémoire sur les blockchains humanitaires, se réfère sur ce point à la décision de la Cour de justice européenne « Breyer v Germany » relative au statut des adresses IP comme des données personnelles[1832]. Le même raisonnement peut être appliqué selon lui aux clefs de chiffrement : « même lorsque cette clef n'est pas publique et n'est pas directement liée à une personne donnée, elle peut toujours conduire à l'identification de l'utilisateur à l'aide d'autres données (nom, heure et lieu de la transaction, historique de la transaction, etc.) (…) La Cour de justice européenne a clairement indiqué dans l'affaire "Breyer contre Allemagne" (concernant la possibilité d'identifier des utilisateurs d'adresses IP dynamiques) qu'une adresse liée à un dispositif informatique constitue une donnée à caractère personnel même si les données pertinentes pour identifier cette personne sont détenues par un tiers. »[1833]

Concernant la clef privée, sa protection est également cruciale, puisqu'il s'agit du mot de passe permettant d'avoir accès aux données financières (montant du solde, numéro d'identifiant de l'unité familiale). Les clefs privées sont gérées par le WFP, qui recourt au provider d'Amazon web service pour générer et stocker ses clefs[1834]. Dans l'absolu, il serait cohérent que ce soient les bénéficiaires qui en ont la responsabilité. Mais pour l'organisation humanitaire, la gestion par un tiers — le WFP — de la clef privée de chiffrement est nécessaire au regard du manque supposé de compétence numérique des exilés. D'où le fait que Building Blocks ne garantit pas l'autodétermination informationnelle des bénéficiaires, au grand regret de Petru Dimitru, auteur d'un rapport sur l'usage des blockchains au sein de l'ONU. Ce dernier déclare en effet que : « les bénéficiaires devraient être les gardiens des clefs privées, qui sont liées aux données biométriques des utilisateurs. Bien que cela constitue une solution pratique, comme

---

[1830] POULLET, Y, DELFORGE, A, « Les blockchains : un défi et/ou un outil pour le RGPD ? » , in : COTIGA, Andrea, JACQUEMIN, Hervé, POULLET,Yves (dir.*), Dans Les blockchains et les smart contracts à l'épreuve du droit*, Collection du CRIDS, Numéro 49, Larcier , Bruxelles, 2020, p. 97-135. <http://www.crid.be/pdf/crid5978-/8630.pdf>

[1831] POULLET, Y, DELFORGE, A, ibid.

[1832] Judgment in Case C-582/14 Patrick Breyer v Bundesrepublik Deutschland
https://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=EN

[1833] « Even when this key is not public and not directly related to a certain individual it can still lead to the user's identification with the help of other pieces of data (name, time and location of transaction, transaction history etc.). Even in cases of zero-knowledge applications similar to the "smart contract" developed in the case of "Building Blocks", the identifiability of the data subject does not change. The CJEU has clearly stated in the "*Breyer v Germany*" case (regarding the identifiability of users of dynamic IP addresses) that an address linked to a computing device constitutes personal data even if the data relevant to identify that person is held by a third party. In the present case study, not only does the WFP hold a record of all transactions in its permissioned ledger, but the UN is in possession of biometric data linked to the users of these devices. The answer to whether a refugee is identifiable in the system is therefore positive. »
STATHAKIS, Ioannis, "Critical perspectives on blockchain for humanitarian aid, How does the technology impact procedural fairness and beneficiary data protection?", Master thesis, law&technology, Tilburg University, 2019 https://arno.uvt.nl/show.cgi?fid=149162

[1834] AWS key manager service https://docs.aws.amazon.com/kms/latest/developerguide/overview.html
DUMITRIU, Petru, "Blockchain applications in the United Nations system: toward a state of readiness", Report of the joint inspection unit, 2020https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2020_7_english.pdf

l'a noté le HCR en ce qui concerne le système Building Blocks, elle nie l'une des propriétés essentielles de l'architecture d'une blockchain, à savoir la décentralisation et l'autonomie des utilisateurs. »[1835]

Et de fait, l'« expérience utilisateur » des bénéficiaires reste la même. Ce dernier paie ses achats en scannant son iris, sans avoir nécessairement conscience que leurs données sont gérées par une blockchain. À vrai dire, il est évident qu'un bon nombre de projets de blockchains humanitaires ne donnent pas accès au « backend » aux bénéficiaires comme le rappellent les chercheuses Theresia Thylin et María Fernanda Novelo Duarte [1836]. Et il semblerait d'après la chercheuse Margie Cheesman qu'on n'ait même pas informé les usagers de Building Blocks de la nature d'une blockchain : « mais personne n'a expliqué la blockchain à ces travailleuses : en tant que concept, le personnel d'UNWOMEN a traité la blockchain selon le principe du "besoin de savoir", jugeant la complexité technique inappropriée en raison de la diversité des compétences des travailleuses en matière d'alphabétisation et de littératie numérique et de leurs capacités techniques. Du point de vue des travailleuses, leur portefeuille (…) était une sorte de compte bancaire. »[1837] Et surtout, comme le fait remarquer le juriste Ioannis Stathakis, les bénéficiaires ne peuvent même pas consulter l'historique de leurs transactions : « Tout d'abord, à l'heure où ce mémoire est rédigé, les réfugiés n'ont pas d'accès individuel à leurs portefeuilles numériques. Le système les suit virtuellement, mais il n'existe pas de moyen efficace pour une personne de voir son solde, de consulter l'historique de ses transactions ou de suivre la procédure elle-même. »[1838] La seule information visible pour les bénéficiaires serait un reçu délivré après un achat par les caissiers. Un ticket de caisse papier contient la somme retirée et le montant restant sur le compte. Les bénéficiaires ne peuvent avoir accès à la liste complète des transactions[1839]. Ajoutons que : « comme la transaction doit être autorisée par le bénéficiaire au moyen de la biométrie, le caissier ne peut

[1835]«Beneficiaries should act as custodians for the private keys of beneficiaries, which are linked to the users' biometric data. While that is a practical solution, as noted by UNHCR with respect to the Building Blocks system, it negates one of the essential properties of blockchain architecture in terms of decentralization and user autonomy »
DUMITRIU Petru, "Blockchain applications in the United Nations system: towards a state of readiness", 2020, https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2020_7_english.pdf

[1836] "Among humanitarian uses, most of the improvements brought by blockchain technology in these cases involve back-end processes, rather than impacting on end-user experiences (*ibid.*). This means that the technology does not interact directly with the affected populations supported by humanitarian action but rather is used for the processes that take place on the backside to generate cost savings, increased transparency, and traceability of information flows." THYLIN, T.,DUARTE, M. F. N., "Leveraging blockchain technology in humanitarian settings – opportunities and risks for women and girls", *Gender & Development*, *27*(2),2019, p. 317–336. https://doi.org/10.1080/13552074.2019.1627778

[1837]"But no one explained the blockchain to these women workers: as a concept, GEN staff treated blockchain on a "need to know basis," deeming the technical complexity inappropriate because of workers' mixed literacy and numeracy skills and technical capacities. From the workers' perspective, their wallet (maHfadda) was a kind of bank account."CHEESMAN, Margie, "Blockchain for refugees", Medium, 08/06/2022 https://medium.com/datasociety-points/blockchain-for-refugees-a46b41594eee

[1838]"First of all, as of the time this thesis is being written, refugees do not have individual access to their digital-wallets. The system keeps virtual track of them, but there is no effective way for a person to see their balance, view the history of their transactions or monitor the procedure itself." STATHAKIS, Ioannis, "Critical perspectives on blockchain for humanitarian aid, How does the technology impact procedural fairness and beneficiary data protection?", Master thesis, Law&technology Tilburg University, 2019 https://arno.uvt.nl/show.cgi?fid=149162

[1839] JUSKALIAN, Russ, "Inside the Jordan Refugee camp that runs on blockchain", *MIT technology review*,11/04/2018, https://www.technologyreview.com/2018/04/12/143410/inside-the-jordan-refugee-camp-that-runs-on-blockchain/
TALHOUK, Reem, GARBETT, Andy, MONTAGUE, Kyle, "Tech can empower refugee communities - if they're allowed to design how it works", *The conversation*, 30/01/2019https://theconversation.com/tech-can-empower-refugee-communities-if-theyre-allowed-to-design-how-it-works-119132

pas demander au hasard le solde du bénéficiaire, à moins que ce dernier n'ait déclenché une transaction. »[1840]


Reçu d'EyePay' dans un supermarché au camp de réfugiés de Zaatari. WFP/Mohammad Batah[1841].

Ces différentes remarques sont d'autant plus problématiques qu'une antenne onusienne destinée aux enjeux de genre, UNWOMEN, a rejoint Building Block afin de lancer un programme destiné à l'autonomisation financière de femmes syriennes[1842]. Et la chercheuse Margie Cheesman a bien montré que les femmes y prenant part n'ont accès qu'à très peu de aux informations relatives à leurs achats[1843].

Et pourtant on peut lire dans la politique de transfert monétaire du WFP que « le WPF vise à donner à chaque personne la possibilité de choisir quand et comment dépenser son argent et où elle souhaite le recevoir. Cela nécessite de lever autant que possible les restrictions appliquées aux sommes reçues, et de s'assurer que les bénéficiaires disposent des informations dont ils ont besoin pour faire les choix les plus adaptés à leur situation. »[1844] Le texte mentionne également le fait que les individus sont au centre des préoccupations de l'organisation : « les personnes qui reçoivent de l'argent doivent se sentir respectées et soutenues dans toutes leurs relations avec le WFP et ses partenaires. Pour respecter ce principe, le WFP sera à l'écoute de leurs besoins, de leurs expériences et de leurs aspirations, et les placera au centre de ses propres opérations de transferts monétaires. »[1845]

Une partie des membres porteurs du projet regrettent les limitations de Building Block. Du moins, le fondateur de Building Block, Houman Haddad souhaite accorder plus d'autonomie

[1840]« The balance is printed at the bottom of beneficiary transaction receipts; and this is a feature that is much valued by the beneficiaries. However, because the transaction must be biometrically authorized by the beneficiary, the cashier cannot randomly query beneficiary balances, unless the beneficiary has triggered a transaction. » ZWITTER, Andrej, GSTREIN, Oskar Josef, "identity and privacy governance", *Frontiers Research Topics*, 2021

[1841] FAULKNER Charlie, "How blockchain technology has changed the game for Syrian refugees in Jordan", *The National,* 03/11/2019https://www.thenationalnews.com/arts-culture/how-blockchain-technology-has-changed-the-game-for-syrian-refugees-in-jordan-1.932432

[1842] UN Women-WFP blockchain pilot project for cash transfers in refugee camps, Jordan Case study, UNWOMEN, 2021 https://jordan.unwomen.org/sites/default/files/Field%20Office%20Jordan/Images/publications/2021/Blockchain%20pilot%20project/UN%20WOMEN-WFP%20BLOCKCHAIN%20PILOT%20PROJECT%20FOR%20CASH%20TRANSFERS%20IN%20REFUGEE%20CAMPS%20JORDAN%20CASE%20STUDY.pdf

[1843] CHEESMAN, Margie, "Blockchain for refugees", *Medium*, 08/06/2022, https://medium.com/datasociety-points/blockchain-for-refugees-a46b41594eee

[1844] WFP, « Politique en matière de transferts monétaires », 12/06/2023 https://executiveboard.wfp.org/fr/document_download/WFP-0000149841

[1845] WFP, ibid.

aux bénéficiaires, comme on peut le lire dans un article de presse : « Haddad envisage cependant une évolution de Building Blocks vers plus d'autonomie pour les réfugiés, en prenant la forme d'un SSI. « M. Haddad imagine un avenir où les réfugiés contrôleront leurs propres clefs cryptographiques pour accéder à leurs fonds (ou "entitlements", dans le jargon des travailleurs humanitaires). Cet élément pourrait être crucial pour rendre l'aide plus facile et plus largement disponible, car les clefs déverrouilleraient des données qui sont actuellement bloquées dans différentes agences d'aide, y compris les dossiers médicaux de l'Organisation mondiale de la santé, les certificats d'études de l'UNICEF et les données nutritionnelles du WFP. "Ce profil commence à s'enrichir pour devenir une identité contrôlée par le bénéficiaire, ce qui ne s'est jamais produit auparavant", explique M. Haddad. »[1846] Il serait intéressant d'en savoir plus sur les différents freins expliquant en interne le fait que le projet ne serait pas allé dans la direction souhaitée par Houman Hadad. Redonner aux utilisateurs une forme de contrôle de leurs données impliquerait surement une reconfiguration du système d'information de l'organisation [1847], ce qui ne va pas sans coût. Or souvenons-nous qu'un des objectifs de Building Blocks est d'acquérir des gains monétaires et d'efficacité. En effet, réduire la dépendance des acteurs bancaire permettrait de réduire les frais de gestions de comptes (taxes, banques, « lourdeur » démarche » administrative). Et comme le déclare l'organisation humanitaire : « Plutôt que de rembourser les commerçants par l'intermédiaire de prestataires de services financiers locaux, le WFP a eu recours à des virements internationaux par le biais d'un système de transfert électronique de fonds à partir de comptes bancaires mondiaux pour rémunérer directement les commerçants. Datarella, une filiale du fournisseur de technologie du secteur privé Baltic Data Science, estime à 3,5 millions de dollars par an les économies réalisées par le WFP. » [1848] Toutefois, selon certaines critiques, le même degré d'efficience aurait pu être atteint sans recourir à des blockchains. On peut lire en effet dans un rapport de l'ONU que : « les économies réalisées en désintermédiant les prestataires de services financiers locaux via la technologie blockchain auraient pu être réalisées grâce à l'utilisation d'une structure de données partiellement

[1846] Haddad envisions a future where refugees control their own cryptographic keys to access their funds (or "entitlements," in aid worker jargon). This element may be crucial to making aid more easily and widely available because the keys would unlock data that's currently stuck in different aid agencies, including medical records from the World Health Organisation, educational certificates at UNICEF, and nutritional data from WFP. "This profile starts to become enriched to become an identity that's controlled by the beneficiary, which has never happened before," Haddad says"
WONG, Joon Ian, "The UN is using ethereum's technology to fund food for thousands of refugees", *Quartz*, 03/11/2017
https://qz.com/1118743/world-food-programmes-ethereum-based-blockchain-for-syrian-refugees-in-jordan

[1847]«la refonte des pratiques et des protocoles existants en matière de gouvernance des données est essentielle à ce changement de culture. Plusieurs personnes interrogées ont fait remarquer que le passage des systèmes traditionnels de gestion des données aux solutions d'identité numérique est souvent plus une question de modification des pratiques de gouvernance des données que de changement technologique. »,"Critical to this culture change is the revision of existing data governance practices and protocols. Several interviewees commented that the transition from traditional data management systems to digital identity solutions is often more an issue of altering data governance practices than effecting technological change." IFRC, ibid.
JUSKALIAN, Russ, "Inside the Jordan Refugee camp that runs on blockchain", *MIT technology review*, 11/04/2018, https://www.technologyreview.com/2018/04/12/143410/inside-the-jordan-refugee-camp-that-runs-on-blockchain/

[1848] Rather than reimburse merchants through local financial service providers, WFP used international wire transfer via an electronic funds transfer system from global bank accounts to remunerate merchants directly. This reportedly reduced transaction costs by over 98%.62 Datarella, an affiliate of private sector technology provider Baltic Data Science, pegs saving costs for WFP at $3.5 million annually.ZAMBRANO,Raul,YOUNG,Andrew, VERHULST, Stephan, "Connecting Refugees to Aid through Blockchain-Enabled ID Management: World Food Programme's Building Blocks",October 2018, GovLabhttps://blockchan.ge/blockchange-resource-provision.pdf
GSMA, "Humanitarian cash and voucher assistance in Jordan : a gateway to mobile financial services", January 2020https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/01/Jordan_Mobile_Money_CVA_Case_Study_Web_Spreads.pdf
GIZ, "Financial inclusion of refugees in Jordan, knowledge note", November 2022, https://www.giz.de/en/downloads/giz2022-en-financial-inclusion-refugees-jordan.pdf

persistante. Une telle base de données peut stocker les données de transaction en temps réel sous la forme d'une liste annexe, ce qui permet au WFP de rembourser les commerçants directement, comme l'a fait la blockchain. De même, la sécurité accrue acquise par le déploiement de la technologie blockchain par le WFP aurait pu être obtenue grâce à une base de données dotée d'une couche de cryptage. »[1849]

### *§ 2 — Iryo[1850]*

Notre deuxième cas d'étude, Iryo se présente comme un dossier médical fondé — en partie — sur de la blockchain. Il a été développé en Slovénie en 2017. Iryo affiche trois objectifs : l'interopérabilité informationnelle, la sécurité des données et l'autodétermination informationnelle[1851]. Mais précisons d'emblée que la blockchain ne permet pas, d'après les fondateurs du projet, de remplir leurs deux premières finalités. L'interopérabilité ne peut être atteinte que par une standardisation des données de santé. Le caractère ouvert des blockchains irait pour l'équipe d'Iryo à l'encontre de la sécurité technique des informations, d'où la nécessité de concevoir une architecture contrebalançant cette limitation et offrant un minimum de confidentialité aux utilisateurs.
Iryo fonctionne donc de la façon suivante : les données personnelles et de santé sont conservées en dehors de la blockchain, sur du cloud et sur les smartphones des utilisateurs. Le groupe préfère en effet utiliser une stratégie de stockage multiple et éviter la centralisation des données : « Iryo considère les données médicales qu'elle détient comme un actif toxique, car nous pensons que le fait de détenir trop de données en un seul endroit présente un risque de responsabilité trop important. »[1852] Garantir l'autodétermination informationnelle aurait signifié pour conserver ses données sur le terminal de l'utilisateur, en l'occurrence des smartphones. Mais leur capacité de stockage n'est pas suffisante. Par conséquent, ils servent à garder une partie seulement des données médicales, et non pas l'intégralité du dossier de santé. Donc, une sauvegarde des données est gardée sur du Cloud, cette technologie étant estimé comme la solution sécurisée pour les ingénieurs à l'origine d'Iryo. Cette modalité de stockage comprend aussi une autre limite : l'utilisateur peut perdre son téléphone. Par conséquent, l'équipe d'Iryo a choisi d'adopter une technique de fragmentation des clefs de chiffrement. L'objectif est de préserver son intégrité en cas de perte de clef et de garantir l'accès d'urgence au smartphone si le patient est inconscient. Une partie de la clef est donc confiée à un tiers de confiance, ce qui permet de la reconstituer si besoin. Quant à la blockchain en tant que telle, elle est publique, et ne contient donc pas de données personnelles. La blockchain sert à gérer l'accès aux données. Aucune donnée personnelle n'y

[1849] « Although the ledger-based identification systems improved the cash transfer program, similar functionality could have been achieved with enterprise technologies. Indeed, as initial WFP program manager Houman Haddad has noted, "what we are doing now could be done on a traditional IT system." "The cost savings achieved through disintermediating local financial services providers via blockchain technology could have been achieved through the use of a partially persistent data structure. Such a database can store transaction data in real time as an append-only list, allowing WFP to reimburse merchants directly just as the blockchain did. Similarly, the enhanced security yielded by WFP's deployment of blockchain technology could have been accomplished through a database with an encryption layer. »
[1850] Iryo signifie médecine en japonais.
[1851] ZAJC, Tjasa, "It should be in everyone's interest to give patients their medical records", *Medium*, 05/07/2018https://medium.com/iryo-network/it-should-be-in-everyones-interest-to-give-patients-their-medical-records-99e079ea67b8
[1852] « Iryo Percieves the medical data it holds as a toxic asset because we believe that holding too much data in one place presents too large a liability risk. » https://iryo.gitbook.io/whitepaper/zero-knowledge-storage

est stockée sur la blockchain, même chiffrée. Les méthodologies cryptographiques ne seraient pas suffisamment protectrices, puisque potentiellement obsolètes. Et comme le déclare un des concepteurs d'Iryo : « les blockchains sont éternelles, alors que les techniques de chiffrement ne le sont pas. » [1853] Elles permettent de conserver les contrats intelligents gérant l'accès aux données des patients et l'historique des demandes d'accès aux dossiers médicaux.

À noter, les ingénieurs impliqués dans le développement d'Iryo critiquent fortement les blockchains privées. Ces dernières ne conserveraient pas selon eux les avantages des blockchains du fait de leurs gouvernances centralisées : « C'est pourquoi l'Iryo Network ne stocke pas de données sur la blockchain, mais l'utilise pour garantir la transparence des transactions. Certains projets prétendent utiliser la blockchain en recourant à des "chaines privées", qui ne sont généralement que des bases de données rebaptisées. »[1854]

Le projet vise à favoriser l'échange de données entre chercheurs et patients via un système d'incitation financière. Il s'agit d'une conception proche du paradigme patrimonial de la protection des données[1855]. Le protocole de partage fonctionne comme suit. Tous les patients, quel que soit leur profil, reçoivent une notification pour des caractéristiques médicales particulières (femme de 30-35 ans ayant du diabète par exemple). Si le patient correspond aux critères, une notification lui est envoyée. Cette dernière détaille l'ensemble des caractéristiques du requérant : le nom de l'institution, la justification de la demande, la finalité de la recherche, le nombre de token associé à l'acceptation de la requête. En effet, le réseau Iryo repose sur un système de « token ». Le projet propose de « récompenser » le partage de données à des études cliniques via un système de token réutilisables pour payer des services médicaux avec les tokens d'Iryo. Les données du patient sont ensuite partagées avec la clinique, sous une forme anonymisée.

De surcroit, les tokens servent aussi à sécuriser la fonctionnalité « bris de glace » d'Iryo. Par exemple, si un médecin souhaite de toute urgence avoir accès au dossier patient, il doit déposer sur son compte des token. Si par la suite le patient valide l'accès comme légitime, les token sont rendus à l'hôpital. Dans le cas contraire, le patient les garde pour lui. Pour les concepteurs d'Iryo, cela est un gage de pouvoir pour le patient : c'est à l'hôpital de prouver qu'il est légitime. Cette facette du projet va de pair avec l'idée d'une patrimonialisation des données personnelles reposant sur la possibilité de les monétiser. Cela s'oppose à l'idéal des données de santé comme bien commun. D'ailleurs, Iryo soutient la privatisation des soins. En entretien, un des membres d'Iryo mène un discours très critique sur le secteur hospitalier public, et le dossier médical est destiné à des cliniques privées[1856]. Ainsi, le dossier médical est

[1853] « Blockchain is "eternal" while encryption is not », RICKS, Brig, "Iryo delivering better health outcomes", *Medium,* 02/04/2018https://medium.com/iryo-network/iryo-delivering-better-health-outcomes-d5aeb55cab63

[1854] « This is why the Iryo Network doesn't store data on blockchain but uses blockchain to ensure the trans-parency of transactions.Some projects pretend to be using blockchain by using 'private chains' which are usually just re-branded databases. Private chains use some elements of blockchain technology but miss key elements thereof like the oversight offered over the validity of the stored data.Public blockchains are mainly useful for two things; value transfer (including initial creation and distribution) and trustless timestamping of the messages. » https://cryptocurrencyaus.com/iryo-network-ico/

[1855] La conception patrimoniale de la protection des données consiste à penser que les données doivent être la propriété des personnes concernées, qui sont alors libres d'en faire le commerce.

[1856] Entretien n°16, dossier médical, 30/01/2020.

aussi soutenu par une compagnie d'assurance slovène, Adriatic Slovenica, dont l'objectif est de favoriser le développement du système médical slovène privé.

Toujours est-il que comme on l'a indiqué, Iryo comprend également une facette humanitaire. Un conseiller d'Iryo — Brian de Francesca — aurait mis en contact la startup avec « Tying Vines », une ONG américaine catholique[1857], dont il connait les fondateurs. En janvier 2018, un membre d'IRYO s'est rendu dans un camp de réfugiés au Liban. Il a fait le constat d'un fort taux d'utilisation de smartphone, du moins selon ses observations personnelles. Ce constat justifie alors le déploiement du projet en mai 2018, sans avoir préparé une étude de contexte plus approfondie. La phase de test s'est déroulée sur deux ordinateurs, où le dossier médical a été testé, non pas auprès directement des exilés, mais auprès de médecins de l'ONG « Tying Vines »[1858].

Tying Vines cherchait alors à améliorer la continuité de la prise en charge médicale des réfugiés. Un des fondateurs d'Iryo a ainsi fait la remarque en entretien que les réfugiés restent parfois de longues années dans un camp, d'où l'importance de conserver un historique médical. D'autant qu'il existe une forte rotation des médecins des ONG, compliquant la continuité de soin. Le fait que le patient détienne lui-même ses informations de santé permettrait aux médecins d'avoir une vue d'ensemble du parcours du patient.

Voici comment le projet est présenté dans un rapport de l'UNFAP (organisme de l'ONU chargé d'enjeux de santé sexuelle et reproductive) : « Iryo permet un enregistrement précis des antécédents médicaux grâce à sa fonction de stockage décentralisé des données. Cela permet de conserver une copie sur un serveur local, une deuxième sur le téléphone portable du patient et une troisième dans le nuage d'Iryo. Ainsi, lorsqu'un patient arrive dans un nouveau camp de réfugiés équipé du système Iryo, les médecins et/ou le personnel soignant peuvent accéder aux dossiers des nouveaux arrivants. Auparavant, les travailleurs médicaux dans les camps utilisaient des feuilles de calcul Excel pour enregistrer leurs notes sur les patients, un processus encore compliqué par l'incohérence de la tenue des dossiers en raison de la forte rotation du personnel médical. »[1859]

À noter, la présentation ne mentionne pas la possibilité pour les réfugiés de contrôler leurs données de santé. En entretien, notre enquêté a mis l'accent sur l'objectif final est de permettre aux réfugiés de conserver leurs données sur eux tout le long de leur exil. Cependant, notre enquêté note que « *Le problème est que l'ensemble du concept est nouveau, même dans le monde développé, et je pense donc qu'il est encore assez difficile pour l'instant*

---

[1857] https://tyingvines.org/about/

[1858] TJASA, ZAJC, "Announcing the first deployment of the Iryo system: improving healthcare for refugees", *Medium*, 17/01/2018, https://medium.com/iryo-network/announcing-the-first-deployment-of-the-iryo-system-improving-healthcare-for-refugees-bee8c441e7e6 Iryo, "Iryo's electronic health data management platform successfully deployed", Medium, 21/05/2018 https://medium.com/iryo-network/iryos-electronic-health-data-management-platform-successfully-deployed-d657bee8d2bf

[1859] « Iryo enables accurate medical history recording thanks to its decentralized data storage feature. This allows one copy to be kept on a local server, a second on the patient's mobile phone and a third in Iryo cloud. Thus, when a patient arrives at a new refugee camp that is equipped with the Iryo system, doctors and/or health care workers will be able to access newcomer records. Previously, medical workers in camps used Excel spreadsheets to record their patient notes, a process further complicated by inconsistent record keeping arising from the high turnover of medical workforce personnel. » MOUAWAFAQ, Safwane, EL BOURI, Hicham, « Innovative solutions to address needs of people on the move for maternal health, sexual and reproductive health, and gender-based violence services in the Arab States Region », UNFPA, 2020
https://iraq.unfpa.org/sites/default/files/pub-pdf/people_on_the_move_final_for_web_14-9-2020.pdf

*de faire quelque chose comme ça, parce que les réfugiés, la population dans son ensemble, doivent saisir le concept et parfois ils ne comprennent pas à quel point les données peuvent être précieuses.* » [1860]

Les réfugiés n'ont donc pas eu accàs à une version de l'application complète. En outre, la version jordanienne d'Iryo n'assure pas le même degré de sécurité. L'enquêté justifie ce point fait en raison d'un cadre législatif contraignant : « *le stockage de données à "zero proof" est encore manquant, principalement parce que la législation sur la confidentialité des données est différente. Les données sont chiffrées évidemment, mais pas avec la technique "zero proof" sur laquelle nous travaillons par ailleurs.* » [1861] Cela dit, il existerait plutôt un vide législatif sur le chiffrement, selon les rapports de Privacy international [1862].

Malgré le fait que cette version ne comprenne pas toutes les fonctionnalités du dossier médical, ce dernier a permis pour Iryo de tester l'application dans des conditions moins favorables en matière de connectivité : « Le projet sur les réfugiés est notre projet pilote qui vise à prouver le concept et à concevoir un modèle pour l'étendre à d'autres endroits présentant des défis similaires en matière de connectivité et d'infrastructure. En menant un projet pilote avec des réfugiés, nous pouvons créer un produit minimum viable et disposer d'une solide preuve de concept. C'est une bonne chose pour les réfugiés, qui ont désespérément besoin de notre aide, mais c'est aussi une bonne chose pour nous de pouvoir démontrer notre approche dans un contexte réel. » [1863]

Iryo avait toutefois vocation à être déployé dans d'autres camps de réfugiés dans les pays suivants : en Syrie, Jordanie, Iraq, en Égypte et à Djibouti. Mais en raison d'un manque de ressources, la version commerciale a été privilégiée, et sa facette humanitaire abandonnée[1864].

---

[1860]« the problem though is that the all concept is new even in the develop world , so I think it is quite strecht still at the moment for something like that, because the refugee, the all population they have to grasp the concept and sometimes they dont get how valuable the data can be. Entretien n°16, Dossier medical, 30/01/2020

[1861] "Zero knowledge data storage is still missing, primarly because obviously data privacy legislation is different. There is encryption but not the true zero knowledge that we are working on" Health unchained, ep.8 : Securing health data- Vasja Bocko, Health podcast network, 09/07/2018 https://healthpodcastnetwork.com/episodes/health-unchained/ep-8-securing-health-data-vasja-bocko-ceo-iryo/
DISNEY, Helen, « Healthcare IT needs a dose of medicine, interview with Vasja Bocko, Iryo », *Unblocked*, 07/02/2018 https://un-blocked.co.uk/2018/02/07/healthcare-it-interview-vasja-bocko-iryo/

[1862]State of Privacy, Jordan, 26/01/2019 https://privacyinternational.org/state-privacy/1004/state-privacy-jordan

[1863] "The refugee project is our pilot project to prove the concept and eventually design a model for scaling to other places with similar challenges regarding connectivity and infrastructure. By running a pilot with refugees, we can create a Minimum Viable Product and have a strong proof of concept. It is good for the refugees, who desperately need our help, but it is also good for us to be able to demonstrate our approach in a real-world setting." DISNEY, Helen, « Healthcare IT needs a dose of medicine, interview with Vasja Bocko, Iryo », *Unblocked*, 07/02/2018 https://un-blocked.co.uk/2018/02/07/healthcare-it-interview-vasja-bocko-iryo/

[1864] Entretien n°16, Dossier medical, 30/01/2020

### *§ 3 - IFRC, « Dignitfied identities in cash assistance »*

Le projet « Dignified identities in cash assistance » (DIGID) remonte à fin 2018. Il est porté par un consortium d'organisations norvégiennes, le Norwegian Red Cross, NRC, Save the Children Norway, Norwegian Church, et une organisation internationale, l'IFRC. Dans un premier temps, la préoccupation des ONG ne concernait pas l'autodétermination informationnelle des bénéficiaires. Le consortium cherchait une solution pour pallier leur exclusion de service humanitaire du fait d'un manque de documents officiels d'identité. C'est sur ce problème que butaient l'IFRC et la Croix rouge kenyane dans le projet « Blockchain Open Loop cash transfer « . Le manque de documents compliquait en effet le partenariat avec des entités de transferts de fonds comme M-PESA, en raison de mesures de KYC (cf. chapitre 4).

L'idée de chercher un moyen de favoriser l'autonomie des bénéficiaires, notamment grâce aux blockchains, serait venue par la suite. Fin 2019 correspondrait au « haut de la vague » de l'engouement pour les blockchains dans l'humanitaire. Le consortium DIGID y a donc pris part, mais s'en distancie. Leurs membres sont restés d'emblée prudents sur la possibilité d'atteindre cet objectif pour un public qu'il qualifie de « vulnérable ». Ainsi le contrôle des données n'est qu'une des facettes du projet. Garantir la dignité des bénéficiaires passe pour le consortium d'ONG par d'autres biais. Citons un passage d'un rapport de DIGID à ce sujet : «Parmi les exemples révélant une forme de dignité, on peut citer le fait que des personnes qui n'avaient pas de carte d'identité officielle ont reçu de l'argent directement au lieu de chercher quelqu'un d'autre ayant une carte d'identité officielle pour en réclamer en leur nom ; les personnes ont pu se présenter et communiquer leurs données pour demander les services dont elles avaient besoin et faire vérifier leur éligibilité ou être orientées plus rapidement vers d'autres agences susceptibles d'offrir des services spécialisés ; et les personnes ont pu consentir à partager leurs données avec d'autres organisations et même révoquer ou supprimer leurs données si elles ne voyaient plus l'utilité de leur carte d'identité numérique. » [1865]

Concrètement, l'objet de DIGID est la création d'un portefeuille d'identités numériques pouvant être gérées, plus ou moins directement, par son possesseur. Il contiendrait des accréditations, soit des informations relatives à différents attributs d'une personne : son nom, son âge, le fait que la personne appartienne à une certaine communauté ou non. L'utilisateur de DIGID pourrait consentir à montrer ou non certaines accréditations à des parties tierces, en l'occurrence des ONG. Il est destiné donc à être utilisé par les humanitaires pour identifier les bénéficiaires au cours de l'allocation d'un service : « les références fournies par les institutions (par exemple, la Croix-Rouge du Kenya par le biais de la vérification communautaire) pourraient être conservées et présentées lorsqu'une vérification est

[1865] "some examples where dignity was observed include seeing people who did not have official IDs receive cash directly instead of resorting to finding someone else with an official ID to claim on their behalf; people were able to present themselves and their data to ask for services that they need and be verified for eligibility or referred more quickly to other agencies who could offer specialised services; and people could consent to share their data with other organisations and even revoke or delete their data if they did not see a need for their digital IDs anymore." IFRC, Kenya Red Cross, Uganda Red Cross, "Dignified identities in humanitarian action : journey and reflection", February 2023https://interoperability.ifrc.org/wp-content/uploads/2023/11/DIGID-Summary-Report-Final.pdf

nécessaire pour accéder à un service ou à une assistance. »[1866] En l'occurrence, DIGID a été conçu pour être testé pour des programmes de transferts monétaires, mais aussi sanitaires et dans des programmes humanitaires destinés à des exilés.

Le projet a donné lieu à différents ateliers de travail en octobre 2020. Puis un prototype a été testé lors d'opérations d'enregistrement de bénéficiaires en avril et mai 2021 au Kenya. L'opération a eu lieu plus précisément dans deux zones : dans un camp informel urbain à Mathare, et dans une zone rurale de Kalokol à Turkana. Une autre expérimentation du projet a été menée en novembre 2021, de nouveau à Mathare. En 2022, un deuxième volet de DIGID a été testé, ce dernier consistait en un portefeuille de gestion de données médicales, testé auprès de migrants au Kenya et en Uganda.

Cette phase de test a compris l'ouverture de portefeuilles numériques et d'« accréditation » d'identité pour chaque bénéficiaire. Le mode de création d'un « portefeuille » dépend du dispositif téléphonique dont dispose un bénéficiaire. Les possesseurs de smartphone reçoivent simplement un SMS avec un lien les dirigeant vers une interface gérée par l'entreprise Gravity, fournisseuse de solution numérique d'identité. Grâce à cette dernière, le bénéficiaire accède à ses données et gère ses demandes d'accès avec un QR Code. Pour les possesseurs de téléphones basiques, un compte est créé sur l'interface par l'ONG. Le bénéficiaire peut ensuite choisir son code PIN en utilisant son propre téléphone qui sert à accéder au portefeuille. L'interface prend la forme d'un menu déroulant et à des envois de SMS lui permettant de gérer les demandes d'accès. Dans le cas où le bénéficiaire ne possède pas de téléphone, le portefeuille est d'abord créé par l'ONG. Puis un QR code imprimé va permettre au bénéficiaire d'accéder à ce dernier, sur un dispositif d'une ONG (smartphone ou ordinateur). En l'absence de téléphone, les demandes de données peuvent simplement être gérées en face-à-face, comme lors d'un recueil classique de consentement. Le bénéficiaire montre son QR code à un responsable, qui recourt à l'application pour scanner le QRcode et extraire les données identifiantes. La possibilité de gérer ses propres données enregistrées sur l'interface est grandement limitée dans ce cas[1867]. Il est précisé qu'un niveau de sécurité

[1866] "where credentials provided by institutions (e.g. Kenya Red Cross through their community verification) could be kept and presented when there is a need for verification to access a service or assistance. » "Dignified identity in cash assistance : lesson learnt from Kenya", 2022 https://cash-hub.org/wp-content/uploads/sites/3/2022/02/DIGID-Lessons-Learnt-from-Kenya-Jan-2022.pdf

[1867] « Les codes QR contenaient certaines informations d'identification de base et étaient cryptés et sécurisés par des codes PIN choisis par les utilisateurs. Les codes QR ne permettaient pas aux utilisateurs de gérer directement leurs données, mais ils constituaient un moyen sûr et sécurisé de s'authentifier en cas de besoin. Les destinataires des codes QR devaient s'en remettre à l'organisation qui leur avait délivré leurs identifiants, en l'occurrence KRCS, s'ils souhaitaient mettre à jour ou confirmer les informations qu'ils détenaient. Dans ce scénario, la KRCS joue le rôle de gardienne des données numériques de l'individu. Les systèmes de gestion des bénéficiaires existants gèrent actuellement les données d'une manière similaire, sauf que le code QR fournit une couche d'authentification qui n'est pas aussi facile à utiliser avec les systèmes de gestion des bénéficiaires traditionnels. », "the QR codes contained certain basic credentials and were encrypted and secured with PINs chosen by the users. QR codes did not confer users with the ability to directly manage their data, but they did provide a safe and secure way to authenticate themselves when needed. QR code recipients had to rely on the organization that issued their credentials, in this case KRCS, if they would like to update or confirm the information being held. In this scenario, KRCS acts as a guardian of the individual's digital credentials. Existing beneficiary management systems currently manage data in a similar way, except that the QR code provides a layer of authentication that is not as easy with traditional beneficiary management system." IFRC, Kenya Red Cross, ICHA, "Dignified identities in cash assistance : lessons learnt from Kenya", January 2022https://cash-hub.org/wp-content/uploads/sites/3/2022/02/DIGID-Lessons-Learnt-from-Kenya-Jan-2022.pdf

supplémentaire peut être ajouté : un code PIN ou des données biométriques permettent de s'assurer que le QR code appartient effectivement au bénéficiaire[1868].

Sachant que les données des bénéficiaires ne sont pas conservées sur l'appareil des bénéficiaires ( contrairement à Iryo), mais sur un cloud, privé, hébergé au Kenya, ce qui est d'ailleurs en accord avec la législation de protection des données locale. Précisons qu'il s'agit de différentes informations nécessaires aux opérations de cash, comme des informations géographiques (pays, région, village) ; personnelles, nom du « leader communautaire » local ; type de carte d'identité et numéro de carte d'identité ; type de téléphone ; le numéro de téléphone ; statut marital ; âge ; nom du chef de famille ; nombre de membres du foyer ; éléments concernant la vulnérabilité ; (handicap dans le foyer, par genre, personnes enceintes, en cours d'allaitement ; maladies chroniques)[1869]. Ce sont ces données que le bénéficiaire choisit de communiquer — ou non — aux ONG. Enfin, DIGID n'utilise pas de mécanisme de type « preuve à divulgation nulle » » : « Les technologies "zero knowledge proof" permettent aux utilisateurs de partager des preuves avec les parties qui se fient à elles sans avoir à démontrer l'intégralité de l'information. Ceci est particulièrement important dans le contexte humanitaire étant donné la nature sensible des données concernant les migrants. La plateforme DIGID ne prend actuellement pas en charge de technologie "zero knowledge proof", mais cela pourrait être développé si cela s'avère nécessaire dans le contexte de la migration. »[1870]

La blockchain utilisée est une blockchain publique, gérée par l'entreprise Tezos, mais elle ne contient pas de données directement identifiantes. En effet, la blockchain stocke des clefs publiques de chiffrement[1871]. Une note de bas de page précise toutefois que selon l'AIPD mené par la Croix rouge kenyane, ces clefs sont considérées comme des données personnelles[1872], signifiant par là qu'une réidentification indirecte est toujours possible. Ajoutons que la possibilité de pouvoir supprimer ses données est incertaine. Sur ce point, le juriste et chercheur Yves Poullet indique que « comme a pu l'indiquer l'Open Data institute (ODI) britannique, pour supprimer une donnée, il faudrait que plus de la moitié des nœuds du réseau travaillent ensemble pour reconstruire la chaine de blocs depuis le moment où la donnée a été ajoutée (…) Cela signifie que toutes les données postérieurement enregistrées

---

[1868] IFRC, Kenya Red Cross, Gravity, "Gravity-Tykn interoperability proof of concept", June 2021,https://static1.squarespace.com/static/5b75620445776e4b290c0d96/t/619113c163634531ee6365e9/1636897731161/DIGID+Interoperability+Tests.pdf
Dignified ID Q&A complied list from information sessions https://static1.squarespace.com/static/5b75620445776e4b290c0d96/t/5c98aada8165f590a8e89158/1553509083480/INF_+20190300+DIGID+INF+-+Questions+and+Answers+combined+%28from+sessions+1-5%29.pdf
Kenya Digital ID workshop summary, May 2019 https://drive.google.com/file/d/1c_4TmpA6cIBlYPgCuvge8_KI3adjcaDv/view
[1869] IFRC, Kenya Red Cross, ICHA, "Dignified identities in cash assistance : lessons learnt from Kenya", January 2022https://cash-hub.org/wp-content/uploads/sites/3/2022/02/DIGID-Lessons-Learnt-from-Kenya-Jan-2022.pdf
[1870]"Zero knowledge proofs allow users to share proofs with relying parties without the need to actually demonstrate the entirety of the information. This is particularly important for the humanitarian context given the sensitive nature of data regarding migrants. The DIGID Platform currently does not support zero-knowledge proofs, but this may be developed if required as part of the migration context "
IFRC, Kenyan Red Cross, ICHA, ibid
DUMAS Jean-Guillaume, LAFOURCADE Pascal, TICHIT Ariane *et al.*, « 48. Qu'est-ce qu'une preuve à divulgation nulle de connaissance ? », dans : , *Les blockchains en 50 questions.* Paris, Dunod, « Hors collection », 2019, p. 253-256. URL : https://www.cairn-sciences.info/--9782100800896-page-253.htm
[1871] Les clefs publiques d'authentification
[1872]IFRC, Kenya Red Cross, ICHA, "Dignified identities in cash assistance : lessons learnt from Kenya", January 2022https://cash-hub.org/wp-content/uploads/sites/3/2022/02/DIGID-Lessons-Learnt-from-Kenya-Jan-2022.pdf

sur la blockchain seraient supprimées. »[1873] Et certes le système permet aux bénéficiaires d'exercer leur droit à l'oubli en leur demandant la suppression de leur portefeuille d'identité mobile, via l'application mobile [1874] . Mais les informations inscrites sur la blockchain (métadonnées, traces d'accès, etc.) sont inaltérables et ne peuvent donc pas être effacées. Et si l'on considère que les clefs publiques sont des données personnelles (ce qui est défendu par certains juristes), le RGPD s'y applique et la question du retrait du consentement se pose. Enfin, il est offert aux bénéficiaires d'avoir accès à ses données, mais cela se limite aux données personnelles, liées directement au programme, et non pas toute une série d'informations techniques, métadonnées, etc. Et surtout, quelle connaissance aurait les bénéficiaires de l'architecture complète du programme ? Les rapports n'indiquent pas s'il a été expliqué aux bénéficiaires ce qu'est une blockchain.

Et plus généralement, l'expérimentation du dispositif a révélé des limites en matière d'autodétermination informationnelle. Tout d'abord, les ONG ont fait le constat d'un manque de littératie numérique chez une bonne partie des bénéficiaires, avec une nette différenciation entre milieu urbain et milieu rural. Des ateliers d'échanges avec les bénéficiaires et des rapports publiés par le consortium conjointement au développement de DIGID donnent quelques éléments de précision sur ce sujet.

En premier lieu, la fracture numérique serait d'abord liée à une carence d'infrastructure. D'après des rapports publiés par l'IFRC, lors d'expérimentation en avril et mai 2021, dans le camp de Mathare, 55 % des bénéficiaires possédaient un téléphone basique et 28 % d'un smartphone. De surcroit, l'équipe du projet a été aux prises avec un problème technique : un certain nombre de smartphones de bénéficiaires n'avaient pas les mêmes standards que ceux utilisés par le KRCS quand ils testaient la plateforme. Par conséquent, ils n'ont pas pu profiter de la plateforme et ont dû recourir à la version réservée aux téléphones basiques, restreinte à un menu USSD [1875].

À Turkana, situé dans une zone rurale, 62 % des foyers n'avaient pas un téléphone mobile et en l'absence de réseau de connexion — les participants ont reçu un QR code[1876]. Pour rappel, seuls les bénéficiaires dotés de téléphones peuvent gérer leur propre système d'identification. Et pour les personnes équipées de téléphones, une partie des personnes ne seraient pas familières avec les codes PIN : « D'après le personnel de KRCS, les habitants des zones rurales ainsi que les personnes âgées et défavorisées ne sont pas familiarisés avec le concept de code PIN. Lorsqu'ils utilisent MPESA[1877], ils s'en remettent à l'agent Safaricom qui fait partie de leur communauté. Cet agent emploie simplement l'année de naissance comme code PIN, de sorte

[1873] POULLET, Y, DELFORGE, A, « Les blockchains : un défi et/ou un outil pour le RGPD ? », in : COTIGA, Andra, JACQUEMIN, Hervé, POULLET,Yves (dir.*), Les blockchains et les smart contracts à l'épreuve du droit*, Collection du CRIDS, Numéro 49, Larcier , Bruxelles, 2020,p. 97-135. http://www.crid.be/pdf/crid5978-/8630.pdf

[1874] Kenya Red Cross, Uganda red cross Society, "Dignified identities in humanitarian action : journey and reflection", February 2023https://cash-hub.org/wp-content/uploads/sites/3/2023/03/DIGID-Summary-Report-Final.pdf

[1875] IFRC, ICHA, Kenya Red Cross, "Dignified Identities in Cash Assistance: More Lessons Learnt from Kenya (July – November 2021) https://cash-hub.org/wp-content/uploads/sites/3/2022/02/DIGID-More-Lessons-Learnt-from-Kenya-Jan-2022.pdf

[1876] IFRC, Kenya Red Cross, ICHA, "Dignified identities in cash assistance : lessons learnt from Kenya", January 2022https://cash-hub.org/wp-content/uploads/sites/3/2022/02/DIGID-Lessons-Learnt-from-Kenya-Jan-2022.pdf

[1877] MPSEA est un système de transfert monétaire très répandu au Kenya, lancé en 2007 par Vodafone pour Safaricom et Vodacom.

que lorsque l'utilisateur présente sa carte d'identité, il sait ce qu'il doit faire. «[1878] Gravity, le partenaire technique, a pu proposer des moyens d'identifications alternatifs, de types biométriques, mais potentiellement sensibles.

Enfin, le fait d'être doté d'un smartphone ne signifie pas nécessairement d'avoir une maitrise complète du numérique. On peut sur ce point se référer à des données d'un atelier d'échanges sur le projet ayant eu lieu au Kenya, en aout 2021 auprès de 43 personnes, dont 77 % possédaient un smartphone. Malgré le fait d'être « équipés », les échanges donnent l'image d'un manque d'assurance concernant les usages numériques liés aux dispositifs d'identité numérique. Ces résultats proviennent d'ateliers d'échange avec réfugiés au Kenya, camp de Kakuma et installations de Kalobeyei[1879].

Au-delà de la littératie numérique, certains bénéficiaires souffriraient d'un faible niveau d'alphabétisation. Une solution serait d'après le rapport d'avoir recours à des systèmes vocaux interactifs (l'Interactive Voice Response (IVR). Ce type de technologie n'a cependant pas été mis en place. « En effet, l'introduction du menu IVR a nécessité plus de temps pour les consultations avec les utilisateurs, le prototypage et une analyse complète des risques liés à la protection des données et de la vie privée avant le test avec les bénéficiaires réels de l'assistance. Étant donné que le projet DIGID met l'accent sur l'interopérabilité entre les différentes ONG, il faut également tenir compte du fait que l'authentification vocale n'est peut-être pas un mécanisme d'authentification largement employé par les autres ONG. »[1880]

Ensuite, il ressort de plusieurs ateliers menés auprès de bénéficiaires d'un intérêt inégal pour les enjeux liés à l'autodétermination informationnelle. Selon un premier atelier effectué en 2020, la plupart des participants ne comprenaient pas cette idée. Sachant que curieusement, une partie des ateliers n'ont pas eu lieu avec un public étranger au contexte humanitaire : « Étant donné que la majorité des participants n'avaient pas reçu d'aide et n'avaient donc pas partagé leurs données avec les organisations humanitaires, il a été difficile d'obtenir des données significatives sur le fait de savoir si les participants estimaient avoir un droit de regard sur les données qu'ils partageaient avec les organisations humanitaires. Par conséquent, le droit de consulter leurs propres données, et le fait de demander leur correction et leur suppression n'ont pas été abordés. Cependant, les participants ont mentionné qu'ils seraient prêts à partager des données avec la Croix-Rouge Kenyane puisqu'il s'agit d'une entité connue. »[1881]

---

[1878] to accounts from KRCS staff, people in rural areas as well as elderly and disadvantaged people are not familiar with the concept of a PIN. When they use MPESA they rely on the Safaricom agent who is part of their community. This agent will simply use the year of birth as their PIN so when the user comes with their ID card they know what to do. »

[1879] IFRC, Cash and voucher assistance in migration context, voices of migrants in Kenya, January 2022 https://cash-hub.org/wp-content/uploads/sites/3/2022/03/Cash-in-Migration-Voices-of-Migrants_Kenya-Final.pdf

[1880] "This is because the introduction of the IVR menu required additional time for user consultations, prototyping and a full analysis of the data protection and privacy risks before testing with real beneficiaries of assistance. Given the DIGID project's focus on interoperability between different NGOs, an additional consideration was that voice authentication may not be a widely used authentication mechanism by other NGOs." Kenya Red Cross, DIGID project, user consultation report", 2020, https://static1.squarespace.com/static/5b75620445776e4b290c0d96/t/603d14c5775eed6fbde2883b/1614615753940/%5BFinal%5D+DIGID+Kenya+User+Consultation+Report.pdf

[1881] "Given that a majority of participants had not received assistance and had therefore not shared their data with humanitarian organizations, it was difficult to obtain meaningful responses on whether participants felt they had agency over the data they shared with

Selon d'autres ateliers — effectués en 2022 cette fois-ci auprès de bénéficiaires de la Croix rouge kenyane —, le degré d'intérêt pour l'autodétermination informationnelle varierait, notamment selon le degré de littératie[1882]. Et en ce qui concerne les personnes faisant preuve d'un manque d'intérêt pour la possibilité de gérer ses données, l'IFRC liste plusieurs raisons :

- Tout d'abord, les bénéficiaires font confiance à la Croix rouge kenyane. Ils considèreraient qu'elle administre bien leurs données.

- « Ils peuvent ne pas percevoir leurs données comme ayant de la valeur et méritant qu'on en revendique la maitrise. Il est peu probable que ce soit le cas, car des membres de la communauté ont indiqué qu'ils connaissaient la valeur de leurs propres données lorsqu'on leur a posé la question. »[1883]

- Le fait de ne pas avoir consacré assez de temps sur le terrain pour sensibiliser les participants à ces enjeux.

Pour éveiller l'intérêt pour le projet et pour l'autodétermination informationnelle, les promoteurs de DIGID conseillent de mettre en avant les aspects concrets pouvant être associés à la gestion de ses données : « L'équipe de projet a indiqué qu'il fallait davantage d'incitations pour que les gens s'approprient et gèrent leurs données. Par exemple, la Croix-Rouge Kenyane pourrait demander aux communautés d'utiliser leur carte d'identité numérique comme preuve d'éligibilité pour accéder à d'autres services que la distribution d'argent. En outre, lorsque l'éligibilité est liée à des attributs changeants, tels que la taille de la famille, il pourrait y avoir plus de motivation pour s'assurer que les données personnelles sont à jour. »[1884]

Le rapport conclut qu'il est nécessaire de mener des actions de sensibilisation. Cela signifie clarifier les avantages associés au partage de ses données — et notamment à l'aspect numérique des SSI : « Cet engagement visait à démystifier et à expliquer l'objectif des cartes d'identité numériques émises par la Croix-Rouge Kenyane — quelles données seraient collectées, comment elles seraient utilisées et ce que les utilisateurs finaux pourraient faire avec les cartes d'identité numériques — ainsi qu'à obtenir les commentaires des utilisateurs sur la solution globale et le problème qu'elle cherchait à résoudre. »[1885] Cependant, il ressort

---

humanitarian organizations. Consequently, questions about the right to view their own data, request for its correction and deletion were not addressed. However, participants mentioned that they would be willing to share data with KRCS since it is a known entity." Gravity, IFRC, "Kenya Red Cross, DIGID project, user consultation report", 2020, https://static1.squarespace.com/static/5b75620445776e4b290c0d96/t/603d14c5775eed6fbde2883b/1614615753940/%5BFinal%5D+DIGID+Kenya+User+Consultation+Report.pdf

[1882] IFRC, "Cash and voucher assistance in migration context, voices of migrants in Kenya", January 2022 https://cash-hub.org/wp-content/uploads/sites/3/2022/03/Cash-in-Migration-Voices-of-Migrants_Kenya-Final.pdf

[1883] « they may not perceive their data as valuable and worth expressing ownership over. This is unlikely to be the case, as community members indicated knowing the value of their own data when asked. »
IFRC, "Kenya Red Cross, Dignified identities in Cash assistance : lessons learnt from Kenya",2022.
https://cash-hub.org/wp-content/uploads/sites/3/2022/02/DIGID-Lessons-Learnt-from-Kenya-Jan-2022.pdf

[1884] "the project team indicated the need for more incentives for people to own and manage their data. For instance, KRCS could ask communities to use their digital IDs as proof of eligibility to access other services beyond cash distribution. Additionally, when eligibility is tied to changing attributes, such as family size, there might be more motivation to ensure personal data is up to date."
IFRC, Kenya Red Cross, ibid.

[1885] Such engagement aimed to help demystify and explain the purpose of the digital IDs being issued by the KRCS – what data would be collected, how it would be used, and what end users could do with the digital IDs – as well as to get users' feedback on the overall solution and the problem it sought to address. Ibid.

de différentes consultations que certains bénéficiaires préfèreraient des dispositifs non numériques d'identité. Or, seules les personnes détentrices d'un téléphone mobile peuvent gérer directement leurs données. Il existerait une contradiction entre la volonté émancipatrice portée par DIGID et une forme de normativité des usages numériques. Et ce alors que l'IFRC conclut dans un rapport sur le projet qu'il semblerait que les identités souveraines ne sont pas adaptées pour les personnes « vulnérables » et dotées d'une faible littératie numérique[1886].

Par voie de conséquence, pour réduire la fracture numérique, les promoteurs du projet ont exploré plusieurs solutions. Certaines d'entre elles impliquent de passer par des tiers, devenant des gestionnaires d'identités. Le projet DIGID propose de mettre en place des « gestionnaires d'identité » ou des « curateurs d'identité »[1887]. L'IFRC reconnait que la solution d'une gestion déléguée des données est plus sûre, mais qu'elle ne permet pas aux bénéficiaires de contrôler leurs propres données : « Mais elle dépend toujours de l'organisation humanitaire émettrice pour garder les données au nom des personnes qu'elle sert, ce qu'elle fait généralement aujourd'hui lorsqu'elle recueille des données. »[1888]

Une solution serait d'avoir recours à un QR code pour accéder aux données en s'identifiant à un point d'identification et accéder aux portefeuilles stockés par une organisation. « En stockant plusieurs portefeuilles sur un seul appareil commun avec des mécanismes d'accès uniques par utilisateur, plusieurs utilisateurs peuvent accéder à leurs données d'identification à distance. Cependant, le fonctionnement de plusieurs types de portefeuilles numériques dépend de la possession d'un smartphone, que de nombreux bénéficiaires de l'aide humanitaire n'ont pas. Dans ce cas, l'utilisation de mécanismes d'authentification analogiques pourrait soutenir le cycle de vie de l'identité sans appareils. Un code-barres sur papier, par exemple, pourrait permettre à un bénéficiaire de s'authentifier à un point d'interaction et d'accéder à ses données d'identification sur un dispositif local hébergé par une organisation humanitaire. »[1889]

Une autre solution consiste à déléguer la gestion des clefs à une organisation (comme peut le faire le WFP). Mais il est envisagé de prendre plus en compte le bénéficiaire. Le consortium a ainsi émis l'idée d'une mise en place de gestion partagée des clefs. Ces dernières seraient « fragmentées » en plusieurs parties : « D'autres mécanismes facilitant une "user centric guardianship" incluent l'utilisation de clefs divisées. En divisant une clef entre trois

---

[1886] "Several lessons related to governance, technology, and user behavior were identified. One is that the pure self-sovereign identity model was not appropriate for the most vulnerable who do not have access to smartphones, have limited digital literacy, and live in areas where there's low connectivity." "Dignified identities in humanitarian action : journey and reflexion", February 2023 https://interoperability.ifrc.org/wp-content/uploads/2023/11/DIGID-Summary-Report-Final.pdf

[1887] "Agree on the principle of users having control over their own data, but someone liable needs to put in the equation for safeguarding of identity. "ibid.

[1888]« But still relies on the issuing humanitarian organization to guard the data on behalf of the people they serve, which is typically what they do now when they collect data" ibid

[1889] "By storing several wallets on a single, common device with unique access mechanisms per user, multiple users could access their credentials remotely. Still, the operation of several kinds of digital wallets depends on possession of a smartphone, which many beneficiaries of humanitarian aid do not have. In these cases, the use of analogue authentication mechanisms could support the identity lifecycle without a device. A paper-based barcode, for instance, could enable a beneficiary to authenticate themselves at a point of interaction and gain access to their credentials on a local device hosted by a humanitarian organization." IFRC, "Digital identity, an analysis for the humanitarian sector", 2021.
https://static1.squarespace.com/static/5b75620445776e4b290c0d96/t/60a53f8ec37bbe66f938df75/1621442472657/Digital+Identity%E2%80%93An+Analysis+for+the+Humanitarian+Sector+Final.pdf

bénéficiaires ou plus, puis en reconstituant une clef unique à un point d'interaction, un bénéficiaire peut contrôler ses données sur une variété de dispositifs non natifs. »[1890] Cependant, le fait de mettre en place des systèmes de gestion d'identification délégués parait difficile dans un contexte migratoire : « Toutefois, dans le contexte migratoire, la manière dont la tutelle numérique sera appliquée lorsque la personne se déplacera d'un pays à l'autre pose question. »[1891]

Plus largement, il existe d'autres formes de délégation de gestion de données. Paul Currion mène une réflexion sur la possibilité de créer des « data stewardship » dans un cadre humanitaire : « Le "data stewardship" est un modèle de gouvernance des données dans lequel un intermédiaire facilite ou détient le consentement et la prise de décision au nom des utilisateurs, parfois avec une responsabilité fiduciaire en vertu de la loi. »[1892] Ce type de dispositifs lui paraissent cependant difficiles à mettre en place : « Il est peu probable que les organisations humanitaires soient elles-mêmes de bons gestionnaires de données en raison a) de priorités concurrentes et b) de capacités limitées. »[1893] Paul Curion propose des pistes pouvant aller dans ce sens. Par exemple, ce type d'initiative pourrait pour lui être reliée à des discussions portant sur la localisation de l'aide : « Elle s'inscrit également dans le cadre des discussions sur l'accroissement de la localisation et de la responsabilité, ce qui devrait faciliter l'obtention d'un soutien. L'application du concept au sein de communautés définies pour des secteurs spécifiques dans des juridictions appropriées devrait être étudiée dans le cadre de l'approche globale de la communauté humanitaire en matière de gestion des données. »[1894]

Mais cette prise en compte des bénéficiaires doit réellement leur donner une alternative, plutôt que de combler une fracture numérique. Cela signifierait d'être ouverts à d'autres modalités de gestions de l'information[1895]. Et on peut lire au détour d'un rapport de DIGID que « les organisations devaient proposer une véritable option de refus pour les solutions

---

[1890] "Other mechanisms of facilitating user-centric guardianship include the use of split keys. By splitting a key among three or more beneficiaries, and then reconstituting a single key at a point of interaction, a beneficiary can control their data across a variety of non-native devices." Ibid.

[1891] « However, in the context of people on the move, this raises concerns about how digital guardianship will be applied when the person moves from country to country. »Ibid.

[1892] « Data stewardship is a model of data governance in which an intermediary facilitates or holds consent and decision-making on behalf of users, sometimes with a fiduciary responsibility under law » CURRION, Paul, "Safe passage, options for data portability in the humanitarian sector", collaborative cash, 2022
https://www.collaborativecash.org/_files/ugd/477045_8adbdc1a90144e67b86f943284d1509b.pdf

[1893] « Humanitarian organizations are unlikely to be good data stewards themselves due to a) competing priorities and b) limited capacity. Any kind of data steward arrangement for the humanitarian sector would be likely to require the identification or (more likely) creation of a third party to act as steward. Given the internal politics of the sector, there is a good chance that the mandate for this would be granted to an existing mandate organization such as UNHCR, which has a stronger legal foundation on which to take on such responsibility. As discussed elsewhere in this report, however, such mandate organizations have tended to take an approach which does not lend itself to stewardship. »
CURRION, Paul, "Safe passage, options for data portability in the humanitarian sector", collaborative cash, 2022
https://www.collaborativecash.org/_files/ugd/477045_8adbdc1a90144e67b86f943284d1509b.pdf

[1894] « It also fits within discussions about increased localization and accountability, which should make it easier to gain support. Applying the concept within defined communities for specific sectors in appropriate jurisdictions should be explored as part of the humanitarian community's overall approach to data management. »
CURRION, Paul, "Safe passage, options for data portability in the humanitarian sector", collaborative cash, 2022
https://www.collaborativecash.org/_files/ugd/477045_8adbdc1a90144e67b86f943284d1509b.pdf

[1895] Paul Currion cautioned that digital identity solutions may remove many of those resistance strategies and make it more difficult for beneficiaries, rather than less [#6]. For one data rights expert, the existence of channels of contestation and the ability for affected individuals to truly make use of them is the bare minimum that needs to be in place for beneficiaries to have any claim to be seen as legitimate, equal, and rights-bearing human beings. Without the option to resist and contestdigital identity-related practices or forms of information control, beneficiaries' data become a "limbo zone in which you can dip in to create things and to collect things ad libitum"IFRC, "Digital identity, an analysis for the humanitarian sector", 2021. https://static1.squarespace.com/static/5b75620445776e4b290c0d96/t/60a53f8ec37bbe66f938df75/1621442472657/Digital+Identity%E2%80%93An+Analysis+for+the+Humanitarian+Sector+Final.pdf

d'identité numérique afin d'atténuer l'asymétrie de pouvoir entre le fournisseur d'aide et la personne. Le déséquilibre de pouvoir s'est manifesté par le fait que les personnes considéraient les dispositions non souhaitables en matière de garde des données comme le seul moyen de recevoir une aide vitale. »[1896] Et s'il existe un droit à l'information et à la connectivité[1897], il devrait également exister un droit à la déconnexion, également pour les plus précaires[1898].

Dans notre septième chapitre, on a voulu compléter le sujet de l'autodétermination informationnelle en nous intéressant aux différentes façons d'outiller technologiquement cette dernière. On est ainsi revenue sur plusieurs projets de blockchain afin de comprendre comment elles peuvent (ou non) reconfigurer les relations de pouvoir entre ONG et bénéficiaires et leur redonner une certaine maitrise de leurs données. La portée émancipatrice de ce type de projet est toutefois limitée par le fait que les blockchains sont des dispositifs complexes, nécessitant une certaine littératie numérique, qui manque en partie aux bénéficiaires. Mais bien plus, les problématiques de fractures numériques auxquelles les ONG font face ne concernent pas tant la compréhension des blockchains que le simple fait de disposer d'un équipement technologique (téléphones mobiles ou smartphone). Pour résoudre ce problème, il a pu être envisagé de passer par des tiers, devenant gestionnaires d'identités, au risque de s'éloigner de l'idéal d'autodétermination informationnelle.

[1896] "Organisations needed to provide a genuine opt-out to digital identity solutions to help mitigate the ways power asymmetry between the aid provider and person manifested. The power imbalance was manifested in the people seeing undesirable data guardianship arrangements as the only avenue towards receiving vital assistance." Kenya Red Cross, Uganda Red Cross Society, "dignified identities in humanitarian action: journey and reflection", February 2023https://interoperability.ifrc.org/wp-content/uploads/2023/11/DIGID-Summary-Report-Final.pdf

[1897] GREENWOOD, Faine, HOWARTH, Caitlin, POOLE, Danielle, RAYMOND, Nathaniel, SCARNECCHIA, Daniel,"The signal code : a human rights approach to information during crisis", 2016 https://reliefweb.int/report/world/signal-code-human-rights-approach-information-during-crisis

[1898] ROSSI, Julien, " A few thoughts on the right to be offline, is there a right not to participate in digital technology?", Working Paper, 03/10/2023 https://www.julienrossi.com/blog/2023/10/03/a-few-thoughts-on-the-right-to-be-offline/

## Chapitre 8 — Redonner un nom aux morts en migration en toute dignité : concilier droit à la vie privée et droit à la vérité

**MONUMENT AUX MIGRANTS MORTS EN MEDITERRANEE, CIMETIERE DE CATANE (PHOTO PERSONNELLE DE L'AUTEURE.)**

## introduction

Le « data protection officer » (DPO) du Comité international de la Croix-Rouge (CICR), Massimo Marelli, soutient que la protection des données dans un contexte humanitaire est une affaire de vie ou de mort[1899]. Mais qu'en est-il de la gestion par des ONG de données de personnes déjà décédées ? Le fait de prendre soin des morts ne va pas de soi pour les humanitaires, dont l'objectif premier est la sauvegarde de la vie de victimes. Lors d'une catastrophe, les traitements consécutifs aux décès restent bien souvent secondaires face à l'urgence de porter assistance aux vivants. Toutefois, lors de morts de masse causés par des catastrophes, les gouvernements locaux ne parviennent pas toujours à remplir les actes minimaux propres à la gestion des morts, à savoir la collecte des corps, l'enterrement, bien souvent dans des fosses communes[1900]. Les ONG peuvent alors soutenir leurs efforts dans cette tâche, voire dans certains cas, se lancer dans le long travail d'investigation menant à

[1899]PFEIFE, Sam, "Doing data protection well in humanitarian efforts", *Iapp*, 25/10/2017 https://iapp.org/news/a/doing-data-protection-well-in-humanitarian-efforts/

[1900] "in some humanitarian contexts, there might be an aversion to address the needs of the dead – in order to first care for the living –, given the time constraints and the challenges that large-scale humanitarian emergencies present. This negatively impacts the dignified management of the dead and contributes to them becoming missing persons." GARIBIAN, Sévane, et al. "The development of guiding principles for the proper management of the dead in humanitarian emergencies and help in preventing their becoming missing persons: First Expert's Meeting", *International Review of the Red Cross*, 2020, vol. 101, no. 912, p. 1213-1229 DOI : 10.1017/S1816383120000223
IRIN, "Why dead body management matters", 31/10/2012https://www.thenewhumanitarian.org/report/96673/analysis-why-dead-body-management-matters
CORBET, Alice, « Invisibles omniprésents, les morts du séisme », dans : LAENNEC, Hurbon (eds), *Catastrophes et environnement*, Éditions de l'École des hautes études en sciences sociales, 2014, p.29-58

l'identification d'un corps[1901]. Or, le CICR s'est donné entre autres comme mission de prendre soin des personnes décédées lors de conflits ou en migration. L'organisation défend en effet la nécessité d'une gestion « digne » des morts. Elle lie la notion de dignité et l'acte d'identification d'un corps, impliquant notamment le fait de leur redonner un nom. Cet acte contribue à rétablir le lien entre un corps et la personne civile décédée. On peut même dire qu'il rend un peu d'humanité à un cadavre. Les morts anonymes peuvent être alors considérés comme des « malemorts »[1902], des morts qui dérogent aux normes en vigueur d'une société[1903]. Et pour ce qui concerne les exilés décédés en migration, ils sortent triplement du corps social, à la fois en tant que parias, en tant que morts et en tant que morts anonymes. Ils sont réduits à être de « purs cadavres » détachés de leur personne passée. Et c'est d'autant plus le cas lorsqu'ils sont réduits à des « restes humains », qui se situent alors aux frontières entre l'humanité et les choses[1904]. Une chercheuse comme Amade M'Charek considère ainsi que leur redonner un nom, c'est leur permettre de retrouver leur appartenance à un groupe social[1905]. C'est ce que suggère la définition que donne le CICR du processus d'identification : « une identification est l'aboutissement d'un processus de comparaison d'informations. Il est nécessaire de déconstruire le concept d'identification fréquemment utilisé, dans un sens restrictif, comme synonyme de la technique employée pour parvenir à la conclusion (par exemple, l'identification génétique ou l'identification dentaire), et d'adopter une approche plus complète, holistique, intégrée et multidisciplinaire. "L'identité" désigne ce qui relie un nom à un corps physique. Mais ce terme englobe également les liens sociaux qui rattachent une personne à un lieu, à une époque et, surtout, à d'autres individus. En ce sens, le processus d'identification doit prendre en compte non seulement les défis techniques, mais aussi les complexités politiques et sociales et ce qu'elles impliquent. »[1906]

Tout ceci s'inscrit dans la continuité de nos réflexions antérieures. Notre fil rouge concernait le lien entre protection des données et concept de dignité. Pour rappel, on s'était demandé comment les ONG procédaient pour respecter les différents droits accordés aux bénéficiaires par le RGPD. L'enjeu était, pour ces derniers, de retrouver une forme de dignité grâce à la

---

[1901] Par exemple c'est la Croix Rouge qui s'était chargée d'enterrer les corps lors de l'épidémie d'Ebola https://www.croixrouge.ca/blogue/2014/9/les-equipes-de-la-croix-rouge-aux-premieres-lignes-de-la-lutte-contre-l-ebola-en-guinee

[1902] Le terme « malemort » désigne les morts violentes, ne pouvant faire l'objet des pratiques prescrites et bénéficier de soins du corps et de rituels appropriés et dignes selon les codes d'un groupe social. La malemort est donc à relier à la circonstance spécifique du décès, au traitement du cadavre et à la pratique rituelle en général. La malemort évoque aussi, notamment dans les cultures asiatiques, l'idée d'un mort parti dans des conditions douloureuses (suicide, assassinat) et qui continue de souffrir.

[1903] CAROL, Anne, RENAUDET, Isabelle, *Des morts qui dérogent, à l'écart des normes funéraires, XIXème-XXème siècles*, Presses universitaires de Provence, 2023,250 p.

[1904] CLAVANDIER, Gaelle, « De nouvelles normes à l'égard des restes humains anciens : de la réification à la personnalisation ? «, *Revue canadienne de bioéthique*, 2 (3),2019, p.79— 87. https://doi.org/10.7202/1066465ar

[1905] Tribune, collectif, "Migration : "inscrivons l'obligation d'identification des défunts anonymes dans le droit européen", *Le Monde*, 30/08/2023https://www.lemonde.fr/idees/article/2023/08/30/migration-inscrivons-l-obligation-d-identification-des-defunts-anonymes-dans-le-droit-europeen_6187087_3232.html

M'CHAREK, Amade, BLACK, Julia," Engaging Bodies as Matters of Care Counting and Accounting for Death During Migration", in, CUTTITTA, Paolo, LAST, Tamara (eds.) , *Border Deaths, Causes, Dynamics and Consequences of Migration-related Mortality,* Amsterdam University Press,2020, 174 p.

M'CHAREK, A., CASARTELLI, S., "Identifying dead migrants: forensic care work and relational citizenship", *Citizenship Studies*, 23(7), 2019, p.738-757. https://doi.org/10.1080/13621025.2019.1651102

[1906] CICR, « Le processus d'identification forensique : une approche intégrée », 2022 https://www.icrc.org/fr/publication/4590-forensic-human-identification-process-integrated-approach

possibilité de maintenir un certain contrôle sur la gestion de leurs données. Leur reconnaitre ces droits suppose de ne plus les considérer comme de « pures » victimes. D'un point de vue académique, cela permet de nuancer les analyses de l'humanitaire comme biopolitique. Dans ce chapitre, on restera dans la lignée de ces réflexions. Nous cherchons toujours à dépasser l'idée que les bénéficiaires sont des « sans droits ». Mais notre approche est quelque peu différente puisqu'on s'intéresse aux droits des morts et à leur dignité. Pour des juristes, le sujet pose question : les morts n'ont en théorie plus de personnalité juridique. Cela dit, dans le détail, il est, malgré tout, accordé des droits subsidiaires aux morts. Et surtout, le travail des médecins légistes, en redonnant une identité administrative aux morts, leur permet de bénéficier de certains droits bien spécifiques. On se demandera alors si le droit à la vie privée en fait partie. Après tout, certains chercheurs réfléchissent sur la vie privée post-mortem. Et l'objectif de ce chapitre est de montrer que s'interroger sur la vie privée des morts n'est pas si incongru. On reviendra donc sur les différents enjeux éthiques et juridiques entourant cette question. Concernant la médecine légiste humanitaire, on verra que rendre une dignité aux morts anonymes va de pair avec un travail d'identification qui nécessite de traiter des données très sensibles. Il existe par conséquent une tension entre identification et protection des données. Remarquons que ce type de tension se retrouve au sujet des initiatives visant à redonner une identité administrative aux personnes dépourvues d'identité légale. Cet acte leur permettrait de les réinscrire dans un corps social, mais il s'accompagne avec de potentielles dérives en matière de protection des données. Il existe ainsi une dialectique entre reconnaissance et surveillance. Les chercheurs Keren Weitzberg, Margie Cheesman et Emrys Schoemaker ont en étudié certaines de ses manifestations opérant au sein de dispositifs d'identité numériques employés par les humanitaires[1907]. On s'intéressera pour notre part à la manière dont on retrouve cette tension au sujet de l'identification des morts. En clair, on se demandera comment les personnes impliquées dans l'acte de redonner un nom aux corps envisagent la protection des données. On reste donc dans la lignée de nos réflexions précédentes, mais avec un léger déplacement. On n'établira pas de liens entre le fait de rendre aux bénéficiaires une dignité et le respect des droits accordés par le RGPD. Il s'agit plutôt de comprendre dans quelle mesure rendre une dignité aux morts (une identité), rentre en tension avec les principes de protection des données. Et surtout, au fil de ce chapitre, on se rendra compte d'un point crucial : les personnes chargées du travail des morts doivent aussi être vigilants quant à la protection des données des familles. Effectivement, retrouver l'identité des défunts nécessite de recueillir et de traiter aussi des données de personnes en vie.

Pour résumer, dans ce chapitre on abordera plusieurs points : 1) le fait que l'identification des morts peut être une tâche remplie par des ONG humanitaires, notamment certaines antennes de la Croix-Rouge et le CICR ; 2) le procédé d'identification des morts en lui-même et le type

[1907] WEITZBERG, K., CHEESMAN, M., MARTIN, A., SCHOEMAKER, E., "Between surveillance and recognition: Rethinking digital identity in aid", *Big Data & Society*, 2021, 8(1). https://doi.org/10.1177/20539517211006744

de données qu'il nécessite de traiter ; 3) le débat concernant le fait de savoir si des morts ont des droits ou non, et le sens que les acteurs donnent au fait de traiter « dignement» les morts 4) la problématique générale de la vie privée des morts et de la protection de leurs données ; 5) et enfin le sujet de la protection des données tel qu'il se pose lors du processus d'identification d'un mort et plus spécifiquement des morts en migration.

## Section 1 — Institutionnalisation des méthodes forensiques : l'usage de la médecine légale dans l'humanitaire.

### § 1 — La médecine légale humanitaire

Les experts en science médicolégale interviennent actuellement dans divers théâtres de « mort de masse »[1908]. Au Mexique, des familles attendent l'identification de victimes de la « guerre contre la drogue », le pays souffrant de ce que Claire Moon qualifie de « crise forensique » [1909]. Les conflits contemporains, en Palestine, en Ukraine, au Soudan et en République Démocratique du Congo, ont également leur lot de disparus et de corps non identifiés[1910]. Et les exilés disparaissent également en masse le long des routes migratoires, à la frontière étatsunienne, en mer Méditerranée ou dans les Balkans.

Mais c'est au début des années 1980 que les sciences médicolégales, d'abord appliquées aux scènes de crimes, aux catastrophes aériennes ou naturelles, ont commencé à être employées dans le cadre d'enquêtes sur des crimes de masses et des crimes contre l'humanité. De premières équipes de médecine légale ont été déployées en Amérique latine, notamment en Argentine, pour rendre compte des violations des droits de l'homme et des disparitions

[1908] SUWALOWSKA, Halina, (et alii), « » Les simili » : des cadavres non identifiés : une crise sanitaire mondiale nécessitant une attention urgente » , *The Lancet*, Novembre 2023 https://www-thelancet-com.translate.goog/journals/langlo/article/PIIS2214-109X(23)00420-5/fulltext?mc_phishing_protection_id=28048-ck9upe70s0vd2qa2kllg&_x_tr_sl=en&_x_tr_tl=fr&_x_tr_hl=fr&_x_tr_pto=sc

[1909] MOON, Claire, TREVINO-RANGEL, Javier, "Involved in something (involucrado en alo)": denial and stigmatization in Mexico's "war on drugs", *The British journal of sociology*, volume 71, issue 4, 2020, p.722-740

[1910] CICR, communiqué de presse, « Conflit armé international entre la Russie et l'Ukraine : 23 000 personnes portées disparues », 19/02/2024 https://www.icrc.org/fr/document/conflit-arme-international-entre-russie-et-ukraine-23000-personnes-portees-disparues

AFP, « Ukraine : au moins 37.000 disparus après deux ans d'invasions russe », 16/04/2014 https://www.mediapart.fr/journal/fil-dactualites/160424/ukraine-au-moins-37000-disparus-apres-deux-ans-d-invasion-russe

LITTELL, Jonathan, « En Ukraine, Boutcha et Kharkiv débordées par les cadavres », *Le Monde*, 11/08/2022 https://www.lemonde.fr/m-le-mag/article/2022/08/11/en-ukraine-boutcha-et-kharkiv-debordees-par-les-cadavres_6137734_4500055.html

OURDAN, Remy, « Guerre en Ukraine : la recherche des disparus, un défi vertigineux », *Le Monde*, 20/05/2024 https://www.lemonde.fr/international/article/2024/05/20/guerre-en-ukraine-la-recherche-des-disparus-un-defi-vertigineux_6234305_3210.html

KENNY, Peter, « Missing in action, who do you turn to? The ICRC's Central Tracing Agency », Geneva Solutions, 22/12/2022 https://genevasolutions.news/peace-humanitarian/missing-in-action-who-do-you-turn-to-the-icrc-s-central-tracing-agency

CICR, Soudan : un an après le début du conflit, la douleur des familles de personnes disparues se fait plus vive à l'heure de célébrer l'Aïd, 10/04/2024https://www.icrcnewsroom.org/story/fr/2085/sudan-after-a-year-of-conflict-missing-family-bring-extra-heartache-during-eid-celebrations

PASSILY, Augustine, « Ces bénévoles qui tentent de retrouver les disparus dans la guerre du Soudan », *Le Temps*, 12/05/2023 https://www.letemps.ch/monde/afrique/benevoles-tentent-retrouver-disparus-guerre-soudan

AFP, « l' » insoutenable » recensement des victimes dans les ruines d'un hôpital de Gaza », *L'Express*, 09/04/2024 https://www.lexpress.fr/monde/linsoutenable-recensement-des-victimes-dans-les-ruines-dun-hopital-de-gaza-IJZRVVOVVREZRIRTFSIGMNNXL4/

forcées sous la junte. Ces initiatives ont une dimension politique et la médecine légale appuie alors la justice pénale internationale. L'objectif premier de ce type d'enquête n'est pas d'identifier des corps, mais d'attester de l'ampleur des massacres, au nom du droit à la vérité[1911].

Les mêmes méthodes ont été utilisées pour témoigner des génocides au Rwanda et en ex-Yougoslavie. Un autre acteur clef des morts de masse a alors vu le jour durant le conflit dans les Balkans : la commission internationale des personnes disparues, l'International commission of missing persons, (ICMP) [1912] . L'organisation a soutenu la cour pénale internationale dans la tenue de procès à la suite du conflit yougoslave. Or le CICR était aussi impliqué dans la recherche des disparus dans les Balkans[1913]. C'est cette expérience qui a servi de « catalyseur » et a impulsé au sein du CICR la création d'une unité de médecine légale, en 2003[1914]. Mais l'approche du CICR n'est pas judiciaire. Le CICR ne s'investit pas dans des démarches de justice pénale en lien avec des violations de droits de l'homme. Elle ne pointe pas les responsabilités politiques de violence, mais elle serait caractérisée par une plus grande prise en compte des besoins des individus et des familles[1915]. Par conséquent, l'identification d'un corps constitue la finalité principale de ce type d'approche, afin que les proches puissent amorcer un travail de deuil.

Le CICR est l'une des rares organisations à vocation humanitaire à posséder une unité forensique, et à proposer une expertise sur le sujet. Cela s'explique par le fait que, comme l'écrit la chercheuse Claire Moon, le CICR s'est depuis longtemps préoccupé du sort des morts et des disparus. Le DIH (droit international humanitaire) a été fondé en réaction aux tueries de la Bataille de Solferino, à la fin du XIXe. Ainsi, la dignité des morts est protégée par ce corpus juridique[1916]. Si l'on se réfère au DIH et aux conventions de Genève, il est clair qu'en situation de conflit armé international, les États parties ont le devoir de rechercher les personnes

---

[1911]NAFTALI, Patricia, La construction du « droit à la vérité » en droit international, Bruxelles : Bruylant, 2017, p.576
Le HCDH et la justice transitionnelle https://www.ohchr.org/fr/transitional-justice/truth
Right to truth, truth(s) through rights, mass crimes impunity and transitional justice, https://right-truth-impunity.ch/fr

[1912] Il s'agit d'une organisation internationale fondée en 1996, à l'initiative notamment de Bill Clinton. Son mandat était d'appuyer les efforts d'investigation relatifs aux disparus dans le conflit en ex-Yougoslavie. Actuellement, elle travaille à « assurer la coopération des gouvernements et d'autres acteurs pour traiter la question des personnes disparues, y compris des dispositions visant à renforcer les capacités institutionnelles, à encourager la participation du public et à répondre aux besoins de la justice, et à fournir une assistance technique aux gouvernements pour localiser, retrouver et identifier les personnes disparues. » Son mandat a été élargi en 2013 et comprend les disparus dus aux « violence organisées », incluant les trafics d'êtres humains, les violences dues aux trafics de drogues, ainsi que les disparitions liées aux migrations. https://www.icmp.int/what-we-do/ https://www.icmp.int/about-us/history/

[1913] ICRC "Unknown fate, untold grief, ICRC activities on behalf of missing persons and their families from the conflicts in Croatia, Bosnia-Herzegovina and Federal Republic of Yugoslavia/ Kosovo", August 2002https://www.icrc.org/en/doc/assets/files/other/sr_balkans_missing.pdf

[1914] CICR, « Les personnes portées disparues et leurs familles, résumé des conclusions des événements préliminaires à la Conférence internationale d'experts gouvernementaux et non gouvernementaux », 19-21 février 2003https://www.icrc.org/fr/doc/assets/files/other/icrc_themissing_012003_fr_10.pdf
DUBOIS, Olivier, MARSHALL, Katharine, SPARKES MCNAMARA, Siobhan, "Nouvelles technologies et nouvelles politiques : l'évolution de l'action du CICR en faveur des familles séparées", *Revue internationale de la Croix rouge*, Volume 94, 2012/4https://international-review.icrc.org/sites/default/files/20-dubois_marshall_mcnamara_cicr94_fr.pdf

[1915]CONGRAM, Derek (eds.), *Missing persons, multidisciplinary perspectives on the disappeared*, Canadian scholars, 2016, 368 p.
ROSENBLATT, Adam, "The danger of a single story about forensic humanitarianism", *Journal of Forensic and legal medicine*, VOl.61, 2019, P.75-77

[1916] GAGGIOLI, Gloria, "international humanitarian law: the legal framework for humanitarian forensic action", *Forensic Science International*, Volume 282, 2018, p.184-194

décédées (GI art. 15 ; GII art. 18, GIV art. 16). Ils doivent également s'efforcer de rassembler les informations nécessaires à l'identification des morts (GI art. 16 et GPI art. 33.2). De même, les morts doivent être respectés, être enterrés honorablement et les sépultures doivent être marquées afin de faciliter l'accès et la protection des tombes (GI art. 17 et GPI art. 34.1). En outre, les restes des personnes décédées doivent être respectés, et le retour à leur famille doit être facilité autant que possible (GPI art. 34.2)[1917].

Ensuite, une des missions historiques du CICR est le rétablissement des liens familiaux (RFL), dont l'origine remonte au conflit franco-prussien en 1870. Ce mandat implique de disposer d'entité d'échange d'information, notamment grâce à l'Agence centrale de recherche[1918]. La Première Guerre mondiale est un autre moment important pour l'agence. Durant ce conflit, la Croix-Rouge prend part au lourd travail de recherche des nombreux disparus de la Grande Guerre, et au travail, encore rudimentaire, de gestion des morts[1919]. Ce dernier inclut la collecte des corps et des tombes, mais aussi les premiers actes d'identification. Après la Première Guerre s'opère une progressive formalisation d'obligations que les vivants doivent aux morts dans le cadre du DIH. Ce corpus juridique a été fondé en réaction aux tueries de la Bataille de Solferino, à la fin du XIXe. Il est tout d'abord simplement mention de l'obligation de collecter les morts et les rendre à chaque partie prenante des conflits. Au cours du XXe, les articles concernant les morts prennent une place plus en plus importante dans le DIH. À la suite de la Première Guerre mondiale, la Convention de Genève de 1929 mentionne les premières recommandations permettant une identification minimale des cadavres des soldats[1920]. Ces obligations sont élargies aux civils après la Seconde Guerre mondiale. Elles

---

[1917] MSF, Personnes disparues et les morts, Dictionnaire pratique du droit humanitaire https://dictionnaire-droit-humanitaire.org/content/article/2/personnes-disparues-et-les-morts/

[1918] En 1870, le CICR crée à Bâle l'agence centrale de recherches. Son objectif, collecter le plus de données possibles sur les soldats blessés ou capturés, mais aussi sur les morts afin de renseigner les familles sur le sort de leur proche porté disparu. JOLI, Frédéric, « Depuis plus de 150 ans, l'Agence centrale de recherches au service des familles en quête de nouvelles de proches portés disparus », *Blog CICR*, 02/06/2022 https://blogs.icrc.org/hdtse/2022/06/02/depuis-plus-de-150-ans-l-agence-centrale-de-recherches-au-service-des-familles-en-quete-de-nouvelles-de-proches-portes-disparus/

[1919]« les soldats ordinaires cessèrent d'être « enterrés où ils tombaient — dans les champs, au bord de la route, parfois seuls, parfois ensemble », écrit un membre de la Croix-Rouge britannique dans son carnet de guerre ; lui et ses collègues entreprirent de « chercher les tombes, identifier les soldats, marquer les sépultures d'une croix, enregistrer leur localisation ». Il rapporte qu'« aucune unité de l'armée n'existait pour faire ce genre de travail de recensement ». LAQUEUR, Thomas, Chapitre IX, les noms de la Grande Guerre, dans : LAQUEUR, Thomas, *Le travail des morts, une histoire culturelle des dépouilles mortelles*, Paris : Gallimard, p.771

« Tout au long de la guerre, la Croix-Rouge s'efforça d'aider les familles à obtenir des nouvelles de proches portés disparus ; une petite équipe composée de 150 volontaires et de 15 dactylographes œuvrait pour trouver des hommes qui pour l'heure n'étaient ni morts ni vivants. Mais bientôt d'autres agences prirent à leur compte les autres rôles de la Croix-Rouge britannique. En octobre 1916, un nouveau Central Prisoners of War Committee au sein du ministère de la Guerre commença à garder la trace des prisonniers, même si la Croix-Rouge travaillait étroitement avec lui. » LAQUEUR, Thomas, ibid.

FOSTER, Ann-Marie, "The Bureaucratization of Death: The First World War, Families, and the State", *Twentieth Century British History*, Volume 33, Issue 4, December 2022, p. 475–497, https://doi.org/10.1093/tcbh/hwac001

CAPDEVILLA, Luc, VOLDMAN, Danièle, "Du numéro matricule au code génétique : la manipulation du corps des tués de la guerre quête d'identité", *Revue internationale de la Croix Rouge*, 2002, Vol.84, n° 848 https://www.icrc.org/fr/doc/assets/files/other/irrc_848_capdevila.pdf

[1920] "Significant leap in the development of the principle of identification is the express instruction in the 1929 Geneva Convention on Wounded and Sick to leave one half of the military identity disc13 on the body, thus making the continuous identification of bodies possible – not only the one-time identification for the drafting of a list of the fallen, but the potential to identify the individual body also in the future. It is in this same instrument that exhumation is first mentioned. "

WELS, Welmoet, "Dead body management in armed conflict : paradoxes in trying to do justice to the dead, international legal framework, recent developments, and future perspectives for a general duty of care for the dead", Master Thesis, Law, University of Leiden, 2015 https://scholarlypublications.universiteitleiden.nl/access/item%3A2866460/view

WELS, Welmoet, "Dead bodies of war in legal historical context", *Articles of war*, 28/03/2023 https://lieber.westpoint.edu/dead-bodies-war-legal-historical-context/

sont promulguées lors de la IVe convention de Genève de 1949 et dans ses protocoles additionnels de 1977 portant sur les articles dédiés aux morts (aussi bien les morts civils que les morts belligérants) qu'on cite le plus souvent. Ainsi, comme indiqué plus haut, selon la Convention de Genève, les États parties du conflit ont maintenant le devoir de rechercher les personnes décédées dans le cadre d'un conflit (GI art. 15 ; GII art. 18, GIV art. 16)[1921]. Ce devoir concerne les morts civils comme les soldats. Pareillement, le mandat de l'agence du RFL connait le même élargissement. Il ne s'agit plus simplement de retrouver les militaires tombés au front, mais aussi des non-combattants. Cette agence est rebaptisée en 1959 la « Central Tracing Agency »[1922]. Mais l'implication du CICR à proprement parler dans l'identification des morts est plus tardive. Et comme on l'a dit, le CICR prend part aux premières initiatives d'identification des morts à partir du conflit des Balkans, dans les années 1980. Et ce n'est que progressivement que la médecine légale s'est stabilisée au sein de l'humanitaire et du CICR. L'identification des morts ne fait pas partie du mandat historique de l'agence, d'ailleurs le travail forensique, perçu comme appartenant au champ du judiciaire, a longtemps été l'affaire des tribunaux internationaux, car ce travail va à l'encontre du principe de neutralité cher au CICR. Il n'y a pas de « cluster » de médecine légale et le cluster santé n'a pas de spécialistes sur le sujet[1923]. Plus largement, il n'y a pas d'ONG humanitaire ayant comme mandat l'identification des cadavres. Or des « entrepreneurs de causes », en majorités des médecins légistes employés par le CICR, ont cherché à « pérenniser » la place de cette discipline au sein de l'institution[1924]. Un de leur objectif est donc d'en faire une composante de l'action humanitaire. On peut ainsi lire dans un manuel de médecine légale du CICR que : « la gestion des morts est un élément essentiel de la réponse aux urgences humanitaires, au même titre que la recherche, le rétablissement et la prise en charge des survivants, ainsi que la fourniture

[1921]GAGGIOLI, Gloria, "international humanitarian law : the legal framework for humanitarian forensic action", *Forensic Science International*, Volume 282, 2018, p. 184-194
MSF, Personnes disparues et les morts, Dictionnaire pratique du droit humanitaire https://dictionnaire-droit-humanitaire.org/content/article/2/personnes-disparues-et-les-morts/

[1922] CICR, Agence centrale de recherches du CICR : un demi-siècle de rétablissement des liens familiaux, 07/04/2010 https://www.icrc.org/fr/doc/resources/documents/interview/centra-tracing-agency-interview-070410.htm

[1923] « One of the most challenging areas continues to be the frequent absence of forensic specialists on the ground in humanitarian emergencies, due to the unavailability, for the most part, of a "cluster" on the management of the dead in national and local emergency services. Professionals of the health "cluster" not experienced in the management of the dead are often mobilized instead, while forensic expertise remains mostly absent from national emergency plans. Shortage of forensic specialists can occur due to the lack of sufficient capacity, including specialized training and necessary resources, observed in some national medico-legal and police institutions. Moreover, in some humanitarian contexts, there might be a reluctance to care for the dead – in order to first care for the living – given the time constraints and the challenges that large- scale humanitarian emergencies present. This negatively impacts the dignified management of the dead and contributes to them becoming missing persons. » « L'un des sujets les plus difficiles reste l'absence fréquente de spécialistes en médecine légale sur le terrain dans les situations d'urgence humanitaire, en raison de l'absence, la plupart du temps, d'un "cluster" chargé de la gestion des morts dans les services d'urgence nationaux et locaux. Les professionnels du "cluster" santé qui n'ont pas d'expérience dans la gestion des morts sont souvent mobilisés à la place, tandis que l'expertise médico-légale reste le plus souvent absente des plans d'urgence nationaux. La pénurie de spécialistes en médecine légale peut être due à l'absence de capacités suffisantes, notamment de formation spécialisée et de ressources nécessaires, observée dans certaines institutions médico-légales et policières nationales. En outre, dans certains contextes humanitaires, il peut y avoir une réticence à s'occuper des morts - afin de s'occuper d'abord des vivants - étant donné les contraintes de temps et les défis que posent les urgences humanitaires à grande échelle. Cela a un impact négatif sur la gestion digne des morts et contribue à ce qu'ils deviennent des personnes disparues ». "the development of guiding principles for the proper management of the dead in humanitarian emergencies and help in preventing their becoming missing persons: First Expert's Meeting", *International Review of the Red Cross*, 2019, 101 ( 912), p.1213-1229 https://international-review.icrc.org/sites/default/files/pdf/1602948923/IRC101_3b/S1816383120000223a.pdf

[1924] MOON, Claire, "Extraordinary death work: New developments in, and the social significance of, forensic humanitarian action", in PARRA, Roberto C, ZAPICO, Sara C., UBELAKER, Douglas H. (eds.), *Humanitarian Forensic Science: Interacting with the Dead and the Living*, Chichester: John Wiley and Sons, 2020,p.37-48

de services de base. »[1925] Différents membres du CICR ont cherché à définir en quoi pourrait consister la médecine légale humanitaire. Pour Stephen Cordner et Morris Tidball Binz, cette dernière consiste tout simplement en « l'application des connaissances et des compétences de la médecine et des sciences médico-légales à l'action humanitaire, notamment à la suite de conflits ou de catastrophes. » [1926]

Parallèlement à ce travail de mise à l'agenda, le mouvement d'institutionnalisation se poursuit, notamment lors du Tsunami touchant l'Asie du Sud-est de décembre 2004. Et en 2010, le service forensique du CICR commence à progressivement se consacrer à la recherche de migrants disparus. Traditionnellement, le mandat du CICR est centré sur l'assistance dans les zones de conflit. L'assistance aux migrants a été progressivement mise à l'agenda de l'organisation au tournant des années 2000, jusqu'à devenir une « priorité stratégique » en 2015[1927]. Ainsi, le CICR dispose d'une délégation en Grèce, qui apporte du soutien aux unités de médecine légale locales. L'organisation a aussi coopéré avec les autorités italiennes pour identifier les migrants morts lors d'un naufrage sur les côtes libyennes, en 2015. Le CICR appuie également les autorités espagnoles et la Croix rouge espagnole, pour l'identification des personnes mortes dans la zone des îles Canaries. Il est en outre présent en Amérique latine, notamment pour soutenir l'identification des morts à la frontière Mexico-Américaine. Et en fin de compte, la médecine légale humanitaire aurait fini d'après Claire Moon par aboutir à une relative institutionnalisation. Cette dernière se traduit par la multiplication des publications[1928], de guides, de standards[1929] et par l'ouverture en 2018 d'un institut de recherche en médecine légale humanitaire en Inde[1930]. Et en 2018, un réseau d'échange sur la médecine légale et l'identification des disparus est créé, le « Missing persons project ». Cela dit, il faut garder à l'esprit qu'on aurait affaire à une institutionnalisation partielle, du moins d'après nos enquêtés, lesquels nous ont fait comprendre que la place de la médecine légale n'était pas encore tout à fait stabilisée au sein du CICR : cette dernière a fait son entrée au

[1925] «The management of the dead is a core component of the response to humanitarian emergencies, together with the search for, recovery, and care of survivors and the supply of basic services. » TIDBALL-BINZ, Morris, "Managing the dead in catastrophes: guiding principles and practical recommendations for the first responders", *International review of the red cross*, Volume 89, number 866, June 2007

[1926] « the application of the knowledge and skills of forensic medicine and science to humanitarian action, especially following conflicts or disaster. » CORDNER, S., TIDBALL-BINZ, M., "Humanitarian forensic action – Its origins and future", *Forensic Science International*, 2017, vol.279, p. 65–71

[1927] BRADLEY, Myriam, "A humanitarian agency in global migration governance: the International Committee of the Red Cross's migration policy and practice", In, PECOUD, Antoine (ed.), *Research Handbook on the Institutions of Global Migration Governance*. Cheltenham, UK : Edward Elgar Publishing, 2023,p.89-101

[1928] Un numéro « spécial » de la revue du CICR sur le « traitement digne des morts » est prévu pour automne 2025. https://international-review.icrc.org/call-for-papers-protection-of-the-dead

[1929]CORDNER, Stephen, MCKELVIE, Helen, "Developing standards in international forensic work to identify missing persons", *RICR* 2002, vol.84, n°848, p.867-884 https://www.icrc.org/en/doc/assets/files/other/irrc_848_cordner.pdf
CICR, "Le processus d'identification forensique : une approche intégrée", 2022 https://www.icrc.org/fr/publication/4590-forensic-human-identification-process-integrated-approach

[1930] ICRC, "World's first International Centre for humanitarian forensics launched in India", International Committee of the red Cross, 21/06/2018
https://www.icrc.org/en/document/worlds-first-international-centre-humanitarian-forensics-launched-india

sein de l'organisation qu'en 2003, alors que le programme de RFL date du début du XXe siècle[1931].

En outre, les experts en médecine légale du CICR ne sont pas toujours directement impliqués dans des enquêtes médicolégales. Le premier objectif des services forensiques du CICR est de soutenir les initiatives d'organisation, de favoriser la coopération entre les acteurs, entre ONG et institutions, et de créer des groupes de réflexion afin d'élaborer et de promouvoir des standards[1932]. Il est important de préciser que le CICR joue un rôle central dans le travail des morts, mais qu'il est aussi en grande partie relayé par différents réseaux d'ONG et de collectifs de familles. Toute la difficulté du sujet est liée à la multiplicité de régimes de vérité, de méthodologies de recherche, et en fin de compte des données traitées pour identifier un mort. Bien souvent, c'est la société civile qui se charge d'un travail d'identification délaissé par les gouvernements[1933], alors qu'en théorie, le « travail des morts » est normalement le fait des États. Dans le cas de décès à l'étranger, c'est au relais diplomatique de suivre les différents processus de prise en charge de la personne décédée[1934]. Des spécialistes en droit international rappellent qu'en cas de disparition ou de corps non identifié, il est dans leur responsabilité de se consacrer au travail d'enquête[1935]. Il implique également le réseau

[1931] Cela dit, le programme RFL lui-même n'a pas toujours occupé une place centrale au sein du CICR, et à connu une crise au tournant des années 2000 et a dû se « réinventer » pour gagner une nouvelle légitimité, ce qui s'est traduit notamment par une refonte de ses standards et une centralisation de son système d'information, ainsi qu'une numérisation progressive de ce dernier. « Les activités de RLF n'étaient pas considérées comme essentielles à la réponse humanitaire du CICR et la plupart des sociétés nationales ne disposaient pas de capacités suffisantes pour traiter la question, et n'avaient que peu ou pas de contacts réguliers avec d'autres membres du Mouvement en ce qui concerne les activités de RLF - et ne prenaient pas part aux discussions stratégiques. Les activités de RLF n'avaient pas une grande importance et n'étaient pas considérées comme une priorité lors des discussions sur le management et les opérations de l'organisation (et l'établissement du budget). ""RFL was not seen as central to the humanitarian response of the ICRC and most national society had inadequate capacity to handle the issue, and little or no regular contact regarding RFL with others part of the Movement - and did not take part of strategic discussion. RFL had low status and was not seen as a priority when management and operations were considered (and budgeted). " SANDVIK, Kristin, *Humanitarian extractivism*, Manchester UNiversity Press, 2023, p.48.

[1932] TIDBALL-BINZ, Morris, HOFMEISTER, Ute, "Forensic archaeology in humanitarian contexts: ICRC action and recommendations", GROEN, Mike, MARQUEZ-GRANT, Nicholas, JANAWAY, Robert (ed.), *Forensic archaeology : a global perspective*, John Wiley & Sons, 2015,p. 427-437

[1933] REINEKE, R. C. "Forensic citizenship among families of missing migrants along the U.S.-Mexico border", *Citizenship Studies*, 2022, *26*(1),p. 21–37. https://doi.org/10.1080/13621025.2021.2018675

Il existe toute une nébuleuse d'organisations dédiées aux disparus et à l'identification des morts. Sans exhaustivité, citons **:** Le Collectif d'Annaba des familles harraga ;Missing at the Borders ; association marocaine des droits humains (AMDH) — Section Nador **;** Association La Terre pour Tous ; Caminando Fronteras **;** Carovane Migranti, Forensic Migrants initiative, etc. A Calais, il faut mentionner le « groupe décès » qui inclut Utopia 56, Médecins Du Monde, le Secours Catholique, l'Auberge des migrants.

BOURGERY, François-Damien, « Reportage : à Calais, des associations rendent leur identité aux migrants décédés », *InfoMigrant*, 23/11/2020 https://www.infomigrants.net/fr/post/28657/reportage--a-calais-des-associations-rendent-leur-identite-aux-migrants-decedes

[1934] https://www.diplomatie.gouv.fr/fr/conseils-aux-voyageurs/informations-pratiques/assistance-aux-francais/deces-a-l-etranger/

[1935]"Under IHRL, states can be held responsible for the interference with the right to life, human dignity, the prohibition of torture, cruel, inhuman, or degrading treatment or punishment, the prohibition of enforced disappearance, the right to private and family life. Notably, the procedural obligation of public authorities to carry out an effective investigation into the circumstances of unlawful or suspicious deaths within the jurisdiction of a State as well as the right to an effective remedy for violations of human rights law can serve to clarify the fate and whereabouts of missing persons. Rules related to the search for and identification of missing migrants may also be found in the international law of the sea, notably the obligation to assist and rescue persons in distress at sea, and in international criminal law . Furthermore, for instance, international disaster response law also contains relevant soft law instruments related to forensic activities and the management of the dead." ICRC, "Counting the dead, how registered deaths of migrants in the southern European sea border provide only a glimpse of the issue", November 2020 https://missingpersons.icrc.org/sites/default/files/2022-11/COUNTING-THE-DEAD-FINAL.pdf

"En vertu de la LIDH, les États peuvent être tenus pour responsables des atteintes au droit à la vie, à la dignité humaine, à l'interdiction de la torture et des peines ou traitements cruels, inhumains ou dégradants, à l'interdiction des disparitions forcées et au droit à la vie privée et familiale. Notamment, l'obligation procédurale des autorités publiques de mener une enquête effective sur les circonstances des décès illégaux ou suspects dans la juridiction d'un État, ainsi que le droit à un recours effectif pour les violations du droit des droits de l'homme peuvent servir à clarifier le sort des personnes disparues et le lieu où elles se trouvent. Les règles relatives à la recherche et à l'identification des migrants disparus figurent également dans le droit international de la mer, notamment l'obligation d'assister et de secourir les personnes

diplomatique ou des organisations intergouvernementales comme Interpol [1936] qui à l'initiative des gouvernements peuvent émettre des notices jaunes (personnes disparues)[1937] ou noires (corps non identifiés). Le CICR travaille avec l'accord des États. Il arrive aussi qu'il appuie et coordonne le travail de gestion des morts effectué par les gouvernements. Cela dit, dans le cadre des morts aux frontières, la plupart des analystes font le constat d'un grave déficit d'engagement de ces acteurs. Leur manque de volonté politique sur ce sujet s'inscrit évidemment dans une action plus large de répression des exilés par les États[1938].

En réaction à l'inaction des États, certaines ONG se sont emparées du sujet, notamment le CICR qui a développé une certaine expertise. On peut commencer par décrire sa méthodologie de recherche pour avoir une idée plus précise du travail d'enquête et des données nécessaires pour identifier un mort. Pour commencer, il faut garder à l'esprit que la frontière entre les disparus et les morts est poreuse. Tant qu'on n'a pas retrouvé un corps, la disparition peut être envisagée. On peut toujours dire que les « disparus » désignent le processus, alors que la mort est l'aboutissement fatal d'un parcours. La définition du CICR des personnes disparues est donc la suivante : « les personnes dont la famille est sans nouvelles, et/ou qui, selon des informations fiables, ont été rapportées comme disparues en raison d'un conflit armé, international ou non international, ou d'une situation de violence interne, de troubles

---

en détresse en mer, et dans le droit pénal international. En outre, par exemple, le droit international relatif aux interventions en cas de catastrophe contient également des instruments non contraignants relatifs aux activités médico-légales et à la gestion des morts. »
GRANT, Stefanie, "Dead and Missing migrants : the obligations of European states under international human rights law", IOM, September 2016
https://missingmigrants.iom.int/sites/g/files/tmzbdl601/files/publication/file/Mediterranean-Missing-Legal-Memo-290816.pdf
Last Rights, "The Dead, the Missing and the Bereaved at Europe's International Borders Proposal for a Statement of the International legal obligations of States", May 2017
https://www.ohchr.org/sites/default/files/Documents/Issues/Migration/36_42/TheLastRightsProject.pdf
Council of Europe,"For the rights of the living, for the dignity of the dead – Time to end the plight of missing migrants in Europe", 29/09/2022
https://www.coe.int/ro/web/commissioner/-/for-the-rights-of-the-living-for-the-dignity-of-the-dead-time-to-end-the-plight-of-missing-migrants-in-europe
Ajoutons que l'objectif 8 du Pacte mondial des migrations (droit mou non contraignant) porte sur l'identification des morts en migration. Il stipule qu'il est nécessaire de « Mettre tout en œuvre, y compris par le biais de la coopération internationale, pour retrouver, identifier et rapatrier les dépouilles des migrants décédés dans leur pays d'origine, en respectant les souhaits des familles endeuillées, et, dans le cas de personnes non identifiées, faciliter l'identification et la récupération ultérieure des dépouilles mortelles, en veillant à ce que les dépouilles des migrants décédés soient traitées d'une manière digne, respectueuse et appropriée. »
https://refugeesmigrants.un.org/sites/default/files/180713_agreed_outcome_global_compact_for_migration.pdf
ANGELI, Danai, "The dead, the missing and the bereaved : Is objective 8 still a priority?", 19/05/2021
https://rli.blogs.sas.ac.uk/2021/05/19/the-dead-the-missing-and-the-bereaved-is-objective-8-still-a-priority/
BOLTON, Syd, JARVIS, Catriona, "GCM Commentary : Objective 8 : Save lives and establish coordinated international efforts on missing migrants", 18/10/2018,https://rli.sas.ac.uk/blog/gcm-commentary-objective-8-save-lives-and-establish-coordinated-international-efforts-missing
STEPPUTAT, F, *Governing the Dead: Sovereignty and the Politics of Dead Bodies*, Manchester: Manchester University Press, 2014, 272 p.

[1936] Interpol a une unité dédiée à l'identification des morts après une catastrophe, de petite ou de moyenne ampleur. Il participe à la standardisation de methodologies d'identification (ses formulaires sur l'identification des victimes de catastrophe (IVC) font référence) et il peut appuyer les États manquant de capacité en médecine légale lors de catastrophes naturelles, ou causées par des humains. A la demande de gouvernement, et pour appuyer des enquêtes à l'international, Il peut également émettre des notices jaunes (disparus) et noires (corps non identifié). Il peut travailler en coordination avec des organisations humanitaires comme le CICR. Sa méthodologie d'enquête est mobilisée dans le cadre d'enquête judiciaire et si elle a pu être réutilisée dans le cadre de crise humanitaire, cette dernière n'est pas toujours adaptée. https://www.interpol.int/fr/Notre-action/Police-scientifique/Identification-des-victimes-de-catastrophes-IVC

[1937] https://www.interpol.int/How-we-work/Notices/Yellow-Notices

[1938] « Selon les normes diplomatiques, en cas de décès d'un étranger dûment constaté par la police, l'État dans lequel le décès est constaté prend contact avec le consulat du pays d'origine du défunt. En l'absence d'une pièce d'identité, la police utilise les indices de présomption à sa disposition pour contacter l'État concerné. Par la suite, c'est au consulat de joindre la famille pour l'aviser du décès et la conseiller pour les formalités administratives et légales de rapatriement ou d'inhumation. Dans l'hypothèse où l'État marocain ne dispose pas d'indices de présomption, il contacte en premier lieu des acteurs associatifs et se décharge ainsi de la procédure de traçabilité du corps sur des acteurs privés. » DIALLO, Alimou, « Politique de l'inanimé : un dispositif informel d'identification des « corps sans vie et sans papiers » au Maroc », *Politique africaine*, 2018/4 (n° 152), p. 141-163. https://www.cairn.info/revue-politique-africaine-2018-4-page-141.htm

intérieurs, ou encore de toute autre situation qui puisse requérir l'intervention d'une institution neutre et indépendante. Le terme de personnes disparues renvoie à des personnes pouvant être vivantes ou mortes. »[1939]

Il se trouve que le CICR a mis au point une méthodologie d'enquête visant à retrouver les disparus et à permettre aux familles de renouer avec leurs proches perdus de vue. Ce type d'action fait partie du mandat historique de l'organisation et a été baptisé « rétablissement des liens familiaux » (RFL).

Mais malgré la porosité entre les deux catégories, il est important de noter que les méthodologies d'enquête relatives aux morts et aux disparus ne sont pas les mêmes. Concernant les « missing », dans la logique du RFL une recherche est lancée uniquement à l'initiative des familles. La Croix-Rouge ne sollicite pas ces dernières si elles n'en font pas la demande[1940]. On ne peut pas imposer un travail de deuil, comme nous l'ont dit des enquêtés[1941]. En cas de disparition, c'est donc à une famille de contacter une délégation du CICR ou une antenne de la Croix-Rouge locale afin d'établir une « requête d'investigation » (« tracing request » en anglais). L'agence humanitaire mène alors un entretien avec la famille puis lance l'enquête. Pour ce faire, le CICR va croiser les informations collectées avec les données qu'elle possède déjà (des listes de personnes détenues, des listes de personnes enregistrées comme recevant ou ayant reçu des soins hospitaliers, des listes de personnes décédées)[1942]. Parallèlement, il est proposé de publier et/ou consulter une base de données, le « face Tracking system ». Créée en 2013, dans la foulée de la stratégie de refondation du service RFL, la base de donnée comprend les photos des personnes recherchant leur proche. La base photographique peut en outre être l'objet de requêtes selon les mots clefs suivants : genre/âge/pays d'origine, elle ne comprend donc pas de données nominatives. Les photographies d'enfants de moins de 15 ans sont conservées hors ligne, et peuvent

[1939] MSF, « Personnes disparues et les morts », *Dictionnaire pratique du droit humanitaire* https://dictionnaire-droit-humanitaire.org/content/article/2/personnes-disparues-et-les-morts/

[1940] A contrario, l'initiative d'envoyer des photographies de soldats russes décédés aux familles autorités ukrainiennes a été très critiquée. L'objectif était de tenter d'insuffler du ressentiment dans la société russe et de la contestation envers ce qui est nommé officiellement « opération spéciale ». Cette initiative contrevient à différentes règles du DIH, d'autant que l'identification des soldats s'est fait en partie grâce à Clearview, un logiciel décrié pour son fonctionnement très intrusif. « Ni le texte des Conventions de Genève, ni les commentaires y afférents, ni la pratique des Etats ne mentionnent qu'une partie à un conflit armé devrait tendre la main aux parents des personnes décédées ou leur envoyer des photos de leurs cadavres. À l'inverse, les commentaires suggèrent plutôt qu'il incombe au Bureau national d'information ou à l'Agence centrale de recherche de transmettre les informations pertinentes sur le lieu où se trouvent les soldats décédés à leurs parents les plus proches. » "Neither the text of the Geneva Conventions, nor the commentaries thereto, nor relevant state practice mention that any party to an armed conflict should reach out to the relatives of dead persons or send them pictures of their corpses. Conversely, the commentaries much rather suggest that it is the responsibility of the National Information Bureau or the Central Tracing Agency to transmit the relevant information about the whereabouts of deceased soldiers to their next of kin" GRAF, Jan-Philip, NEUMANN, Jannik, "Between accuracy and dignity, legal implication of facial recognition for dead combatants", *Volkerrechtsblog*, 30/09/2022 https://voelkerrechtsblog.org/between-accuracy-and-dignity/

[1941] Entretien n°35, OI2, 14/05/2020

[1942] "Q&A: The ICRC's engagement on the missing and their families", *International review of the Red cross*, 2017, 99 (2), p.535-545 https://international-review.icrc.org/sites/default/files/irrc_99_905_5.pdf

CRETTOL, Monique, MILNER, Lina, LA ROSA, Anne-Marie, STOCKWELL, Jill, "Establishing mechanism to clarify the fate and whereabouts of missing persons: a proposed humanitarian approach, " *International review of the red cross*, 99 (2), p.589-618 https://international-review.icrc.org/sites/default/files/irrc_99_905_8.pdf

simplement être consultées par les officiels de l'ICRC. Les photographies sont stockées sur une base de données interne, non pas sur un cloud public, par mesure de sécurité[1943].

## §2 — Les morts en migration

Concernant les enquêtes sur les disparus dans le cas de morts en migration, le procédé diffère. Mais l'objectif est toujours de comparer les témoignages des familles avec les données collectées sur les corps (procéder à un recoupement des données ante-mortem, post mortem). Ce procédé s'appuie sur une méthodologie de médecine légale spécifique, formalisée notamment par Interpol, fruit de son expérience acquise en matière d'enquête lors de catastrophes. Mais elle n'est pas adaptée à toutes les crises, et c'est le cas des morts en migration. En effet, deux points font obstacle à l'identification d'un mort :

- Les familles ne font pas de demandes d'enquête (elles peuvent ignorer que leur proche a disparu). Dans ce cas, il est nécessaire d'effectuer ce qui est qualifié de « reverse tracing », de traçage inversé. Cela signifie partir du corps pour retrouver les familles qui pourront alors participer au processus d'identification. Cela représente donc un changement de méthode qui ne va pas de soi au sein du mouvement de la Croix-Rouge.

- La plupart des corps des migrants ne sont pas retrouvés[1944].

Or, on s'intéresse pour notre part à ce dernier cas. Et enquêter sur des morts en exil complexifie largement le modèle théorique qu'on a évoqué. Dans ce type de situation, les familles ne font pas toujours la démarche de lancement de procédure de recherche. Tout d'abord, il faut reconnaitre l'existence d'une disparition. Les familles peuvent ne pas être informées du décès d'un de leurs membres, ou bien le savoir via des canaux informels, mais être dans le déni (la dimension psychologique est ici importante). Ou bien, elles peuvent le savoir, mais ne pas savoir à qui s'adresser. Ou bien, elles peuvent le savoir, mais ne pas avoir envie de contacter les institutions, que ce soit le CICR ou les ambassades. Enfin, les ONG peuvent perdre la trace des familles. Elles peuvent demander l'identification d'un corps à une ONG sur place, mais elles ne restent pas sur place à attendre que l'identification soit faite. Il arrive qu'elles ne soient plus joignables (en raison d'un changement de numéro de téléphone par exemple). Les ONG peuvent alors se retrouver avec un corps identifié, mais sans pouvoir joindre la famille[1945]. Et il ne faut pas oublier que la plupart des cas de disparitions ne

[1943] BOLLAG, Burton, "Help me find my family", *Devex*, 02/05/218https://www.devex.com/news/help-me-find-my-family-92470
[1944] CICR, » le processus d'identification forensique », 2020https://www.icrc.org/fr/publication/4154-forensic-identification-human-remains
CICR, « Le processus d'identification forensique : une approche intégrée », 2022 https://www.icrc.org/fr/publication/4590-forensic-human-identification-process-integrated-approach
[1945] Entretien n°10, identification des morts n°5, 10/04/2020

déclenchent pas de processus d'enquête, les corps n'étant pas retrouvés. Ils restent oubliés au fond de la mer Méditerranée.

Le fichage des vivants contraste donc avec l'anonymat des migrants morts sur les routes migratoires. Ce sont des corps oubliés et anonymes, des morts clandestines dans des lieux périphériques, de corps frappés par une « invisibilité radicale » comme l'écrit Evelyne Ritaine.[1946] L'invisibilité de leur mort résulte également d'une absence de décompte officiel à l'échelle européenne, pour Charles Heller et Antoine Pécoud : « les États ne voient que ce qu'ils « chiffrent » (…). En négligeant de recenser les morts aux frontières, les États condamnent ces morts à l'invisibilité. »[1947]

D'où la volonté de rendre ces morts plus « visibles »[1948]. Ainsi des cartes permettant de se représenter plus directement le phénomène des morts en mer Méditerranée ont été publiées à partir du début des années 2000. La plus célèbre est celle d'Olivier Clochard, intitulée « Mourir aux portes de l'Europe ». Compter les disparus peut être un instrument d'interpellation[1949]. Mais établir une comptabilité précise de ces morts reste délicat et difficile, du fait d'un grand nombre de disparus, et de différentes méthodes statistiques. Il n'y a effectivement pas de définition commune du terme « morts aux frontières ». Dans cette catégorie peuvent être inclus ou non des décès dus aux noyades, aux suicides, aux disparitions forcées[1950]. Il n'y a également pas d'accord sur la zone géographique à prendre en compte.

Donc, le projet « borderdeath » a comptabilisé — entre 1990 et 2013 - 3 188 morts retrouvés par des autorités locales en Grèce, Espagne, Italie, et à Gibraltar et à Malte[1951].

En juin 2023, l'organisation « United for intercultural action » estime que, toute cause de décès confondue,-plus de 52 760 migrants sont morts depuis 1993[1952].

---

[1946] RITAINE, Évelyne, « Migrants morts, des fantômes en Méditerranée », *Rhizome*, 2017/2 (N° 64), p. 16-17. https://www.cairn.info/revue-rhizome-2017-2-page-16.htm

[1947] HELLER, Charles, PECOUD, Antoine, « Compter les morts aux frontières : des contre-statistiques de la société civile à la récupération (inter)gouvernementale », *Revue européenne des migrations internationales*, vol. 33 - n°2 et 3 | 2017, http://journals.openedition.org/remi/8732

[1948] SQUIRE, Vicki, *Europe's Migration Crisis, border deaths and human dignity*, Cambridge university press, 2020, 280 p.

[1949] TAZZIOLI, M.,"The politics of counting and the scene of rescue. Border deaths in the Mediterranean », *Radical Philosophy*,n° 92, July/Aug 2015, p. 2–6.

HELLER, Charles, PECOUD, Antoine « Compter les morts aux frontières : des contre-statistiques de la société civile à la récupération (inter)gouvernementale », *Revue européenne des migrations internationales*, vol. 33 — n° 2 et 3, 2017, http://journals.openedition.org/remi/8732

DIAZ, Paola Diaz, NICOLOSI, Guido, « Corps, identités et technologies "par les nombres" dans l'imaginaire migratoire », *Socio-anthropologie*, 40, 2019, https://doi.org/10.4000/socio-anthropologie.5577

[1950] LUTHER,Ben, ELENGA, Touere, « La disparition forcée des migrants : une question de droit international. », *La Revue des droits de l'homme* 18 | 2020, URL : http://journals.openedition.org/revdh/9962

[1951] http://www.borderdeaths.org/

LAST, Tamara,SPIJKERBOER, Thomas, ULUSOY, Orcun, "Deaths at the Borders: Evidence from the Southern External Borders of the EU." *Revue Hijra*, 2016, p. 5–23

http://www.borderdeaths.org/wp-content/uploads/Preliminary-Findings.pdf

[1952]https://unitedagainstrefugeedeaths.eu/wp-content/uploads/2014/06/ListofDeathsActual.pdf

En mars 2020, l'OIM estime le nombre de morts en mer Méditerranée à 20 000 environ depuis 2014[1953]. Et le sujet des morts en migration est toujours d'actualité en 2024[1954]. On peut sur ce sujet se référer au graphique qui suit constitué à partir des statistiques du Missing Project de l'OIM.


Le CICR précise que les corps retrouvés (sans être nécessairement identifiés) représentent une minorité de l'ensemble de l'estimation du nombre de morts : « les restes des migrants décédés dans les trois pays (y compris les cas encore inconnus de l'épave de Catane/Melilli) représentent environ 13 % des plus de 20 000 migrants disparus/décédés signalés par l'Organisation internationale pour les migrations au cours de la même période. »[1955]

Et surtout, au-delà de ce travail statistique, des personnes tentent de rendre un nom à ces morts, pour leur rendre une forme de dignité post-mortem et restaurer leur appartenance à une communauté[1956]. Ce travail d'identification dépend bien souvent d'initiatives ponctuelles, des proches, mais aussi des professionnels travaillant plus ou moins directement en lien avec les morts, que ce soient des légistes, des garde-côtes, des pêcheurs. De façon générale, leur engagement serait caractérisé par un manque de coordination : « *Notre principale recommandation est la création de mécanismes nationaux qui seraient l'autorité responsable*

---

[1953] ONU Info, « La barre des 20 000 migrants morts en Méditerranée franchie après un naufrage au large de la Libye »,06/03/2020 https://news.un.org/fr/story/2020/03/1063431

[1954]JULLIEN, Dorian, « Naufrage en Méditerranée : plus de 2000 hommes, femmes et enfants sont morts ou disparus depuis le début de l'année. Le bilan de 2022 est déjà dépassé », *Le Monde*, 16/08/2023 https://www.lemonde.fr/les-decodeurs/article/2023/08/10/naufrages-en-mediterranee-avec-plus-de-2-000-morts-depuis-le-debut-de-l-annee-le-bilan-de-2022-est-deja-depasse_6185020_4355770.html
« Plus de 2500 hommes, femmes et enfants sont morts ou disparus en Méditerranée en 2023, selon l'ONU », *le Monde avec AFP*, 29/09/2023 https://www.lemonde.fr/afrique/article/2023/09/29/plus-de-2-500-migrants-morts-ou-disparus-en-mediterranee-depuis-le-debut-de-l-annee-selon-l-onu_6191504_3212.html

[1955]« According to the study, for six years, the remains of deceased migrants in the three countries (including the yet unknown total caseload of the Catania/Mellili shipwreck), represent around 13% of the over 20,000 missing/deceased migrants reported by the International Organization for Migration during the same period. » ICRC, "Counting the dead, how registered deaths of migrants in the southern European sea border provide only a glimpse of the issue", November 2020 https://missingpersons.icrc.org/sites/default/files/2022-11/COUNTING-THE-DEAD-FINAL.pdf

[1956] Tribune, collectif, "Migration : "inscrivons l'obligation d'identification des défunts anonymes dans le droit européen", *Le Monde*, 30/08/2023https://www.lemonde.fr/idees/article/2023/08/30/migration-inscrivons-l-obligation-d-identification-des-defunts-anonymes-dans-le-droit-europeen_6187087_3232.html
M'CHAREK, Amade, BLACK, Julia," Engaging Bodies as Matters of Care Counting and Accounting for Death During Migration", in , CUTTITTA, Paolo, LAST, Tamara (eds.) , *Border Deaths, Causes, Dynamics and Consequences of Migration-related Mortality,* Amsterdam University Press,2020, 174 p.
M'CHAREK, A., CASARTELLI, S., "Identifying dead migrants: forensic care work and relational citizenship", *Citizenship Studies*, 2019, 23(7), p.738-757. https://doi.org/10.1080/13621025.2019.1651102

*ou chef de file de la coordination d'une grande partie de ce travail. Pour l'instant, c'est beaucoup… c'est beaucoup trop fragmenté.* »[1957] Toute la difficulté du sujet est liée à la multiplicité de régimes de vérité, de méthodologie de recherche, et en fin de compte de données traitées pour identifier un mort. En outre, les morts sont pris en charge dans différents pays méditerranéens comme l'Italie, l'Espagne, la Grèce, la Tunisie, ou le Maroc. Et ces pays comportent une grande variété de cadres juridiques, d'acteurs impliqués et de tradition d'identification médico-légale. Ils ont cependant un point commun : un manque de moyens et d'application des procédures et des standards existants, ainsi qu'un manque plus généralisé de volonté politique de se consacrer à l'identification des morts. Le faible taux d'identification est aussi résultant d'un manque structurel d'investissement quant à cette question, faisant de la mer Méditerranée une zone de mort et une politique de destruction des identités [1958] . Les disparus en mer Méditerranée sont la conséquence d'une nécropolitique, pour citer cette notion forgée par Achille Mbembe[1959].

Il n'existe que peu d'exemples de mobilisations coordonnées établies à l'appel des autorités. En Grèce, il a fallu attendre un naufrage en juin 2023 ayant entrainé la mort d'environ 600 victimes[1960]. En Italie, ce ne sont que deux naufrages qui ont fait l'objet d'une enquête impliquant directement l'État, en 2013 et 2015, ce dernier drame ayant causé jusqu'à 800 morts.

## § 3 — L'identification des exilés morts en migration, le cas italien

En guise d'exemple, on peut évoquer le cas italien. Dans ce pays, la plupart du temps, le travail d'enquête à la suite d'un naufrage où sont victimes des exilés est minime. En Italie, le procureur ne déclenche en effet d'autopsie complète qu'en cas de soupçon de crime. S'il y a une enquête, elle serait bien fréquemment motivée par un objectif sécuritaire [1961]. Une enquêtée nous confie qu'« *En Italie, il n'y a pas d'obligation d'identifier un migrant, ce n'est une obligation que si quelqu'un le demande. Ainsi, l'identification d'un mort à la frontière est essentiellement un effet secondaire de l'enquête. Les procureurs ou les garde-côtes ne*

[1957] « Our primary recommendation is the creation of national mechanisms to be the responsible or lead authority coordinating a lot of this work. For the moment it is far… it is far too fragmented » Entretienn°24, identification des morts n°3, 20/03/2020

[1958]ANSTETT, Elisabeth, DREYFUS (ed.), Jean-Marc,*Destruction and human remains, disposal and concealment in genocide and mass violence*, Manchester University Press,2014, 263 p.

[1959] MBEMBE Achille, « Nécropolitique », *Raisons politiques*, 2006/1 (nº 21), p. 29-60. https://www.cairn.info/revue-raisons-politiques-2006-1-page-29.htm])

[1960] « Pour la première fois dans le cadre de la réponse à un naufrage, les autorités grecques ont activé le Protocole d'identification des victimes de catastrophes (IVC) afin d'identifier les victimes grâce à la coopération de la police grecque, du ministère des Migrations et de l'Asile, du Comité international de la Croix-Rouge (CICR), de la Commission internationale pour les personnes disparues et des pays d'origine. » "Grèce : 6 mois après le naufrage de Pylos, la justice n'a toujours pas été rendue", Human Right Watch, 14/12/2023 https://www.hrw.org/fr/news/2023/12/14/grece-6-mois-apres-le-naufrage-de-pylos-la-justice-na-toujours-pas-ete-rendue

[1961] ATTIA, Ben, et al. »Missing Migrants: Management of Dead Bodies in Sicily. Mediterranean Missing", OIM, 2016 https://missingmigrants.iom.int/sites/g/files/tmzbdl601/files/publication/file/Mediterranean-Missing-Italy-report-long.pdf

*s'occupent pas de l'identification, ils se moquent de savoir s'il s'agit d'un numéro ou d'un nom, leur seul objectif étant d'enquêter pour trouver les passeurs*. »[1962]

Ainsi, des données qui pourraient servir à identifier le corps ne sont pas recueillies systématiquement. Mais cela n'empêche pas qu'une fois l'examen (sommaire) du corps complété, le docteur édite un certificat de décès. Le procureur publie alors ensuite une autorisation d'inhumer et ces documents sont transmis au registre civil des municipalités de la ville où le corps a été retrouvé. Notons que le corps peut être transféré si le cimetière local ne dispose pas de place. Et surtout, ce transfert peut ne pas être documenté. Il n'y a pas de traçabilité des corps, comme l'a démontré l'anthropologue Giorgia Mirto[1963]. En somme, d'après Filippo Furri et Carolina Kobelinsky, le système juridico- médico-administratif est pensé pour une gestion quotidienne des décès des autochtones et locaux. Et aucune institution n'a pour objectif l'identification des « morts qui viennent d'ailleurs »[1964].

Toutefois, en réaction à cette situation, quelques acteurs ont cherché à pallier ce manque. Une première initiative a mobilisé la Croix-Rouge de Catane[1965]. Elle a consisté en la création d'une base de données centralisant les informations sur les morts du cimetière de Catane[1966]. Une deuxième initiative a été impulsée par des acteurs venus de la médecine légale, et notamment le Labanof. Il s'agit d'un laboratoire médico-légal — situé à Milan. Il est composé de biologistes, de médecins légistes et d'anthropologues judiciaires, et il est doté d'une mission de recherche, d'enseignement et d'aide technique pour des identifications. Il est dirigé par Cristina Cattaneo, experte auprès de la justice italienne, et membre depuis 2014 d'un groupe de travail de médecine légale du CICR. Mais contrairement à la Croix-Rouge et à l'ICMP, le laboratoire n'est pas initialement voué à l'identification de victimes de conflits ou de crises humanitaires. Depuis 2011, le CICR collabore avec le Labanof, afin d'établir un protocole standardisé d'identification[1967]. Mais la collaboration entre l'ONG et le laboratoire s'est renforcée à la suite des naufrages survenus à Lampedusa en octobre 2013, et du naufrage dit du « barcone »[1968] en avril 2015. À la suite de ces deux naufrages, le Labanof a en effet été missionné pour examiner des dépouilles et recueillir des données identifiantes, et stocker les

[1962]"in Italy there is no duty to identify a migrant, it is anobligation only if someone is pushing for it. so the identification of a border death is mainly a side effect of invistagion. Procecutor or coast guard do not anything about identification, they dont care, if it is a number/ a name, their only objectif is to investigated to find smuggler." Entretien n°27, identification des morts n°4, 06/04/2020

[1963] MIRTO, Giorgia, "*Procedure di gestione delle vittime delle frontiere in Italia",* in CRUA, G., GILETTI, S., PRONO, F. (eds)*, Desaparecidos e migranti nel Mediterraneo e nelle Americhe*, Gruppo Editoriale Bonanno, Acireale-Roma, 2018.

[1964] KOBELINSKY, Carolina, FURRI, Filippo, *Relier les rives, sur les traces des morts en Méditerranée*, La Découverte, 2024, 200 p.

[1965] Catane se situe en Sicile, la ville a été, entre autre tragédies, marquée par un naufrage particulièrement dramatique ayant causé jusqu'à 800 morts. « Le naufrage en Méditerranée a fait 800 morts, selon le HCR », *le Monde avec AFP*, 21/04/2015 https://www.lemonde.fr/europe/article/2015/04/21/des-survivants-du-naufrage-en-mediterranee-sont-arrives-en-sicile-deux-arrestations_4619530_3214.html

[1966] FURRI, Filippo, KOBELINSKY, Carolina, « Les Autres morts. Gestion des corps et présence des morts de la migration dans la ville de Catane », dans BENEÏ, V. , TIJOUX, M. E. (éds.), Racismes, Corps, Attentes : Figures de la migration en contexte contemporain, *L'Harmattan*, 2021,288 p

[1967] OTTAVY, Eva, « Perdre sa vie, mais pas son nom », *Plein droit*, 2016/2 (n° 109), p. 15-18. https://www.cairn.info/revue-plein-droit-2016-2-page-15.htm

[1968] Le nom du chalutier Égyptien n'a pas été identifié, le mot « barcone » signifie la grande barque en italien. L'embarcation a été exposée en mai 2019 à la Biennale de Venise.

effets personnels des victimes du chalutier naufragé le 18 avril 2015, ainsi que des échantillons d'ADN[1969].

Dans le premier cas, pour le naufrage de 2013, le Procureur d'Agrigente a requis un examen externe (et non pas une autopsie complète) des corps, et un échantillonnage ADN. Cela a été fait avec l'équipe de médecine légale de la police scientifique. Dans le second cas, pour le naufrage de 2015 d'environ 800 victimes, le Procureur de Catane a tout d'abord décidé qu'il n'y avait pas assez de ressource pour lancer une enquête. Le cas était clos, et il n'y avait pas de besoin juridique d'identifier les victimes. Mais face au retentissement de ces drames, les autorités italiennes ont été incitées à lancer une investigation de plus vaste ampleur, et un protocole d'accord a été signé entre le Commissariat extraordinaire pour les personnes disparues[1970] du ministère de l'intérieur italien, le laboratoire d'anthropologie du Labanof (et notamment sa directrice, Cristina Cattenao), et le CICR.

On peut à ce stade donner une rapide description des protocoles fondés sur les techniques de médecine légale, notamment celui d'Interpol[1971]. Ils consistent à rapprocher des données collectées auprès des familles (données ante-mortem) avec des données collectées sur les corps (données post-mortem)[1972]. Or, lors de naufrages, la collecte de données ante-mortem n'est d'abord pas envisageable. C'est pour cela que Cristina Cattenao surligne l'importance des données secondaires dans ce type de situation. Les légistes peuvent se fonder sur d'autres données, recueillies par exemple à partir d'objets. Il peut s'agir de photos, de lettres, de billets, de papiers d'identité, parfois faux, de vêtements, de médicaments, de paquets de cigarettes où sont inscrits des numéros de téléphone, des bracelets, de brosses à dents. Tout ce qui maintient un semblant d'individualité aux corps anonymes. Cristina Cattenao déclare ainsi que : « même sans l'ADN, on peut arriver à identifier un individu… Oui, il y a cette dent cassée, cette ancienne fracture… Et il y a aussi les objets. Comme cette femme qui reconnaît son frère en voyant son propre numéro de téléphone inscrit sur une feuille qu'il avait dans sa poche

---

[1969]BERTOGLIO, Barbara, GRIGNANI, Pierangela, DI SIMONE, Paola, POLIZZI, Nicolò, DE ANGELIS, Danilo, CATTANEO, Cristina, IADICICCO, Agata, FATTORINI, Paolo, PRESCIUTTINI, Silvano, PREVIDERE, Carlo," Disaster victim identification by kinship analysis: the Lampedusa October 3rd, 2013 shipwreck", *Forensic Science International: Genetics*, Volume 44, 2020,https://doi.org/10.1016/j.fsigen.2019.102156.
CATTANEO, C., TIDBALL BINZ, M., PENADOS, L., PRIETO, J., FINEGAN, O., GRANDI, M., "The forgotten tragedy of unidentified dead in the Mediterranean", *Forensic Science International*, Volume 250, 2015, Pages e1-e2,
CATTANEO, C., DE ANGELIS, D., MAZZARELLI, D. et al. "The rights of migrants to the identification of their dead: an attempt at an identification strategy from Italy", *Int J Legal Med*, 137, 2023, p. 145–156https://doi.org/10.1007/s00414-022-02778-1 https://www.thelancet.com/journals/langlo/article/PIIS2214-109X(16)30106-1/fulltext
CATTANEO, Cristina, *Naufraghi senza volto: dare un nome alle vittime del Mediterraneo*, Raffaello Cortina Editore, 2018, 198 p.
M'CHAREK, A., CASARTELLI, S., « Identifying dead migrants: forensic care work and relational citizenship », *Citizenship Studies*, 2019, 23(7), p. 738-757. https://doi.org/10.1080/13621025.2019.1651102
TERVONEN, Taina, *Au pays des disparus*, Paris: Fayard, 2019, 256 p.

[1970] Commissariat inauguré en 2007 par le ministère des affaires Intérieures italien, la question des morts en migration n'est mise à l'agenda de l'organisation qu'à partir du naufrage de 2013. Mis à part ces deux naufrage, il ne recueillerait qu'une partie réduites des personnes disparues au large des côtes italiennes. KOBELINSKY, Carolina, FURRI, Filippo, *Relier les rives, sur les traces des morts en Méditerranée*, La Découverte, 2024, 194 p.

[1971]Disaster Victim Identification, Interpol https://www.interpol.int/How-we-work/Forensics/Disaster-Victim-Identification-DVI

[1972] Certains experts sont critiques sur l'usage de ces termes : « Par le passé, le terme ante-mortem s'appliquait à toutes les informations relatives aux personnes disparues, et le terme post-mortem à celles relatives aux restes humains non identifiés. Cependant, ces termes sont restrictifs et ne conviennent pas à tous les scénarios, ce qui signifie que leur usage générique n'est pas adapté à tous les cas de figure. En effet, toutes les personnes disparues ne sont pas mortes, et l'expression ante-mortem (« avant la mort ») n'est donc pas appropriée étant donné qu'elle peut sous-entendre le décès de l'individu, et ce sans aucune preuve. « CICR, « Le processus d'identification forensique : une approche intégrée », 2022 https://www.icrc.org/fr/publication/4590-forensic-human-identification-process-integrated-approach

quand il est mort. Les objets sont très importants. Ils nous aident à arriver au moins à établir une correspondance. Et ils nous ouvrent le monde de l'émotivité. Voir ce que ces adolescents ont dans leurs poches, leur bulletin scolaire, un petit sac contenant une poignée de terre de leur pays, c'est prendre un coup dans l'estomac. Tu t'identifies immédiatement. »[1973]

Cela dit, d'après des enquêtés, la méthodologie du Labanof, basée sur la médecine légale, reste fortement focalisée sur la collecte de données ADN. L'ADN est considéré comme la « reine des preuves », mais précisons que les données génétiques n'ont de valeur que dans les cas où l'on dispose également de l'ADN des familles. Afin de tenter de joindre des proches, des appels sont lancés aux ambassades et ONG (OIM, la Croix-Rouge italienne, le CICR, Amnesty International, Borderline Europe…). Pour le cas des naufrages de 2013, 66 familles de disparus, venant d'Allemagne, de Suisse, d'Italie, de Norvège, d'Angleterre, du Danemark et de France, ont pu faire le voyage jusqu'à Milan et Rome. Les familles ont pu fournir des informations permettant l'identification des corps [1974]. On leur a ensuite montré les photographies des morts, avec leur accord, pour une première identification, devant être confirmées par des méthodes scientifiques.

Ensuite, une dernière étape du processus d'identification consiste à tenter d'établir un rapprochement entre des données ante-mortem et post-mortem afin de procéder à l'identification des corps, en fonction de la correspondance des données. On peut lire dans un guide d'identification forensique le protocole suivant :

1) Identification : une correspondance complète entre les données génétiques, anthropologiques, odontologiques (concerne la dentition et les maxillaires), et des données médicales.

2) Correspondance des données biologiques : cela ne suffit pas pour identifier pleinement une personne disparue.

3) Correspondance d'objets : l'identification doit être confirmée par un examen des données anthropologiques, odontologiques et génétiques

4) Pas de correspondance : peut signifier qu'un recueil supplémentaire de données ante-mortem est nécessaire pour établir une identification.

5) Reconnaissance : les proches reconnaissent le disparu sur les photographies. Des examens supplémentaires doivent être mis en place.

---

[1973] BABY Sophie, NERARD François-Xavier, « Les objets des disparus. Exhumations et usages des traces matérielles de la violence de masse », *Les Cahiers Sirice*, 2017/2 (N° 19), p. 5-20. https://www.cairn.info/revue-les-cahiers-sirice-2017-2-page-5.htm
BARAYBAR, JP. » When DNA is not available, can we still identify people? Recommendations for best practice", *J. Forensic Sci.*, 2008 May, 53(3), p.533-40.

[1974] PISCITELLI, Vittorio (et alii.), "Italy's battle to identify dead migrants", *The Lancet*, Volume 4, Issue 8, 2016 https://www.thelancet.com/journals/langlo/article/PIIS2214-109X(16)30106-1/fulltext

6) Fausse reconnaissance : l'examen de données supplémentaire a établi qu'une première reconnaissance visuelle n'était pas bonne.

Toutefois, dans le cas des enquêtes portant sur les deux naufrages, le taux d'identification est très faible[1975]. Et la question de la généralisation de ce protocole est toujours d'actualité. En Italie, il n'y a pas eu d'autres initiatives, notamment du fait de la droitisation toujours plus croissante du gouvernement italien et la moindre médiatisation de ces drames. Et surtout ce protocole a plusieurs limites : dans de nombreux cas, les familles n'ont pas fait de demande d'enquête et les corps ne sont pas retrouvés. Par voie de conséquence, le rapprochement des données ante mortem du défunt avec les données post mortem n'est que rarement possible.

Alors, comment enquêter si l'on ne dispose pas de corps ? La médecine légale traditionnelle ne parait pas pouvoir être de grand recours, puisqu'elle est fondée sur la matérialité d'un cadavre. Un autre protocole d'enquête est nécessaire. Ainsi l'unité forensique du CICR, notamment le légiste José Pablo Baraybar explore d'autres pistes. Une méthodologie expérimentée consiste à mettre en place une analyse de réseau complexe[1976]. Pour ce faire, le CICR a lancé une collaboration avec des statisticiens et des mathématiciens, et noué un contrat avec une université de Buenos Aires. Ce genre de méthodologie a notamment été utilisée en Amérique latine, dans le cadre d'un programme nommé « Angelus »[1977]. Précisons que l'objectif de cette méthodologie n'est pas simplement l'identification d'une personne, mais la reconstruction de l'événement selon une perspective sociale. Pour José Pablo Baraybar, il faut prendre en compte l'ensemble des personnes présentes, même si l'on ne peut pas les identifier individuellement[1978].

---

[1975] "Between 2014 and 2019 there were 964 deaths of presumed migrants registered by Italian authorities, the majority of which remain unidentified (73%). Cases registered as identified (27%) were accomplished primarily through visual recognition. There remain some cases (e.g. 6 in Taranto, Puglia) to be further verified which have therefore not been considered in this report; the cases of Lampedusa (7, October 2019) and later have not been added because they have not been verified with official documentation and will be integrated into the update. However, as mentioned above, the number does not include the approximate 800 bodies recovered from the Mellili/Catania operation (the case is still under investigation, no exact number of victims has been released yet). Including that operation would increase the total number of bodies for the period 2014-2019 to approximately ~2,609" ICRC, "Counting the dead, how registered deaths of migrants in the southern european sea border provide only a glimpse of the issue", November 2020 https://missingpersons.icrc.org/sites/default/files/2022-11/COUNTING-THE-DEAD-FINAL.pdf

[1976] BARAYBAR, Jose Pablo, CARIDI, Ines, STOCKWELL, Jill, "A forensic perspective on the new disappeared : migration revisited", in : PARRA, Roberto C., ZAPICO, Sara, UBELAKER, Douglas (ed.), *Forensic science and humanitarian action : interacting with the Dead and the Living*, John Wiley & Sons, 2020,p.101-116

[1977] un programme appelé Angelus, développé au Mexique par des mathématiciens en collaboration avec la Commission nationale de recherche de personnes disparues et qui repose sur l'utilisation d'un réseau d'algorithmes, de l'intelligence artificielle et de l'apprentissage automatique. Ce programme représente une bonne pratique, car il permet de traiter et de croiser une énorme quantité de données et de détecter l'existence de modèles, de contextes et de connexions qui peuvent faciliter la recherche des personnes disparues.
MIRELES CHAVEZ, Victor, MARTINEZ SANCHEZ, Marian, YANKELEVICH WINOCUR, Javier, SANCHEZ NATERAS, Gerardo, « Searching for the disappeared persons of the dirty war: computational ontologies and the search for truth », 2021, http://ri.ibero.mx/handle/ibero/6015

[1978] « Le fait d'attribuer correctement un nom à une personne à l'issue du processus d'identification, en tant que tel, ne représente qu'une partie du travail d'information des familles. La reconstitution rétrospective des circonstances expliquant ce qui lui est arrivé et l'endroit où elle se trouve constitue une autre part essentielle du processus d'identification, non seulement à des fins d'identification définitive, mais aussi pour que les familles sachent dans quelles conditions leur proche a disparu ou est décédé. Il est par conséquent crucial de s'assurer que tout est fait pour élucider ces deux aspects (le sort et la localisation). « CICR, « Le processus d'identification forensique : une approche intégrée », 2022 https://www.icrc.org/fr/publication/4590-forensic-human-identification-process-integrated-approach


**Figure 7.1** Example of a small network. There are two types of nodes, missing persons (ellipses) and survivors or witnesses (rectangles), and three different types of links (a continuous line means that the connected individual began the travel together, a double line means that the connected individuals boarded the same boat, and the dashed line means that one of the individuals, survivor or witness, saw the other one). All networks were built using Cytoscape (cytoscape.org; Shannon et al., 2003) and R software (www.r-project.org).



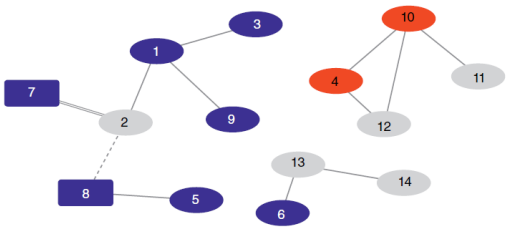



**Figure 7.2** Network involving missing (ellipses) and survivors (rectangles). Colours represent the fates of the individuals: blue for those individuals belonging to the event of shipwreck A, red for event shipwreck B, and those in grey for those individuals whose whereabouts are unknown.

**ANALYSE DE RESEAU COMPLEXE APPLIQUEE AUX DISPARUS EN MER MEDITERRANEE**[1979]

Les informations collectées forment différents types de réseaux. La forme de ces derniers varie selon leur nombre de nœuds, leur caractère dynamique ou non, leur vitesse d'évolution. Une fois que le réseau a été constitué, il peut être utilisé pour déduire des informations qui ne viennent pas des entretiens de terrains. De fait, il est possible que deux individus de la même région partagent des variables similaires telles que la date et le lieu de départ de leur voyage, la langue, la profession. Dans de tels cas, leurs relations sont implicites.

Les deux méthodologies d'enquête qu'on a évoquées reposent sur des traitements de données spécifiques, des données génétiques, des entretiens auprès des survivants et/ou des familles. Chacune pose des enjeux spécifiques en matière de protection des données. La multiplicité des acteurs et des techniques d'investigation complexifie le cadre de référence éthique et juridique en matière de protection de la vie privée des morts, des disparus et de leurs familles. Mais avant de rentrer dans le détail de ce sujet, il est nécessaire d'aborder les débats concernant le statut juridique des morts.

[1979] BARAYBAR, Jose Pablo, CARIDI, Ines, STOCKWELL, Jill, "A forensic perspective on the new disappeared : migration revisited", in : PARRA, Roberto C., ZAPICO, Sara, UBELAKER, Douglas (ed.), *Forensic science and humanitarian action : interacting with the Dead and the Living*, John Wiley & Sons, 2020,p.101-116

## Section 2 — Droit des défunts et protection des données des morts

Dans les deux derniers chapitres, on a cherché à voir comment les ONG tentaient d'assurer les droits des bénéficiaires et ne plus les réduire à de « pures victimes » en garantissant leur autodétermination informationnelle. Pour les morts, le situation est différente : le fait de leur accorder des droits fait débat. Ils ne disposent plus d'un statut de personne dans le sens juridique du terme. Cela dit, une grande partie des chercheurs considèrent en fin de compte qu'ils ne bénéficient que de droits résiduels, dont, généralement, le droit à la vie privée ne fait pas partie.

### § 1 — Le statut juridique des morts

Donc le statut juridique des défunts ne fait cependant pas consensus, et les juristes peinent à trouver une façon de qualifier les cadavres. Ils ne sont ni tout à fait des objets ni des sujets de droits.[1980] Le débat sur les droits des morts est loin d'être tranché. Il n'existe pas de consensus ou de cadres harmonisés relatifs aux droits dont ils peuvent bénéficier. Cette indécision juridique est due au statut même de la mort dépendant de représentations culturelles et sociales[1981], d'où l'indécision des juristes cherchant à qualifier ce « je ne sais quoi » qu'est un cadavre.

Selon une première interprétation, la mort signifie la disparition pleine et entière de la personne morale. Selon la maxime latine : « Actio personalis moritur cum persona. » Le cadavre est alors considéré comme une chose. Sont alors opposés — en héritage du droit romain — selon une « summa divisio », les choses et les personnes, les objets et les êtres humains animés et vivants. Cette position parait difficilement défendable. Nous nous retrouvons alors à refuser une réification complète des morts tout en ne pouvant les considérer comme des personnes. Il existe toutefois une troisième voie permettant de sortir de la division binaire entre chose et personne. Pour certains juristes, les morts sont au moins dotés d'une « demi-personnalité ». Ils conservent donc quelques droits, notamment le droit à une inhumation digne. Et plusieurs champs juridiques et éthiques se sont penchés sur la question du statut des morts : les notaires, les chercheurs en bioéthique (concernant les autopsies et le don d'organe), et la médecine légale. Ainsi, pour faire une autopsie, le consentement (a priori) de l'individu est nécessaire. Cela dénote une survie de la volonté de

[1980] TOUZEIL-DIVINA, Mathieu, BOUTEILLE-BRIGANT, Magali, « Le droit du défunt », *Communications*, 2015/2 (n° 97), p. 29-43. https://www.cairn.info/revue-communications-2015-2-page-29.htm

[1981] LE BRETON, David, « Le cadavre ambigu : approche anthropologique », *Études sur la mort*, 2006/1 (n° 129), p. 79-90. https://www.cairn.info/revue-etudes-sur-la-mort-2006-1-page-79.htm

la personne après sa mort. Par exemple, en bioéthique, le « respect dû au corps humain », et donc à l'intégrité corporelle, « ne cesse pas avec la mort »[1982].

## §2 — Les droits de l'homme des morts selon la médecine légale humanitaire

On s'intéressera pour notre part à la façon dont ce débat a été investi par les chercheurs et médecins légistes engagés dans l'identification des corps de victimes de massacre de masse et de crime contre l'humanité. Or les légistes et les chercheurs ne s'accordent pas sur les réponses à donner à ces questions. On peut par exemple commencer par exposer la position de l'anthropologue Adam Rosenblatt sur ce sujet. Ce dernier affirme que le langage des droits de l'homme, curieusement, n'est pas utilisé dans le champ de la médecine légale pour parler des morts[1983]. L'objectif des médecins légistes est de rétablir leur droit à la vérité pour les familles. Il s'agit de défendre leur droit à connaitre le sort de leur proche. Mais les médecins légistes n'évoqueraient pas le sort des morts en s'appuyant sur le langage des droits humains, du moins c'est ce que démontre Adam Rosenblatt. Ce dernier rejoindrait en partie les positions d'Antoon De Baets[1984].

Pour Antoon De Baets, les personnes décédées conservent cependant des traces de leur humanité passée de façon symbolique. Cela implique qu'ils bénéficient d'une forme de dignité posthume qui est au fondement du respect que les vivants leur doivent. En effet, les morts sont incapables de se faire respecter, de protéger leur dignité, c'est aux vivants de s'en assurer. Ces derniers ont donc à l'égard des morts une série d'obligations, résumées par De Baets dans le tableau suivant :

---

[1982]En droit français, ceci est rappelé par l'article R. 4127-2 (alinéa 2) du Code de la santé publique, l'article 2 in fine du Code de déontologie médicale (interne à la profession).

[1983] « In an era where "rights talk" occupies a privileged place in justifying humanitarian action, the human rights of the dead seem like a natural place for forensic teams to seek moral and political authority for the work they do. Yet this crucial part of the circle that human rights makes around international forensic investigation remains undrawn, beyond the reach of both the scientific and the moral-political vocabularies employed in the field. » ROSENBLATT, Adam, *Digging for the disappeared, Forensic science after atrocity*, Standford university press, 2015, p.155

[1984]The dead are no longer human beings (or persons) but are still reminiscent of them, marking them with powerful symbolism. It follows that there is only one possible definition for the dead: the dead are past human beings or past persons. My definition of the dead has one important consequence: since the dead are not human beings, they have neither full nor residual human rights (and even no rights at all)"
"With its dual claim that the dead do not have rights and the living have duties toward the dead, the posthumous dignity thesis is situated halfway between the legal maxim of actio personalis moritur cum persona ("personal action dies with the person") in common law and the dignitarian approach in civil law. The thesis rejects two extreme and mutually exclusive positions: one that sees the dead as mere bodies without any influence and one that allocates full agency to the dead with own lives separate from the living."
DE BAETS, Antoon, « the posthumous dignity of dead persons, in: PARRA, C., Roberto, UBELAKER, H., Douglas, (ed.), *Anthropology of violent death, theoretical foundations for forensic humanitarian action*, John Wiley &Sons, 2023 P.18

**Table 5.1** Living duties regarding the deceased.

| Category | Duties |
|---|---|
| Body and property-related | Body – To provide protection regarding the remains of the deceased.<br>Funeral – To honour the dead by conducting funerary rites.<br>Disposal – To dispose of the deceased (burial or cremation) and not to disturb their place of rest.<br>Will – To respect the will of the deceased concerning their body and property. |
| Personality-related | Identity – To search for and identify the deceased; to record their death, cause of death, and details of the deceased, including name, date of birth and (if applicable) their nationality.<br>Image – To consider the privacy and reputation of the deceased when publicly portraying them after death.<br>Speech – To consider the privacy and reputation of the deceased when publicly conveying information about them. |
| General | Heritage – To identify and safeguard the heritage of the deceased. |
| Consequential rights | Memory – The right to mourn, to bury and cremate, and to commemorate.<br>History – The right to know the truth about past human rights abuses. |

Source: De Baets (2009, 123), slightly adapted and abridged by this author.

### DEVOIRS DES VIVANTS A L'EGARD DES MORTS D'APRES ANTOON DE BAETS[1985]

Or Adam Rosenblatt se distingue quelque peu des théories d'Antoon De Baets. Ce dernier aurait une interprétation erronée de la notion de dignité, qu'il confond avec celle de respect et d'égard[1986]. Pour Adam Rosenblat, la dignité est une qualité inhérente, qui ne peut être perdue, puisqu'elle est au fondement de la possibilité d'avoir des droits. Ce n'est pas le cas des morts, qui l'aurait définitivement perdue. Adam Rosenblatt se distancie ainsi d'Hannah Arendt. Sa conception des droits de l'homme est liée à l'appartenance à une communauté politique, et à la capacité d'une personne de s'en revendiquer. Les exilés et les parias en sont donc dépourvus, ainsi que logiquement, les morts. Ces derniers ne font pas (du moins dans la culture occidentale) partie d'une communauté politique. Mais contrairement à Hannah Arendt, Adam Rosenblatt a une conception dynamique des droits: il est possible de les perdre, mais toujours de les retrouver[1987]. Du moins pour les vivants. Il considère qu'un paria peut toujours réintégrer une communauté politique. Ce n'est pas le cas des morts et surtout pas le cas des morts anonymes dont le corps a été réduit à néant. Adam Rosenblatt écrit ainsi que :

« Les chambres à gaz, les bombes atomiques et les formes plus grossières de violence peuvent enlever aux morts des choses qui ne pourront jamais leur être rendues : leur identité, leur place dans le monde, leur corps. L'élément crucial de la vision morale des droits de l'homme est qu'ils sont inaliénables — que l'intouchable, le prisonnier d'un camp de concentration, la personne enfermée dans une chambre d'hôtel sordide ou à l'arrière d'une camionnette peut encore s'y raccrocher comme une revendication, un espoir et une réprimande. Le fait que les

[1985] DE BAETS, Antoon, « the posthumous dignity of dead persons, in: PARRA, C., Roberto, UBELAKER, H., Douglas, (ed.), *Anthropology of violent death, theoretical foundations for forensic humanitarian action*, John Wiley &Sons, 2023 P.18

[1986] Antoon De Baets se réfère à une citation de Claude Lévi Strauss qui postule le caractère universel du respect et aux égards que l'homme accorde à ses morts. Antoon traduit cependant « respect » par « dignity », ce qui est pour Adam Rosenblatt une erreur. « Il n'existe probablement aucune société qui ne traite ses morts avec égards. Aux frontières mêmes de l'espèce, l'homme de Néanderthal enterrait aussi ses défunts dans des tombes sommairement aménagées. » LEVI-STRAUSS, Claude, *Tristes tropiques*, Pocket, 2001 p. 269

[1987] "The danger in calling refugees, stateless people, prisoners, and others "rightless," a term used by Arendt and many contemporary critics, is that it renders static and hopeless a situation that is open to change. In this way, it seems to naturalize the violence of perpetrators and the indifference of the world. "Rightless" is a description of the person, whereas rights violations are actions that can be protested, acknowledged, and reversed." ROSENBLATT, Adam, *Digging for the disappeared, Forensic science after atrocity*, Standford university press, 2015, p.160

morts puissent être si clairement et si complètement hors d'état de restaurer leurs droits signifie qu'ils n'ont jamais eu de droits de l'homme en premier lieu. »[1988]

Cela dit, il est toujours possible de respecter un cadavre, d'en prendre soin, de considérer qu'il a le droit à un traitement en accord avec ce qui est considéré comme un traitement « digne ». Qu'en est-il des personnes dont on ne dispose plus des corps ? Adam Rosenblatt s'interroge : « S'il est encore légitime de parler de certaines revendications de ces morts à l'égard des institutions qui leur survivent (par exemple, que leurs biens soient distribués conformément à leurs souhaits), il semble presque impossible d'imaginer qu'une personne vaporisée, réduite en cendres, dont le corps est irrévocablement perdu, puisse avoir des droits de l'homme. »[1989] Cette interrogation fait écho aux réflexions de la chercheuse Gaëlle Clavandier sur le statut, juridique et éthique, à accorder aux « restes humains ». Elle entend par là des restes humains qui n'ont pas pour propriété intrinsèque d'être des dépouilles mortelles, mais qui sont « des restes liminaires. Dans la mesure où ils se situent à la marge, car ne correspondant pas, point par point, à ce qui qualifie un cadavre et n'étant pas non plus de simples déchets ou objets. »[1990] Et cela est d'autant vrai pour les migrants morts en migration. Ces derniers sont doublement dépourvus de droits : il s'agit d'exilés, des « parias » et des disparus, noyés au fond de la Méditerranée.

Adam Rosenblatt conclut, un peu abruptement, le chercheur en a conscience, que la protection des morts ne relève pas des droits de l'homme ni du respect de leur dignité[1991]. Il reconnait malgré tout que les morts ont certains droits, comme le droit d'être inhumé, de ne pas faire l'objet de dissection sans consentement, etc. Mais ces derniers varient grandement selon les contextes nationaux, et ne peuvent avoir le caractère transcendant et universel des droits de l'homme. Le fait que ces derniers n'incluent pas les morts ne signifie cependant pas qu'on ne doit rien aux morts. Selon Adam Rosenblatt, on peut faire trois choses pour les morts : ne pas les traiter de façon irrespectueuse selon les codes d'une communauté, leur redonner une identité, leur redonner une sépulture, et surtout en prendre soin. Et contrairement aux droits humains, qui sont culturellement situés malgré leur caractère

[1988] "Gas chambers, atomic bombs, and cruder forms of violence can take things away from the dead that can never be put back :their identities, their places in the world, their bodies. The crucial element of the moral vision of human rights is that they are inalienable - that the untouchable, the concentration camp prisoner, the person locked in a squalid hotel room or the back of a van can still hold onto them as a claim, hope and rebuke. The fact that the dead can be so clearly and utterly past any hope of restoring their rights means they never had human rights in the first place. ", ROSENBLATT, Adam, ibid.

[1989] " While it still might be legitimate to talk about certain claims these dead people make on the institutions that outlive them ( for example, to have their estates distributed according to their wishes), it seems nearly impossible to imagine that a vaporized person, a person turned to ash, a person whose body is irrevocably lost, can have human rights" Ibid.

[1990]CLAVANDIER, Gaelle, « De nouvelles normes à l'égard des restes humains anciens : de la réification à la personnalisation ? « , *Revue canadienne de bioéthique*, 2019, 2 (3), p.79— 87. https://doi.org/10.7202/1066465ar

[1991] "the dead are often treated with respect and consideration, but they do not have inherent dignity thus they cannot have human rights in the universal, inalienable sense that forms the moral core of every major human rights declaration and instruments." ROSENBLATT, Adam "International Forensic Investigations and the Human Rights of the Dead", *Human Rights Quarterly*, Volume 32, Number 4, November 2010, p. 921-950 https://doi.org/10.1353/hrq.2010.0015

universel, le fait de préserver l'identité d'un mort serait pour l'anthropologue un invariant civilisationnel[1992].

Redonner un nom à un mort va de pair avec le fait d'en prendre soin. L'anthropologue utilise la notion de « care » pour se référer aux différents gestes accordés aux personnes décédées. Il se réfère directement aux théories de Joan Troncoso pour penser la médecine légale. Une éthique du « care » met l'accent sur la dimension sensible de la relation du médecin légiste avec les corps des morts. Adam Rosenblatt la définit comme suit : « Les soins médico-légaux visent à restaurer l'intégrité du corps mort et sa place dans le monde social et matériel dont il a été violemment arraché. Elle cherche, dans chaque contact, examen et pratique technique auxquels le corps mort est soumis, à répondre à la violence subie, à l'inverser et/ou à la réparer. »[1993] Les pratiques de médecine légale contribuent en partie (avec le fait de lui restituer un nom) à une réhumanisation post-mortem via la reconstitution de corps malmenés, voire torturés. En somme, le soin que l'on doit aux morts ne découle pas d'une obligation inscrite dans les droits de l'homme, ni du fait de respecter leur dignité, mais du cadre éthique propre à la médecine légale.

L'anthropologue Claire Moon défend une thèse opposée à celle d'Adam Rosenblatt : les morts peuvent bénéficier de certains *droits humains*. Sa démonstration repose sur le fait que malgré l'absence de textes en matière de droits de l'homme se référant aux morts, les vivants se comportent comme s'ils avaient des obligations à leur égard. Ils traitent les morts comme s'ils avaient des droits humains. Autre argument, la plupart du corpus relatif aux droits de l'homme est lié aux morts, quand bien même il ne leur accorde pas directement de droits. Claire Moon rappelle ainsi que les différents textes de droits de l'homme ont été élaborés en réaction à un génocide. Ils sont en quelque sorte l'expression de ce qu'on doit aux morts. Elle écrit alors que : « l'invention de nouvelles institutions qui ont tenté de poursuivre ces crimes et l'intégration de la prise en charge des morts dans les enquêtes sur les droits de l'homme sont toutes, d'une certaine manière, l'expression de ce que nous devons aux morts. En ce sens, ces mesures fonctionnent comme des mémoriaux ainsi que comme des instruments préventifs et punitifs. Elles sont tournées vers le passé, en mémoire et en l'honneur des morts, autant qu'elles sont tournées vers l'avenir, pour tenter d'empêcher que les atrocités ne se reproduisent. »[1994] Ainsi, les principaux textes internationaux en matière de droits de

[1992] "the deprivation of identity is a violation whether or not it takes place in a cultural context in which each individual grave is marked with a name and date. Even in those cultures where bodies are cremated or sent off to sea, these practices are carried out by a community that knows the identity of the dead person. stripping someone's identity from her, during life and in death, is a violation whether or not all cultures choose to mark or preserve those identities in the same way." ROSENBLATT, Adam, ibid.

[1993] « the possibilities for care do not end at death. Caring actions create real changes in the conditions and status of dead bodies, bodies that are and sadly must remain beyond the reach of the absolute guarantees of human rights. Forensic care aims to restore the dead body's own integrity, and its place within the social and material world from which it was violently torn. It seeks, in every touch, examination, and technical practice to which the dead body is subjected, to respond to, reverse, and/or repair the violence suffered. » Ibid.

[1994] « the invention of new institutions which attempted to prosecute such crimes, and the incorporation of the care of the dead into human rights investigations are all in some way expressions of what we owe the dead. In this sense, these measures work as memorials as well as preventive and punitive instruments. They look backwards in memory and honor of the dead as much as they look forwards in an attempt to prevent the future repetition of atrocities. » MOON,Claire, » What remains? Human rights after death", in SQUIRE, Kirsty, ERRICKSON, David, MARQUEZ-GRANT, Nicholas, « *Ethical approaches to human remains: a global challenge in bioarchaeology and forensic anthropology,* Springer nature, 2020, 649 p.

l'homme ne contiennent pas de dispositions précises sur les personnes disparues ou la prise en charge des dépouilles. Mais des organes de l'ONU (notamment le groupe de travail sur les disparitions forcées) ont interprété différents traités de manière à en déduire des obligations relatives aux défunts et à leurs proches. En particulier, le droit à la vie impose aux États l'obligation procédurale d'enquêter sur les décès résultant d'actes illégaux ou suspects qui relèvent de leur juridiction. Et les organes compétents en matière de droits de l'homme et les tribunaux régionaux ont également reconnu le droit à la vérité, notamment dans le cadre de disparitions forcées.

Claire Moon fonde son argumentation sur la place qu'occupe la notion de dignité dans le Droit humanitaire et le corpus éthique de la médecine légale. Pour rappel, les obligations des vivants envers les morts dérivent de la convention de La Haye en 1907, des conventions de Genève de 1929 et 1949, ainsi que des protocoles additionnels de 1977, et des statuts de Rome de 1998, qui ont inauguré la cour pénale internationale. Par exemple, le DIH pose différents principes : le soin du corps, le rétablissement des liens familiaux, l'enterrement digne des morts qui doivent être « disposés de manière digne et leurs tombes respectées et correctement entretenues.»[1995] Il est clair qu'en situation de conflit armé international, les États parties ont le devoir de rechercher les personnes décédées (GI art. 15 ; GII art. 18, GIV art. 16). Ils doivent également s'efforcer de rassembler les informations nécessaires à l'identification des morts (GI art. 16 et GPI art. 33.2). En vertu du droit international humanitaire, les morts doivent être respectés, être enterrés honorablement et les sépultures doivent être marquées afin de faciliter l'accès et la protection des tombes (GI art. 17 et GPI art. 34.1). En outre, les restes des personnes décédées doivent être respectés et le retour à leur famille doit être facilité autant que possible (GPI art. 34.2)[1996].

Elle note ensuite que l'éthique de la médecine légale contient aussi de nombreuses références au terme de dignité, ce que ne relève pas Adam Rosenblatt, pour qui la médecine légale ne se prononce pas sur le fait d'accorder ou non des droits humains aux morts[1997]. Claire Moon se réfère notamment au protocole de Minnesota (son édition de 2016), principal texte normatif de la médecine légale qui stipule « que l'identification du ou des corps devrait répondre aux droits de l'homme et au droit humanitaire et à d'autres besoins sociaux et culturels. »[1998]

Mais surtout, Claire Moon cite l'ensemble des publications éditées par le CICR. En effet, l'organisation a identifié un manque au sein de la doctrine propre à la médecine légale, qui ne comprendrait pas un cadre éthique prenant en compte la nécessité de s'assurer d'un

---

[1995] Customary IHL, Vol II, Chap 35, Section II, Rule 113. Treatment of the Dead, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule113 « disposed in a respectful manner and their graves respected and properly maintained.»

[1996] MSF, « Personnes disparues et les morts », Dictionnaire pratique du droit humanitaire https://dictionnaire-droit-humanitaire.org/content/article/2/personnes-disparues-et-les-morts/

[1997] SQUIRES, Kirsty, ERRICKSON, David, MARQUEZ-GRANT, Nicholas, *Ethical Approaches to Human Remains : A Global Challenge in Bioarchaeology and Forensic Anthropology*, Springer nature, 2020, 649 p.

[1998] "Human identification is the allocation of the correct name/identity to human remains. In any death investigation, the identification of the body or bodies is a major priority. It also meets humanitarian, human rights, and other social and cultural needs." the Minnesota protocol on the investigation of potentialy unlawful death, 2016, United Nations of human rights

traitement « digne » des morts[1999]. Le CICR appelle à combler ce déficit, en produisant une série de guides et de « soft law » visant à clarifier dans quelle mesure la médecine légale est liée à l'obligation de respecter la dignité des morts. Comme on l'a déjà dit, c'est l'acte d'identification d'un corps qui assure un traitement respectueux de ce dernier. Donc pour Morris Tidball Binz : « L'identification scientifique découle de notre responsabilité partagée à l'égard des morts, d'où la nécessité humanitaire d'assurer leur récupération, leur gestion, leur analyse et leur identification, afin de protéger leur dignité et d'éviter qu'ils ne deviennent des personnes disparues. » [2000] De façon concrète, traiter les morts de façon « indigne » signifie ne pas collecter les corps et les identifier a minima (via un numéro), ne pas récolter d'information sur les cadavres, etc. En clair, compromettre la possibilité de les identifier. On peut ainsi lire dans un manuel du CICR que « ce n'est pas l'impact visuel (des défunts non numérotés, non examinés ou non enregistrés) qui rend la gestion de ces morts indigne ; c'est le fait que cette gestion rend leur identification "impossible, plus difficile ou prolongée de manière injustifiée", que ce soit dans un avenir proche ou à plus long terme. »[2001]

La récupération et la gestion des restes humains, leur analyse en vue d'établir la cause du décès et l'identification du corps permettent en elles-mêmes de garantir le respect de la dignité des personnes décédées[2002]. L'acte d'identification propre à la médecine légale est motivé par la nécessité d'arracher les morts à leur condition de disparus. Il faut redonner aux morts une identité sociale, les inclure à nouveau dans un groupe, et il faut faire en sorte de traiter selon les normes existantes des morts qui « dérogent » jusqu'alors aux codes sociaux en vigueur[2003]. Pour la chercheuse Claire Moon, le travail d'identification permet de réunir le corps avec l'identité passée de la personne. La médecine légale est une pratique de « ré-humanisation » post-mortem. Elle contribue à préserver la part d'humain d'un cadavre et sa dignité, qui est une qualité résiduelle survivant à la mort de la personne. Or, c'est ce reste d'humanité qui rend possible pour Claire Moon la reconnaissance des droits de l'homme propres aux morts. Notons qu'elle mène là une interprétation personnelle de la notion de dignité au sein du corpus éthique du CICR. Pour rappel, l'organisation humanitaire, qui reste

---

[1999] Existing guidelines for managing the dead, such as INTERPOL's Disaster Victim Identification Guide4 and the manual for first responders for the management of the dead published by the ICRC and the World Health Organization (WHO),are accomplished from a technical point of view, but offer little or no guidance for ensuring the respectful and dignified management of the dead and their remains."
« Les lignes directrices existantes pour la prise en charge des morts, telles que le Guide d'identification des victimes de catastrophes d'INTERPOL et le manuel à l'intention des premiers intervenants pour la prise en charge des morts publié par le CICR et l'Organisation mondiale de la santé (OMS), sont efficaces d'un point de vue technique, mais n'offrent que peu ou pas d'indications pour assurer une prise en charge respectueuse et digne des morts et de leurs dépouilles. » First Expert's Meeting", *International Review of the Red Cross*, 2019, 101 (912), p.1213-1229 https://international-review.icrc.org/sites/default/files/pdf/1602948923/IRC101_3b/S1816383120000223a.pdf

[2000] "Scientific identification arises from our "shared responsibility for the dead, from which derives the humanitarian need for ensuring their proper recovery, management, a analysis and identification, to protect their dignity and to prevent them from becoming missing persons » ICRC, "Guiding Principles for Dignified Management of the Dead in Humanitarian Emergencies and to Prevent them Becoming Missing Persons", November 2021 https://www.icrc.org/en/publication/4586-guiding-principles-dignified-management-dead-humanitarian-emergencies-and-prevent

[2001] "It is not the visual impact (of unnumbered, unexamined, or unrecorded deceased) that renders the management of these dead undignified; it is the fact that such management renders their identification "impossible, more difficult, or unjustifiably prolonged" either in the near future or over the longer term." CORDNER, Stephen, TIDBALL-BINZ, Morris, "Guiding principles for the dignified management of the dead in humanitarian emergencies and to prevent them from becoming missing persons, PARRA, Roberto, UBELAKER, Douglas, *Anthropology of violent death : theoretical foundations for forensic humanitarian action*, John Wiley & Sons, 2023, p.351-375

[2002] ICRC, Advisory service on international humanitarian law, "Humanity after Life: respecting and protecting the dead, April 2020 https://www.icrc.org/en/document/humanity-after-life-respect-and-protection-dead

[2003]CAROL, Anne, RENAUDET, Isabelle, *Des morts qui dérogent : à l'écart des normes funéraires, XIXème, XXème siècle*, PUP, 2023, 242 p.

attachée au principe de neutralité, n'utilise pas le langage des droits de l'homme. Ceci est valable également pour les morts. Toujours est-il que Claire Moon déclare ainsi que « La dignité est le concept fondamental des droits de l'homme, et c'est le principe unique qui définit ce qui est "être humain" à la fois dans la vie et, en relation avec les histoires et les protocoles décrits, dans la mort. En outre, les protocoles juridiques et les pratiques médico-légales existants régissant le traitement des morts exigent que les morts soient traités comme s'ils avaient droit à la dignité, et que les vivants agissent en accord avec cette croyance. »[2004]

Plus profondément, ce traitement digne des corps implique d'accorder un certain statut aux morts, de redéfinir la façon d'en prendre soin et faire en sorte qu'ils ne fassent pas l'objet d'une gestion mécanique et standardisée. Il suppose traiter les morts de façon à prendre en compte leur agentivité, de façon à rester à l'écoute de ce qu'ils ont à dire aux vivants. Un de nos enquêté en est convaincu : « *Traiter des personnes comme des objets, les mettre dans des dispositifs de gestions des corps, produit des informations, mais laisse la personne qui te donne des informations passives, alors que moi je crois que tout migrant est actif, et que même les morts, les disparus, parlent, donnent des informations ; et reconnaitre cette capacité de communiquer, des personnes, des corps, de s'exprimer, recevoir la voix, les traces de l'autre, c'est une question éthique de respect, alors que la gestion mécanique des corps, ça ramène à toute la littérature sur la biopolitique et du bon vieux Foucault et compagnie. Agamben parle de vie nue, et je pense que les morts en Méditerranée sont des morts nus, des morts désocialisés, c'est de la matière, et donc la gestion de cette matière, dans une perspective biopolitique/nécropolitique… Donc d'où cette idée de protéger les droits des personnes, même des morts. »*[2005]

Toutefois, il n'est pas question pour Claire Moon d'affirmer que les morts peuvent bénéficier pleinement de droits humains. Elle précise que la plupart de ces derniers ne sont pas applicables aux morts. Les droits post-mortem sont des droits résiduels. Et les morts ne peuvent évidemment pas revendiquer le respect de ces derniers, mais ils peuvent être considérés comme titulaires de droits. Ce sont les vivants qui les leur accordent. Par conséquent, Claire Moon parle donc plutôt des droits humains des morts *pour* les vivants. Et en clair, il resterait trois types de droit pouvant être accordés aux morts : le droit d'être identifié, d'être retourné aux familles[2006], et le droit à une inhumation digne. Soit une série de droits que l'on retrouve dans la déclaration de Mytilène, un texte porté par l'organisation

[2004] « Dignity is the core concept of human rights, and it is the single principle that defines what it is to 'be human' both in life and, in relation to the histories and protocols outlined, in death. In addition, existing legal protocols and forensic practices governing the treatment of the dead require that the dead are treated as if they have the right to dignity, and they require that the living act in ways that are concordant with this belief. » MOON, Claire, « What remains? Human rights after death." in SQUIRES, Kisty, ERRICKSON, David, MARQUEZ-GRANT, Nicholas (eds), *Ethical approaches to human remains : a global challenge in bioarchaeology and forensic anthropology*, Springer, 2019, p.39-58

[2005] Entretien n°36, identification des morts n°8, 21/05/2020

[2006] BARANOWSKA, Grazyna,"Advances and progress in the obligation to return the remains of missing and forcibly disappeared persons", *International Review of the Red Cross*, 2017, 99 (2), p.709-733 https://international-review.icrc.org/sites/default/files/irrc_99_905_13.pdf

« Last Rights », engagée dans la lutte pour la reconnaissance d'un traitement digne des morts en migration et de leurs familles[2007].

## §3 — Vie privée post-mortem

Notons bien que Claire Moon n'a pas cité le droit à la vie privée comme droit humain résiduel des morts. Cela ne signifie pas qu'il faille en conclure que les personnes décédées ne bénéficient pas de ce droit. Plusieurs auteurs et juristes ont commencé à s'intéresser à la problématique de la vie privée « post-mortem ». Ainsi la notion déjà évoquée de « dignité posthume » d'Antoon De Baets inclut la protection de la vie privée. Elle englobe plusieurs obligations : l'obligation de confidentialité par le médecin ; le respect de l'intimité du mort ; le fait que les familles puissent inhumer leur mort sans intrusion publique. Une deuxième facette de la dignité posthume relative à la protection de la vie privée est liée à la protection de la réputation et l'honneur de la famille. Il faut faire en sorte de ne pas diffamer un mort en exposant post-mortem des faits nuisant à son image et à celle des proches. Ces points ne constituent cependant qu'une facette de la vie privée des morts. Il nous semble qu'Antoon de Beats en laisse d'autres dimensions de côté. En effet, les morts continuent de « produire » des données. Le médecin légiste peut récolter des données relatives au corps de la personne. En outre, l'ensemble des données qu'on a décimées de notre vivant nous survit. Ce qui n'est pas sans poser problème. En effet, différentes affaires portant sur l'accès aux données numériques des défunts par les héritiers et les proches ont attiré l'attention de juristes. En Allemagne, une affaire a par exemple fait grand bruit : des parents ont en effet souhaité avoir accès au compte Facebook et à la messagerie de leur fille. Cette dernière s'étant suicidée, ils désiraient connaitre le motif de son passage à l'acte. Or la firme a opposé un refus à cette demande. Mais l'affaire a été portée en justice, et un juge a commencé par estimer que le désir des parents était légitime. Toutefois, la Cour d'appel de Berlin a ensuite tranché : quelles que soient les règles en matière de succession pour les contrats, le droit allemand relatif à la vie privée lui interdisait l'accès aux messages de sa fille[2008]. Cette affaire donne un premier aperçu des enjeux relatifs à la gestion de données d'un mort. Ajoutons qu'entre aussi en compte la question de la suppression ou non des données d'un mort. En absence de volonté précise d'un défunt, qui prend la responsabilité de supprimer un compte ? Peut-on se référer à un droit de propriété concernant les données des morts ? Qui dans ce cas devient propriétaire des données ? Le responsable de traitement ? Les héritiers ? Et surtout, quel type de texte juridique permet de s'accorder sur ces questions ?

[2007] http://www.lastrights.net/LR_resources/html/LR_mytilini.html
[2008] Landgericht Berlin, 21 U 9/16, 31 mai 2017

Si on se fonde sur le droit à la protection des données, la situation est à priori claire : le RGPD ne couvre pas les données des morts. Citons son considérant 27 : « le présent règlement ne s'applique pas aux données à caractère personnel des personnes décédées. Les États membres peuvent prévoir des règles concernant le traitement des données à caractère personnel des personnes décédées. » Il n'existe donc pas de cadre juridique harmonisé au niveau supranational s'appliquant à ces données post-mortem. L'encadrement des données des morts dépend du contexte national et du type de données, selon qu'on ait affaire à des données de santé ou des données d'un compte des médias sociaux. Le cadre juridique est donc hétérogène. Cependant, la juriste Edina Harbinja s'est intéressée à la façon dont le droit répond à ces questions[2009]. Et son analyse met à jour une opposition entre une conception patrimoniale et anglo-saxonne du sujet selon laquelle les héritiers ont une libre gestion des données du mort, et aux partisans du droit à l'oubli, prônant la suppression des données du défunt. Ainsi, les États-Unis ont d'abord adopté des solutions qui visent à insérer les données *post-mortem* dans une logique successorale en laissant des actifs numériques accessibles aux héritiers[2010]. La France se situerait entre les deux. Pour faire court, dans le cas français, la notion de « mort numérique » a été mise à l'agenda lors des délibérations conduisant au vote de la loi République numérique de 2016. Elle aboutit à la modification de l'art. 40-1 de la loi 78-17 du 6 janvier 1978) [2011]. L'article 63 de la loi pour une République numérique ajoute un paragraphe I à l'article 40 de la loi informatique et libertés. Pour rappel, cet article est dédié aux différentes actions attribuées aux personnes concernées (droit de rectification, mise à jour, effacement). Le texte de loi précise que, par défaut, les droits d'une personne s'éteignent avec sa mort. Ils peuvent être toutefois maintenus par l'émission de directives relatives à la conservation, à l'effacement et à la communication de ses données après son décès. Ces directives sont enregistrées par un tiers de confiance, certifié par la CNIL. Il existe d'ailleurs une industrie de niche consacrée à la « death tech », certaines entreprises proposent une série de service facilitant la gestion des données post-mortem par les proches[2012].

Cette possibilité ne se retrouve pas dans tous les différents textes de droit des pays européens. Par exemple, le code italien de la vie privée 196/2003 a été abrogé en 2018 par décret[2013], afin de prendre en compte le droit d'accès des familles aux données des personnes décédées. L'article précité prévoit qu'un droit d'accès aux données du défunt peut être exercé par ceux

---

[2009] HARBINJA, Edina*, Digital Death, Digital Assets and Post-Mortem Privacy*, Edinburgh university press, 2022, 272 p.

[2010] "Aux USA l'US Unifor law commission a travaillé à une première loi en 2014 : Uniform fiduciary Access to digital Assets Act ( UFADAA). Une première version est votée en 2014. Elle permet un accès par défaut des fiduciaires aux données post-mortem, sauf volonté contraire du défunt. Ce dernier peut soit établir un testament actant le refus d'accès à ses données, soit donner un accès aux héritiers aux données ayant de la valeur patrimoniale. Les autres données font l'objet d'une demande de fermeture de compte. Ce texte a fait l'objet de révision en 2015, sous la pression de lobbying de GAFAM, favorables à plus de garanties pour la privacy post-mortem. Ce débat a abouti au vote de la Revised Uniform fiduciary access to digital assets acts (RUFADAA). Seul le catalogue des données du défunts peuvent être accéder, et non leur contenu. Ce dernier peuvent être communiquées qu'avec le consentement du mort ou bien avec l'injonction du juge. » CASTEX, Lucien, HARBINJA, Edina, ROSSI, Julien, « Défendre les vivants ou les morts ? Controverses sous-jacentes au droit des données *post mortem* à travers une perspective comparée franco-américaine », *Réseaux*, 2018/4 (n° 210), p. 117-148. https://www.cairn.info/revue-reseaux-2018-4-page-117.htm

[2011] BORDES, Candice, « Prévoir sa mort numérique, le devenir des données numériques post-mortem » *RDLF chron*.n° 09, 2020http://www.revuedlf.com/personnes-famille/prevoir-sa-mort-numerique-le-devenir-des-donnees-numeriques-post-mortem/

[2012] REY, Lucienne, "Du testament en ligne au zombie numérique, synthèse de l'étude "la mort à l'ère numérique", TA-Swiss,2024

[2013] DECRETO LEGISLATIVO 10 agosto 2018, n. 101 https://www.gazzettaufficiale.it/eli/id/2018/09/04/18G00129/sg

qui ont un intérêt propre (soit les héritiers), ou ses tutelles, ou encore les proches. C'est à la personne concernée de s'opposer à ce droit d'accès en publiant de son vivant une déclaration. Cette dernière est ensuite communiquée à l'autorité de protection des données italienne. La loi espagnole de protection des données est relativement équivalente. Elle laisse la possibilité d'un droit d'accès aux données par les proches, ainsi qu'un droit d'opposition pour le mort. Ce dernier peut être édicté sous la forme d'un formulaire fixé avant le décès de l'individu[2014]. En revanche, en Grèce, le droit national de la protection des données n'évoque pas les morts, qui sont laissés dans un vide juridique.

Mais surtout, la littérature et le droit de la vie privée des morts paraissent s'être concentrés sur les enjeux touchant l'accès aux données des morts par des proches. Or que se passe-t-il lorsqu'on a affaire à un corps anonyme ? Ce cadre juridique répond-t-il aux enjeux de l'identification des morts ?

## Section 3 — La protection des données des morts en migration

Il semblerait que la protection des données n'est toujours pas perçue comme prioritaire par les différents organisations et acteurs s'occupant de l'identification des morts. Elle viendrait freiner un travail d'identification et prolonger l'incertitude des familles. Ainsi un enquêté avoue qu' : « *au CICR, les protocoles sont très lourds. Avec les petites ONG sur le terrain, c'est plus simple, il suffit de s'envoyer des informations par e-mail. (…) Les ONG peuvent travailler plus rapidement parce qu'elles n'ont pas cette protection stricte des données.... Mais je pense que c'est… c'est surtout pour aider la famille. Nous avons mis en place moins de protection des informations, parce qu'ils veulent des informations rapidement*. »[2015] Un autre enquêté avance qu'il aimerait bien « *que l'ICRC accepte certaines possibilités, certains risques dans la gestion des données des personnes en migration, qu'elles soient vivantes ou décédées.* »[2016] Et, la docteure légiste Cristina Cattaneo soutient alors que « Les problèmes de protection des données doivent être résolus. Dans de nombreux cas, il est demandé que les données ne soient pas incluses dans les bases de données des services répressifs et, par conséquent, le respect de la vie privée et la protection des données sont d'une importance capitale. Toutefois, ces problèmes doivent être résolus dans une perspective d'ouverture d'esprit afin

[2014] CRESPO OTERO, M. "Post-Mortem Data Protection and Succession in Digital Assets Under Spanish Law", In: CARNEIRO PACHECO DE ANDRADE, F.A., FERNANDES FREITAS, P.M., DE SOUSA COVELO DE ABREU, J.R. (eds) *Legal Developments on Cybersecurity and Related Fields. Law, Governance and Technology Series,* vol 60. Springer, 2024 https://doi.org/10.1007/978-3-031-41820-4_10

[2015] « At the ICRC, the protocols are really cumbersome. With small NGOs in the field, it's simpler, you just send each other information by e-mail. (…) NGO can work faster because they don't have this strict data protection…. But I think that's… it is very much to help the family I think so. We have less information protection in place, because they want information fast. »Entretien n°23, identification des morts n°2, 17/03/2020

[2016]Entretien n°36, identification des morts n° 8, 21/05/2020

de ne pas entraver l'identification.»[2017] Enfin, un enquêté considère que le principe de minimisation, principe clef de la protection des données, n'est pas adapté au travail d'identification des morts. Pour lui, il s'agit plutôt de collecter le plus possible d'informations afin de maximiser les chances d'identification. En outre, selon les standards de protection des données, les informations de la personne concernée doivent être supprimées une fois l'objectif du traitement atteint. Cela, dans le cas de l'identification des morts, peut avoir lieu des années après la collecte des données, [2018] d'autant plus que lors d'un naufrage, le processus d'enquête nécessite de prendre en compte les interconnexions entre les individus, et réutiliser les données d'un mort peut servir à l'identification d'un autre corps. Une enquêtée remarque ainsi que : « *De nombreuses questions se posent quant à savoir qui devrait détenir de l'ADN et pour combien de temps. Cela pourrait être trop court pour certaines personnes qui pourraient avoir besoin de rester dans les fichiers pendant de nombreuses années si elles recherchent une personne disparue. Je pense qu'elle devrait l'être parce qu'on ne sait jamais, je veux dire que des restes ont été découverts de nombreuses années après et qu'il serait tragique que ces liens possibles aient été perdus après tout ce temps.* » [2019]

Mais pour le CICR, dès 2002, la question de la confidentialité de l'information est à l'agenda des membres de l'organisation travaillant sur l'identification des morts[2020]. La vie privée est identifiée comme un élément clef de la gestion « digne » des morts. On peut lire ainsi dans un manuel de « médecine légale humanitaire » qu' : « à tout moment », la pratique médico-légale doit respecter « la dignité, l'honneur, la réputation et la vie privée » des personnes décédées[2021].

Cependant, le rapport du groupe de travail d'experts à l'origine de la création de l'unité de médecine légale du CICR fait état d'un vide juridique sur ce sujet : « en pratique, dans plusieurs contextes, il n'y a pas eu de cadre juridique approprié, pour ce qui est de la protection de la

---

[2017]« Data protection issues need to be solved. In many cases it is called for that data should not enter law enforcement databases, and therefore privacy and protection are of paramount importance. However, these problems should be solved with an open-minded perspective in order not to hinder identification. »CATTANEO, Cristina (et alii.), " the approach to unidentified dead migrants in Italy", in, PARRA, Roberto, ZAPICO, Sara, UBELAKER, Douglas, *Forensic science and humanitarian action : interacting with the dead and the living*, Wiley, 2020, p.559-570

[2018] « Même identifiés, des restes incomplets doivent être expertisés afin de décider quels éléments de preuve demeurent requis pour identifier les parties de corps manquantes. Une dépouille incomplète identifiée grâce à ses empreintes digitales, mais à laquelle il manquerait un membre inférieur, nécessitera par exemple de conserver d'autres éléments de preuve pour être en mesure d'identifier le membre manquant une fois qu'il aura été retrouvé et de le réunir au reste du corps. Ce qui peut se produire des jours, des semaines, des mois, voire des années plus tard. » CICR, « Le processus d'identification forensique : une approche intégrée », 2022 https://www.icrc.org/fr/publication/4590-forensic-human-identification-process-integrated-approach

[2019] « There are a lot of issues about who should held DNA and for how long. It may be to short for some people who may need to reside on the files for many many years if you are looking for a missing person. I think it should because you just don't know I mean remains have come to light many years after, and it would be tragic if those possible links have been lost after all the time. It is tricky, it is got the records have to maintain with the greatest possible integrity, whith checks and balances, and never in the hands of too few people who are unaccountable. » Entretien n°24, identification des morts n° 3, 20/03/2020

[2020]OP/REX 02/522 Update No. 17/2002 The Missing - The right to know Action to resolve the problem of people unaccounted for as a result of armed conflict or internal violence and to assist their families, https://reliefweb.int/report/world/icrc-update-project-missing-current-developments-no-2

CICR, Principes pour légiférer sur la situation des personnes portées disparues par suite d'un conflit armé ou de situation de violence interne : mesures de prévention des disparitions et de sauvegarde des droits et des intérêts des personnes portées disparues et de leur famille 2002.https://www.icrc.org/fr/doc/assets/files/other/model-law-missing-0209-fre-.pdf

[2021]« at all times" forensic practice must respect the "dignity, honour, reputation and privacy" of the dead. ICRC, "The missing: action to resolve the problem of people unaccounted for as a result of armed conflict or internal violence and to assist their families. Progress Report", 2003 https://www.icrc.org/en/doc/assets/files/other/icrc_themissing_012003_en_10.pdf

vie privée et des données à caractère personnel, pour la recherche des personnes disparues et l'identification des restes humains. » [2022] Or s'assurer d'un cadre éthique solide est d'autant plus nécessaire qu'une partie des données traitées pour identifier un mort est « sensible ». Il s'agit effectivement de données médicales, génétiques, ethniques et sexuelles. Et donc en l'absence de droit dur unifié sur le sujet, le guide de protection des données du CICR conseille de se référer au « droit mou » produit par des organisations[2023]. Or dans un premier temps, les propres guides et recommandations du CICR en matière de médecine légale humanitaire semblent contenir peu d'éléments réellement précis sur la protection des données. Par exemple, entre 2007 et 2016, le médecin légiste Morris Tidball-Binz a rédigé deux documents contenant des recommandations pour la gestion des morts. Elles ne comprennent que peu de références sur le sujet. Certes, la nécessité d'assurer la protection des données et la vie privée de la famille et des victimes est mentionnée, mais sans plus de détail. Elle semble être associée à la communication d'information par la presse[2024]. Cela dit, dans les échanges plus récents sur le sujet, et au sein des groupes de discussion ambitionnant de pallier le manque de cadre éthique relatif à l'identification des morts[2025], les enjeux de confidentialité sont abordés. Un enquêté nous relate la finalité du projet « Missing » : « *pour la première fois on a mis à la table, la question de la migration, et ça ne marche pas comme dans les autres cas de missing, d'où le travail qu'on mène, discussion. Y a cette volonté, d'à la fois d'aller plus loin, de la part de l'ICRC, tout en restant très vigilant, pour eux même, c'est important de respecter le cadre légal, sur la privacy*. »[2026] Les différentes réunions du programme ont abouti à la publication d'un document intitulé : « Missing Guiding Principles for the Dignified Management of the Dead in Humanitarian Emergencies ». Deux articles de ce dernier peuvent se rapporter à notre sujet :

L'article VIII qui postule que « Toutes les sources d'information nécessaires, telles que les registres et les bases de données, y compris celles qui contiennent des données pertinentes pour l'identification des personnes décédées, devraient être rassemblées, gérées, mises à disposition, consultées, utilisées et conservées en tenant dûment compte de la protection des données conformément au droit international et aux normes internationales. » Notons que le corpus juridique spécifique relatif à la protection des données des morts n'est pas cité, peut-

[2022]« in practice, in several contexts there has been no proper legal framework, in terms of the protection of privacy and personal data, for the search for the missing and the identification of human remains. »The Missing: action to resolve the problem of people unaccounted for as a result of armed conflict or internal violence and to assist their families, the legal protection of personal data & human remains, electronic workshop, Final report and outcome, ICRC 02/04/2002-06/05/2002 https://www.icrc.org/en/doc/assets/files/other/icrc_themissing_072002_en_1.pdf

[2023] "The lack of a uniform approach in data protection law to the Personal Data of deceased individuals means that Humanitarian Organizations should adopt their own policies on this matter (for example, by applying the rules applicable to the Personal Data of natural persons to the deceased, insofar as this makes sense). For organizations that do not enjoy immunity from jurisdiction, this question may be regulated by the applicable law." Christopher, MARELLI, Massimo (ed.), *Handbook on data protection in humanitarian action, second edition*, 2020 https://www.icrc.org/en/data-protection-humanitarian-action-handbook

[2024] "-Care is needed to respect the privacy of victims and relatives. - Journalists should not be allowed direct access to photographs, individual records or the names of victims. However, authorities may decide to release this information in a managed way to help with the identification process." https://international-review.icrc.org/sites/default/files/irrc_866_10.pdf

[2025] The development of guiding principles for the proper management of the dead in humanitarian emergencies and help in preventing their becoming missing persons: First Expert's Meeting https://international-review.icrc.org/sites/default/files/pdf/1602948923/IRC101_3b/S1816383120000223a.pdf

[2026]Entretien n°36, identification des morts n°8, 21/05/2020

être en raison du manque d'harmonisation de ce dernier. Le lecteur se retrouve cependant démuni en absence de précisions.

Et l'article XX qui postule que « les dispositions finales concernant les personnes décédées devraient être prises dans le respect de leur dignité et de leur vie privée, ainsi que de celles des membres de leur famille et de leur communauté. Des mesures devraient être prises pour protéger les sites et monuments funéraires contre toute profanation ou perturbation et pour les entretenir. »[2027]

On retrouve une trace de cette nécessité dans les différents documents publiés par ce groupe, notamment celui visant à constituer une « approche intégrée » de l'identification des morts[2028]. Il ressort de leur lecture qu'en matière de vie privée plusieurs points doivent faire l'objet d'une attention particulière. Tout d'abord, il est évident que l'examen corporel ainsi que l'éventuelle autopsie exigent des conditions particulières pour préserver la vie privée du défunt. Le corps ne doit pas être exposé au vu de tous et doit être examiné dans des conditions respectant l'intimité du défunt. Dans les différents cadres juridiques existants, pour l'autopsie, le consentement est présumé implicite, même si la famille peut s'opposer à ce geste médical. Enfin, il est précisé que les données collectées lors de l'identification des personnes décédées doivent être traitées de façon responsable, surtout en ce qui concerne les données génétiques. Nous n'avons cependant pas trouvé d'indications supplémentaires sur ce point.

Mais puisque les migrants morts en migration peuvent être tout d'abord considérés comme des « personnes disparues », il parait judicieux d'examiner les codes éthiques du service de rétablissement des liens familiaux. D'autant qu'il se trouve que le service de RFL s'est pourvu d'un cadre normatif propre à son unité concernant la protection des données, formalisé en 2015[2029]. Une résolution a été votée fin 2019 sur le sujet[2030]. Le fait d'avoir publié un cadre éthique est de toute façon nécessaire : le CICR est une organisation internationale, et il n'a pas à appliquer le RGPD. Notons aussi que les disparus ont un statut ambigu : ils ne sont ni tout à fait vivants ni tout à fait morts. Cela est psychologiquement éprouvant, mais cela laisse aussi un certain flou sur le type de cadre juridique à appliquer. Au-delà du CICR, la situation est plutôt incertaine : s'ils sont vivants, de façon plus générale, le RGPD s'applique, s'ils sont morts, c'est logiquement le droit national où le corps a été retrouvé qui s'applique. Pour ce qui concerne le CICR, les codes éthiques des services RFL tranchent en indiquant qu'ils

[2027] ICRC, "Guiding Principles for Dignified Management of the Dead in Humanitarian Emergencies and to Prevent them Becoming Missing Persons", November 2021

[2028] « lors des recherches menées pour localiser des personnes disparues, les efforts déployés pour reconstituer leur parcours permettront d'expliquer exactement à leur famille, à leur communauté et à la société dans son ensemble ce qui leur est arrivé (respectant ainsi leur droit de savoir et leur droit à la vérité). Il est également important de tenir compte des aspects relatifs à la protection des données et au principe consistant à "ne pas nuire", notamment lorsque les familles se trouvent encore en situation de vulnérabilité du fait de plusieurs facteurs qui vont au-delà de la disparition. » CICR, « Le processus d'identification forensique : une approche intégrée », 2022

[2029] ICRC, « Restoring family links, Code of conduct on data protection », November 2015, Version 1.0 https://www.icrc.org/en/document/rfl-code-conduct

[2030] 33rd International conference of the red cross and red crescent Geneva, Switzerland 9–12 December 2019 Restoring Family Links while respecting privacy, including as it relates to personal data protection https://rcrcconference.org/app/uploads/2019/12/RFL-Resolution_12-December-FINAL-at-1430_CLEAN_en.pdf

s'appliquent aussi bien aux données des vivants que des morts[2031]. Ils précisent en effet que les activités de RFL peuvent nécessiter de gérer des données de personnes décédées. Mais ils ne donnent pas plus de détail sur l'éventuelle spécificité du traitement de ces dernières.

Donc, à la lecture de ces documents, on peut en conclure que le vide juridique entourant les données des morts a été pris en compte, et le sujet peut être abordé au sein de groupes de travail. Mais il semblerait qu'il n'ait pas été traité de façon exhaustive, les manuels restant relativement généraux sur les enjeux de vie privée. On tentera donc dans les paragraphes qui suivent de préciser quels sont les enjeux spécifiques associés à la protection des données des morts.

### §1 — Accès aux données des personnes décédées

Pour commencer, au-delà du geste forensique et des données d'autopsie, identifier un corps peut nécessiter la consultation de données variées, conservées par de multiples acteurs, que ce soient des dossiers médicaux, des archives policières ou des registres de cimetières.

Or l'accès à certaines données peut être restreint juridiquement et il est vrai que le droit de la protection des données peut sembler constituer a priori un obstacle aux enquêtes. C'est le cas des données de santé. Précisons tout d'abord qu'identifier un mort peut nécessiter d'avoir des informations sur son aspect physique, y compris sur son profil biologique, ainsi que ses antécédents médicaux. Il est donc nécessaire de réunir des supports photographiques, des radiographies médicales et dentaires, des empreintes dentaires. Un certain nombre de ces informations sont recueillies lors de l'autopsie. D'ailleurs, la Convention du 4 avril 1997 pour la protection des droits de l'homme et de la dignité de l'être humain à l'égard des applications de la biologie et de la médecine précise que : « Toutes les données à caractère personnel concernant la personne sur laquelle a été pratiqué le prélèvement d'organes ou de tissus ainsi que les données concernant le receveur doivent être considérées comme confidentielles. Elles ne peuvent être collectées, traitées et communiquées que dans le respect des règles relatives au secret professionnel et à la protection des données à caractère personnel. » Mais il peut aussi être utile de consulter des dossiers de santé. Leur accès reste cependant très réglementé : les défunts bénéficient toujours du secret médical. En 1994, la déclaration d'Amsterdam concernant le droit des patients stipule bien que « Toutes les informations concernant l'état de santé d'un patient, sa situation médicale, le diagnostic, le pronostic et le traitement, ainsi que toutes autres informations de caractère personnel doivent être tenues

[2031] « This CoC applies to the processing of personal data (including data relating to deceased persons) by the Data Controllers in respect of the enquirer(s), sought person(s) and other individuals related to RFL activities. » « le présent CdC s'applique au traitement des données à caractère personnel (y compris les données relatives aux personnes décédées) par les responsables du traitement des données en ce qui concerne le(s) demandeur(s), la(les) personne(s) recherchée(s) et d'autres personnes liées aux activités du RFL. » ICRC, "Restoring family links", Code of conduct on data protection, November 2015, Version 1.0 https://www.icrc.org/en/document/rfl-code-conduct

confidentielles, même après le décès ». Mais dans certaines juridictions, les familles peuvent bénéficier d'un droit d'accès plus ou moins étendu[2032]. Et surtout, des dérogations existent dans certaines législations pour les médecins légistes ou pour la police judiciaire[2033]. Cela dit, pour le sujet qui nous occupe, il peut arriver qu'aucun dossier médical ou dentaire ne soit pas disponible ou exploitable. Plusieurs raisons peuvent l'expliquer. Cela peut être dû à l'accès limité des exilés aux services de santé dans leurs pays d'origine, à la destruction d'archives, à la mauvaise qualité des dossiers ou encore à la perte ou à la destruction de ces derniers. Seuls des entretiens avec les membres de la famille ou l'entourage proche de l'individu permettront d'obtenir des informations de santé, au risque de devoir se contenter de données imprécises[2034].

On peut également mentionner un autre type de données potentiellement intéressantes pour l'identification des morts : les informations détenues sur les téléphones des exilés. La journaliste Taina Tervonen raconte que lors de sa visite au Labanof, elle avait été frappée par la vue d'un sachet contenant un téléphone Nokia jaune citron retrouvé dans une épave. C'est tout ce qu'il restait d'un migrant mort lors d'un naufrage en mer Méditerranée[2035]. Est-il alors possible et souhaitable d'accéder aux données qu'il renferme dans le cadre d'une enquête ? Généralement, l'accès aux données contenues dans les mobiles est réservé aux forces de l'ordre. L'accès à des données téléphoniques et de réseaux sociaux, pour des opérations de « digital forensic » reste — théoriquement — encadré par la loi[2036]. Et au regard de la criminalisation des exilés, il parait peu souhaitable que les forces de l'ordre puissent avoir accès à ce type de données. L'extraction de données des téléphones est plutôt associée à des enquêtes criminelles de façon générale, et au contrôle des exilés, l'accès aux données des smartphones est requis lors des demandes d'asile, mais cette pratique reste décrié par les activistes de défense des migrants au nom de leur vie privée[2037].

Au-delà des forces de l'ordre, certains enquêtés mentionnent la possibilité d'identifier un possesseur de téléphone grâce à sa carte SIM. Ils ne spécifient pas la légalité de ce geste. Mais ils s'y opposent par éthique personnelle : « *On peut retrouver des cartes SIM. On peut se servir*

---

[2032] POISSON, Dominique, « Que devient le secret médical après le décès d'une personne ? », *Laennec*, 2007/1 (Tome 55), p. 49-58. https://www.cairn.info/revue-laennec-2007-1-page-49.htm

[2033]SCHULIAR Yves, « Les morts judiciaires – le rôle de la Médecine Légale. Le cas particulier de l'identification des victimes de catastrophes », *Études sur la mort*, 2012/2 (n° 142), p. 193-223. https://www.cairn.info/revue-etudes-sur-la-mort-2012-2-page-193.htm

[2034]CICR, « Le processus d'identification forensique : une approche intégrée », 2022

[2035]TERVONEN, Taina, *Au pays des disparus*, Fayard, 2019, 256 p.

[2036] Standards and best practices for digital forensics,UNODC https://sherloc.unodc.org/cld/en/education/tertiary/cybercrime/module-4/key-issues/standards-and-best-practices-for-digital-forensics.html

GOLDSTRAW WHITE, Janice, "legal and policy framework for digital forensics: a resource for practitioners a policy and Practice Briefing from the Digital Forensics and Social Media project funded by the Dawes Trust", 2022 https://perpetuityresearch.com/wp-content/uploads/2022/09/Final-Legal-Procedural-and-Guidance.pdf

HORSMAN, Graeme, "Defining principles for preserving privacy in digital forensic examinations", *Forensic science international* : *digital investigation,* volume 40, 2022 https://www.sciencedirect.com/science/article/abs/pii/S2666281722000191

[2037] SCHEEL, S., "Epistemic domination by data extraction : questioning the use of biometrics and mobile phone data analysis in asylum procedures", *Journal of Ethnic and Migration Studies*, 2024, *50*(9), p. 2289–2308. https://doi.org/10.1080/1369183X.2024.2307782

*des cartes SIM pour contacter des proches*[2038]*. Mais c'est compliqué : on ne sait pas à qui on a affaire. Cela serait comme s'introduire dans la vie des gens.* »[2039] Et même lorsqu'il n'est pas question d'accéder à des données téléphoniques, mais contacter les proches grâce à un numéro de téléphone écrit sur un papier retrouvé sur des corps de personnes décédées, certains de nos enquêtés hésitent à franchir le pas.

Le droit réserve l'accès aux données des registres réservés aux « professionnels » du travail des morts, ou dans certains cas aux proches et aux familles. Or concernant les morts en migration, c'est bien souvent des membres de la société civile qui s'en charge. Il peut être plus difficile pour ce type d'acteur d'avoir accès à certaines données. Et certains enquêtés nous ont confié leur frustration sur ce point. De surcroit, des enquêtés mettent en doute certaines restrictions d'accès. Une enquêtée déclare que dans certains cas : « *Il y a la question de l'accès des familles aux informations détenues par les autorités, qui mettent en place des obstacles, en raison de ce qu'elles considèrent comme des limitations dues à la protection des données, quant à la quantité d'informations qu'elles peuvent partager*. » [2040] Selon un autre témoignage : « *La vie privée est utilisée comme excuse pour empêcher les gens d'obtenir des informations, elle est utilisée contre… c'est plus un bouclier que pour la vie privée, parce qu'encore une fois, les morts n'ont pas de vie privée. Je pense que certaines de mes demandes d'accès à des informations ont été refusées sous prétexte de respect de la vie privée. »*[2041]

Cependant, il arrive que certaines bases de données puissent être accessibles à des acteurs de la société civile. Des autorisations d'accès peuvent être accordées sous forme de protocole et d'agrément. Cela a été le cas pour l'antenne de la Croix rouge de Catane, qui a signé en 2018 un accord avec la mairie de cette ville. L'objectif était de pouvoir exploiter des données non publiques[2042]. Et l'accord a permis d'accéder aux données d'acteurs de l'État civil, des pompes funèbres et aux employés du cimetière. Un deuxième accord a permis à la Croix rouge de Catane de consulter et compiler des informations détenues par la police judiciaire et scientifique. L'objectif était de rapprocher les différentes sources de données pour contribuer à identifier les morts du cimetière de Catane, puis remonter jusqu'aux familles, soit une inversion de la logique habituelle de RFL. Les données concernant les morts sont en effet éparpillées dans des documents divers. Il s'agit soit des décrets d'enterrement et d'exhumation, de certificats de décès, de formulaires d'inscription d'informations médico-

[2038]« Les outils du commerce à destination des acteurs judiciaires permettent l'analyse des cartes SIM dans le but de lire et d'enregistrer les informations utiles contenues dans ces dernières sans en modifier les données. Les renseignements collectés sur ce support sont nombreux. Parmi les données intéressantes, nous retrouvons le numéro de série de la carte (ICCDI) et le numéro de l'abonné (IMSI) qui permettent d'identifier le propriétaire. Des réquisitions judiciaires peuvent alors être notifiées à l'opérateur qui a fourni cette carte afin d'obtenir toutes les informations liées à l'abonné telles que la liste des appels par exemple. La carte SIM contient parfois un répertoire téléphonique, additionnel à celui du téléphone ainsi que des messages SMS. » https://www.gendarmerie.interieur.gouv.fr/pjgn/institut-de-recherche-criminelle-de-la-gendarmerie-nationale/l-expertise-decodee/analyse-numerique/faire-parler-les-telephones

[2039]Entretien n°30, identification des morts n°5, 10/04/2020

[2040] « There is the issue of the access for families for information which is held by authorities, who put obstruction in place, because of what they consider data protection limitation, of how much they can share. »Entretien, identification des morts n°3, 20/03/2020

[2041] « privacy is used as an excuse to not allow people to get people some information, it is used against…it is more a shield rather than privacy, because again, the death don't have privacy. I think some of my requests of information access were refused with the excuse of privacy n°4, 06/04/2024

[2042]FURRI, Filippo, KOBELINSKY, Carolina « Une bureaucratie pour les morts en Méditerranée », communication au colloque *« Tri migratoire » et expériences du blocage : Afrique, Amérique, Europe*, Nice, juin 2021.

légales, de procès-verbaux de témoignages de survivantes et survivants obtenus sur l'embarcation avant l'accostage à Catane. En l'absence de protocole spécifique, le recueil des données des morts est partagé entre les garde-côtes, le médecin légiste local, les personnes chargées du traitement administratif des personnes décédées (les services délivrant l'autorisation d'inhumer). Les données recueillies n'ont pas vocation à servir à l'identification des corps, mais à l'enregistrement du décès de ces derniers. Et il n'y a donc pas de stockage centralisé de l'ensemble des données du mort[2043]. Par conséquent, souligne un rapport de l'OIM « une identification basée sur ces données est rarement effectuée »[2044]. L'initiative de la Croix rouge vise à pallier ce manque en centralisant l'ensemble de ces données. Ainsi, une première « base de données » a été constituée. Son objectif est l'identification des morts anonymes enterrés au cimetière de la ville de Catane, ainsi que la rectification de l'acte de décès[2045]. Une première version de la base de données comprenait trois colonnes. Une première colonne précise le moment où un lien entre un corps et un nom a été rapporté (lors du débarquement ou bien plus tard). Une deuxième colonne comprend des informations sur la personne qui a établi le lien (une mère, un père, une sœur, un frère, un ami). Enfin, une dernière colonne est consacrée à la manière dont la correspondance s'est opérée (reconnaissance du corps, des photographies, d'objets retrouvés sur le corps du mort)[2046]. Cette démarche est décrite comme exceptionnelle par les chercheurs, mais son ambition contraste avec sa modestie en matière moyen humain (la constitution de la base de données n'implique « que » quelques personnes), et pour ce qui est de la complexité de la modalité d'enquête.

Sachant que la base de données comprenait différents niveaux de confidentialité, selon la profession et la fonction de son utilisateur. Les informations produites par la police scientifique et par le tribunal ne sont pas censées pouvoir être consultées par les employées de l'État civil. La base de données autorise donc des accès différenciés, en fonction de l'identité de la personne y accédant. Seuls les membres de l'équipe RFL ont accès à sa totalité. Un tel accord ne donne pas toute licence en matière d'utilisation des données : « *pour accéder à des données plus en profondeur, il faut un protocole, ce cadre de protection des données, parce que moi quand je vais avec les collègues de Catane, quand on va voir les données qui concernent le mort, on accède parfois à des témoignages, chez la police, ou des données qui concerne le mort, et d'autres personnes, des proches, des familles, etc., donc à ce moment-là,*

---

« The Italian Red Cross in Catania has signed a MoU with the Municipality and the Procura (the Office of the Public Prosecutor) to gather forensic information. This includes mapping cemeteries in Catania, and cross-referencing gravesites with missing persons reports from relatives (Catania Today, 2018). » Comune, protocollo con la Croce Rossa per dare un nome ai migranti morti, *Catania Today*, 20/03/2018 https://www.cataniatoday.it/cronaca/comune-protocollo-migranti-croce-rossa-20-marzo-2018.html

[2044] IOM," Improving data on missing migrants, Fatal Journey", Vol.3 Part 1, 2017 http://www.statewatch.org/news/2017/sep/iom-fatal-journeys-vol-3-1-missing-migrant-data-9-17.pdf

ROBINS, Simon, « Analysis of Best Practices on the Identification of Missing Migrants Implications for the Central Mediterranean, central mediterranean route thematic » report series, issue n° 2,2018https://publications.iom.int/system/files/pdf/identification_of_missing_migrants.pdf

[2045] FURRI Filippo, KOBELINSKY Carolina, « Donner un nom aux morts en Méditerranée : l'expérience de Catane », *Plein droit*, 2023/2 (n° 137), p. 19-22. DOI : 10.3917/pld.137.0021

CARAYON Lisa, KOBELINSKY Carolina, « Mourir. Puis disparaître ? », *Plein droit*, 2023/2 (n° 137), p. 3-5. https://www-cairn-info.ezproxy.utc.fr/revue-plein-droit-2023-2-page-3.htm

[2046] KOBELINSKY, Carolina, FURRI, Filippo, *Relier les rives, sur les traces des morts en Méditerranée*, Paris : La Découverte, 2024,p.129

*moi je dois considérer d'un côté comment je peux utiliser ces informations, qui concernent les corps, les morts, et son entourage ponctuel, les gens qui étaient autour de lui au moment du naufrage, les survivants, et aussi l'entourage relationnel, la famille, la personne chez qui ils allaient »* « *Tu rentres dans un domaine où les informations personnelles, on n'est plus en train de parler des informations personnelles du mort, mais on parle d'un deuxième cercle d'information, qui est connecté à la personne décédée, mais qui concerne des tiers, des personnes qui sont surement vivantes. Moi j'ai souvent des informations de personnes, bah je ne sais pas qui c'est, mais qui pourraient me dire qui est la personne décédée. Est-ce que j'ai le droit, est-ce que je peux, comment contacter cette personne pour pouvoir avoir une collaboration de leur côté, est-ce que l'institution peut le faire, est-ce que des réseaux informels peuvent le faire ? »*[2047]

## § 2 — Base de données forensique et protection des données

La base de données de Catane est une initiative présentée comme inédite, certes très localisée, mais qui a permis une première centralisation d'informations jusqu'alors dispersées. C'est aussi le souhait d'un bon nombre d'acteurs et organisations impliqués dans l'identification des morts et des disparus, appelant à poursuivre un effort de mise en commun des données à l'échelle nationale, voire internationale. Le désir d'atteindre un tel objectif est partagé par le Labanof[2048], l'ICRC, l'IMCP[2049], Interpol, l'Organisation internationale des migrations (OIM)[2050] ou le groupe de travail de l'ONU sur les disparitions forcées[2051]. Ces derniers plaident, chacun à leur manière, pour une amélioration de la coopération entre acteurs impliqués pour systématiser les échanges d'information, faciliter l'accès aux bases de données existantes, ou créer des bases de données régionales ou internationales[2052]. Un

---

[2047] Entretien n°36, identification des morts n°8, 21/05/2020

[2048]CATTANEO,M. TIDBALL BINZ, M., PENADOS,L., PRIETO, J., FINEGAN, O., GRANDI, M., "The forgotten tragedy of unidentified dead in the Mediterranean", *Forensic Science International*, Volume 250, 2015, Pages e1-e2,
CATTANEO, C., DE ANGELIS, D., MAZZARELLI, D. *et al.* "The rights of migrants to the identification of their dead: an attempt at an identification strategy from Italy". *Int J Legal Med,* 2023*,* 137,p. 145–156 https://doi.org/10.1007/s00414-022-02778-1

[2049] PARSONS, Thomas, HUEL, Rene, BAJUNOVIC, Zlatan, "Large scale DNA identification : The ICMP experience", *Forensic Science International: Genetics,* 38-2019, p. 236-244

[2050] "In all situations, research and reporting have generally confirmed the need to improve how bodies are cared for, recorded and "managed" to ensure that burial practices respect both the right to dignity and the religious beliefs of the dead, as well as create a system of centralized data collection, regionally, nationally and locally" ;« Dans toutes les situations, les recherches et les rapports ont généralement confirmé la nécessité d'améliorer la façon dont les corps sont pris en charge, enregistrés et « gérés » afin de garantir que les pratiques funéraires respectent à la fois le droit à la dignité et les croyances religieuses des défunts, et de créer un système de collecte centralisée des données, aux niveaux régional, national et local » « Identification and tracing of dead and missing migrants », IOM, Fatal journeys, Volume 2, 2016, https://publications.iom.int/system/files/pdf/fataljourneys_vol2.pdf

[2051]« il peut exister plusieurs bases de données, souvent situées dans différents pays, qui contiennent des informations pertinentes, mais qui n'offrent pas d'interopérabilité, notamment parce qu'elles ne suivent pas de critères harmonisés en ce qui concerne les données collectées, ce qui finit par faire échouer les tentatives de recherche. »
« Nouvelles technologies et disparitions forcées », Rapport du Groupe de travail sur les disparitions forcées ou involontaires, septembre-octobre 2023 A/HRC/54/22/Add.https://www.ohchr.org/sites/default/files/2024-04/A-HRC-54-22-Add-5-FR.pdf

[2052] VAN LAMMEREN, Sylvie, VON KONIG, Florian, "Missing migrants and their families: a call for greater international cooperation", *Forced migration review*, n°66, March 2021 https://www.fmreview.org/sites/fmr/files/FMRdownloads/en/issue66/vanlammeren-vonkoenig.pdf
ICRC, "Guidelines on Coordination and Information-Exchange Mechanisms for the Search for Missing Migrants", November 2021 https://www.icmp.int/wp-content/uploads/2021/10/ICRC-Missing-Migrants-Mechanism-Guidelines.pdf

argument mobilisé en faveur de la création d'une telle base de données concerne le caractère international du travail d'identification. Les victimes d'un même naufrage pouvant être retrouvées sur le territoire de plusieurs pays[2053]. Sans compter le fait que les familles peuvent être elles-mêmes dispersées entre plusieurs États. Cela légitimerait la création de « banques de données forensiques » à l'échelle régionale (Européenne par exemple), ou bien l'amélioration de l'interopérabilité entre bases de données nationales.

Mais ce type d'initiative pose question. Tout d'abord, certains de nos enquêtés s'interrogent sur le mode de gouvernance de telles bases de données : « *Je ne sais pas s'il doit y avoir une seule base de données globale, et si c'est le cas, qui la détiendrait ? Il devrait s'agir d'une base de données approuvée par les Nations unies et financée par eux, oui, un pays ne pourrait pas la détenir. »*[2054] D'autres enquêtés s'interrogent plutôt sur la faisabilité technique d'une base de données centralisée en l'absence d'une standardisation des pratiques : « *La création d'une base de données européenne n'a aucun sens si les bases de données nationales ne sont pas en place. Il s'agit en effet d'un grand nombre de pays, avec des méthodes de collecte d'informations et des lois différentes. Il faut aligner tous les pays avant de créer une base de données européenne. Même s'ils essaient de le faire, cela prendra des années et des années parce qu'il y a beaucoup de variations entre les pays, à quel point il faut aligner le cadre juridique. Je pense que le meilleur moyen est de commencer au niveau national, parce que le plus gros problème, c'est que les données sont collectées, mais qu'elles ne sont pas normalisées.* » [2055]

Et surtout la création d'une telle base de données soulève un bon nombre de questions en matière de vie privée. En effet, une grande partie des informations stockées dans les bases de données forensiques sont génétiques[2056], soit des informations particulièrement sensibles[2057]. Le régime de vérité de la médecine légale repose traditionnellement sur de ce type de données[2058]. Filippo Furri rappelle que le terme d'identification a différents sens, selon qu'on ait affaire à une identification visuelle, faite par les familles, ou judiciaire (grâce aux données ADN notamment). Le chercheur oppose mémoire subjective et traces objectives[2059]. L'ADN est

---

[2053]TERVONEN, Taina, *Au pays des disparus*, Fayard, 2019, 256 p.

[2054] "I don't know if it should be one global database, and if there is a global database, who would hold it? It should be an UN approved and resourced, yes you couldn't have a country holding it." Entretien n° 24, identification des morts n° 3, 20/03/2020

[2055] "There is no sense to create an European database if the national database are not in place. Because we are talking about many countries there, with different ways of collecting information, different laws. You must align all countries before create an European database. Even they try to do it, it gonna take years and years because there is a lot of variation between countries, how fare you have to align the legal framework. I think the best way is to start at the national level, and start there, because the biggest problem, data is collected, but it is not standardized way, if you find a standardized way of collecting data…"Entretien n° 23, identification des morts n° 2, 17/03/2020

[2056] WHITE, Thomas, LEE, Steven, "Forensic Genetics, Ethics, Privacy, and Public Policy", in: ERLICH, Henry, STOVER, Eric, WHITE, Thomas (eds), *Silent Witness: Forensic DNA Evidence in Criminal Investigations and Humanitarian Disasters*, New York, Oxford Academic, 2020
KATSANIS HUSTON, Sara, "Re-thinking international missing persons DNA databases"https://www.promega.com/-/media/files/products-and-services/genetic-identity/ishi-27-oral-abstracts/12-katsanis.pdf

[2057] Citons par exemple la déclaration de l'UNESCO sur les données génétiques humaines : les données génétiques collectées au cours d'une investigation criminelle doivent être détruites lorsqu'elles ne sont plus nécessaires. La déclaration sur les génomes humains et les droits humains établit que « les données génétiques associées à une personne identifiable et stockée ou traitées pour des finalités de recherches ou pour toutes autres finalités doivent être conservées de manière confidentielle, selon les conditions fixées par la loi. (article 7). https://www.ohchr.org/fr/instruments-mechanisms/instruments/universal-declaration-human-genome-and-human-rights

[2058] TOOM, V., WIENROTH, M., M'CHAREK, A. (Eds.), *Law, Practice and Politics of Forensic DNA Profiling: Forensic Genetics and their Technolegal Worlds*, Routledge, 2022, 272 p.

[2059] KOBELINSKY, Carolina, FURRI, Filippo, *Relier les rives, sur les traces des morts en Méditerranée*, Paris : La Découverte, 2024, 194 p.

souvent perçu comme la « reine des preuves ». Ainsi, un médecin légiste dans l'ouvrage de la journaliste Taina Tervonen fait remarquer que « le plus gros problème est le peu d'informations disponibles. Les familles habitent souvent dans des villages éloignés et ne possèdent que rarement des photos des disparus. Il n'y a ni archives dentaires ni registre médical. La seule chose vraiment fiable dont on dispose, c'est l'ADN. »[2060] Rappelons toutefois que l'ADN n'est pas toujours disponible, tout simplement parce qu'il n'est pas toujours possible de contacter les familles. Mais malgré tout, un certain nombre d'acteurs continuent, dans une certaine mesure, d'accorder une importance centrale à ce type de données. C'est par exemple le cas de l'International commission on missing persons » (ICMP). L'utilisation de données génétiques par l'organisation remonterait à la fin des années 1990, à la suite des conflits ayant ravagés les Balkans. Cette période correspond à la généralisation de l'usage de l'ADN en médecine légale [2061] , et l'organisation se présente elle-même comme une précurseure concernant son application dans l'identification des morts de masse[2062]. Depuis, l'ICMP a ainsi opéré différentes opérations de collecte de masse de données génétiques, dans des contextes de post-conflits, en Bosnie donc, mais aussi en Irak, en Libye, en Chypre. L'ICMP a recouru à des données génétiques dans le cadre d'enquêtes portant sur des disparitions politiques (Chili, Colombie, Afrique du Sud, Albanie, et Brésil), ou lors de catastrophes naturelles (Tsunami de 2004, Katrina). D'après l'ICMP, sa base de données contiendrait à la date de 2019 jusqu'à 100 000 références génétiques familiales [2063]. Concernant les migrants, dès 2013, l'organisation propose de lancer un programme d'identification génétique des disparus et des morts en mer Méditerranée, en coordination avec l'OIM[2064]. L'ICMP a aussi pu conduire en 2018, en 2019 et en 2021 différentes entrevues avec des pays méditerranéens

[2060]TERVONEN, Taina, *Au pays des disparus*, Fayard, 2019, p.26

[2061]C'est aussi le début des bases de données policières génétique. La base de donnée des services de police britannique date de 1995 ;la France créé en 1998 le fichier national des empreintes génétiques, la même année le FBI a créé CODIS (Combined DNA Index System).
VAILLY, Joelle, *ADN Policier*, Presses universitaires de France, 2024, 264 p.
VAILLY, Joelle, *the Birth of a Genetics Policy social issues of newborn screening*, Routledge, 2014, 228 p.

[2062]« Les tests d'ADN pour l'identification humaine sont aujourd'hui utilisés dans les laboratoires de police scientifique du monde entier et sont peut-être connus de nombreuses personnes grâce aux séries policières télévisées. Cependant, la situation n'avait rien de routinier en 1999 lorsque la CIPD a commencé à envisager l'utilisation de l'identification par l'ADN pour aider à identifier certaines des 40 000 personnes disparues à la suite des conflits dans l'ex-Yougoslavie. À l'époque, on ne savait pas si les tests ADN pouvaient être appliqués à grande échelle dans un tel contexte ». "DNA testing for human identification is today used in forensic laboratories around the world, and may be familiar to many people through popular TV detective shows. However, there was nothing routine about the situation in 1999 when ICMP began to consider the use of DNA identification to help identify some of the 40,000 people missing as a result of the conflicts in the former Yugoslavia. At that time, it was not known if DNA testing could be applied on a massive scale in such a context." PARSONS, Thomas, "DNA led-human identification", https://www.icmp.int/news/dna-led-human-identification/

[2063] PARSONS, Thomas, HUEL, Rene, BAJUNOVIC, Zlatan, RIZVIC, Adnan, « large scale DNA identification : The ICMP experience », *Forensic science international : Genetics*, n° 38, 2019, p. 236-244
KLEISER, Andreas, PARSONS, Thomas J., "Large Scale Identification of the Missing: Experiences and Perspectives of the International Commission on Missing Persons", in : ERLICH, Henry, STOVER, Eric Stover, WHITE,Thomas (eds), *Silent Witness: Forensic DNA Evidence in Criminal Investigations and Humanitarian Disasters*, Oxford University Press, 2020

[2064]" Last year, ICMP and IOM signed a cooperation agreement that aims to draw on ICMP's long experience in using DNA testing to trace the missing and its sizeable database of reference and victim profiles and align this with IOM's presence in origin countries where it could collect missing person information and DNA samples." "Better management of dead and missing migrants needed in Europe", *The New humanitarian*, 28/07/2014https://www.thenewhumanitarian.org/analysis/2014/07/28/better-management-dead-and-missing-migrants-needed-europe
IOM, "Counting the missing migrants"https://weblog.iom.int/counting-missing-migrants
ICMP, "ICMP and IOM co-host inter-agency meeting on missing migrants", 14/12/2016
https://www.icmp.int/news/icmp-and-iom-co-host-inter-agency-meeting-on-missing-migrants/

(l'Italie, la Grèce, Malte, Chypre, l'Espagne, et plus récemment la Libye[2065]) afin de s'accorder sur des mécanismes de coopération et d'échange à l'échelle régionale, ainsi que l'éventuelle création d'une base de données commune[2066]. Sa mise en œuvre n'est pas à l'ordre du jour en 2024. La coopération entre l'ICMP et les pays de la Méditerranée est réduite pour le moment à du soutien logistique ponctuel en matière de gestion de collecte de données génétiques. Cela put être le cas en juillet 2023 pour un naufrage en Grèce[2067]. Sachant que le traitement de telles données pour un public vulnérable et criminalisé posent évidemment question.

## §3 — Volet policier et humanitaire de l'enquête

D'autant que peuvent intervenir dans le processus d'enquête des forces de l'ordre, car une partie du mandat des autorités de police porte bien souvent sur les personnes disparues[2068]. Un bon nombre de bases de données forensiques sont sous la responsabilité des forces de l'ordre. Elles sont rattachées soit aux ministères de la Justice (comme c'est le cas en Grèce) [2069]ou de l'Intérieur (comme c'est le cas en Italie)[2070].

---

[2065] ICMP,"The International Commission of Missing Persons and Libyan Judicial Expertise Center, Representing Ministry of Justice and Permanent Technical Committee on Mass Graves and Missing Migrants, Sign Technical Cooperation Agreement", 27/06/2023 https://www.icmp.int/news/icmp-and-libyas-center-for-judicial-expertise-sign-cooperation-agreement/
ICMP,"Libyan Experts Visit ICMP to Advance Work On Locating Missing Migrants & Other Missing Persons", 27/06/2023 https://www.icmp.int/news/libyan-experts-visit-icmp-to-advance-work-on-locating-missing-migrants-other-missing-persons/

[2066] Developing a Joint Process on the Issue Of Missing Migrants in the Mediterranean Region, 11/06/2018 https://www.icmp.int/press-releases/developing-a-joint-process-on-the-issue-of-missing-migrants-in-the-mediterranean-region/
ICMP, "statement on the issue of missing migrants by representatives of Cyprus, Greece, and Malta at the conclusion of the 2nd meeting of the joint process 13 june 2019" https://www.icmp.int/wp-content/uploads/2019/06/icmp-gr-mm-047-3-doc-joint-statment-2nd-meeting-of-the-joint-process-geconverteerd.pdf
ICMP,"statement on the issue of missing migrants by representatives of Cyprus, Greece, and Malta at the conclusion of the 3 rd meeting of the joint process", Athens, 19 November 2021 https://www.icmp.int/wp-content/uploads/2021/11/icmp-gr-mm-084-3-doc-statement.pdf
ICMP, Missing Migrants and refugees program https://www.icmp.int/wp-content/uploads/2020/12/Missing-Migrants-Program-Factsheet-English.pdf

[2067] ICMP, "Mediterranean States Can Access Forensic Capacity And Expertise to Locate and Identify Missing Migrants", 05/07/2023 https://www.icmp.int/news/mediterranean-states-can-access-forensic-capacity-and-expertise-to-locate-and-identify-missing-migrants/
ICMP, "Act Now to Save Lives and Prevent Migrants From Going Missing", 07/03/2022 https://www.icmp.int/press-releases/20931/

[2068] https://www.service-public.fr/particuliers/vosdroits/F31558
https://www.interno.gov.it/it/ministero/commissari/commissario-straordinario-governo-persone-scomparse

[2069] "The laboratory is the first to deal with cases requiring DNA analysis and cooperates with judicial authorities as well as the Police and Lesbos Coroner -the same applies to all other Coroners in Greek territory, in charge of violent deaths. All the DNA samples of migrant bodies found, both identified and unidentified, are sent, stored and indexed in this laboratory. There is no general law provision or internal regulation providing for the future use of the sample, as there is for the Directorate of Criminal Investigations – see below, but the Director has introduced an electronic system to compare automatically every "new arrival" of DNA sample with the existing ones. This database is at the disposal of every migrant who refers to Greek Police or Interpol in search of missing persons." KERASIOTIS,Vassilis, SPILIOTAKARA,Maria, "Missing and Dead Migrants at Sea: The legal framework in Greece", OIM, September 2016 https://missingmigrants.iom.int/sites/g/files/tmzbdl601/files/publication/file/Mediterranean-Missing-Greek-legal-memo.pdf
VOULTSOS, Polychronis, NJAU, Samuel,TAIRIS, Nikolaos, PSAROULIS, Dimitrios, KOVATSI, Leda, « Launching the Greek forensic DNA database. The legal framework and arising ethical issues », *Forensic Science International : Genetics*, Volume 5, Issue 5,2011,p. 407-410

[2070] " When a missing person is reported, the judicial police, if it considers necessary, will collect information about the missing person and any personal effects in order to obtain a DNA profile. The blood relatives can be asked to provide a biological sample on a voluntary basis. In this case the DNA profile of the blood relative is kept in a special section of the Database. This is done by the Police laboratories or by other laboratories of 'highly specialized' institutions. The DNA profile is then loaded into the Central Database by order of the judicial authority. If the analysis of the sample was conducted by the laboratory of a specialized institution, the upload is made by the Police laboratory specified

Le travail d'identification des morts comprend donc potentiellement un volet policier. Tout d'abord, il faut rappeler que les échanges de données stockées dans ces bases de données génétiques nationales se font via les mécanismes instaurés par le traité de Prüm. Initialement, ce dernier concernait les enquêtes criminelles, notamment en matière de contreterrorisme. Mais son champ d'application a été élargi. En effet, depuis l'adoption de Prüm II en février 2024, le traité couvre aussi les enquêtes portant sur des personnes déclarées disparues, sur des corps non identifiés, ainsi que sur des victimes de catastrophes naturelles[2071]. Une telle extension des finalités du mécanisme de Prüm n'a pas manqué d'alerter les organisations de défense des droits de l'homme [2072]. Ces dernières s'inquiètent des risques associés au brouillage entre finalité humanitaire et sécuritaire. D'autant qu'un autre acteur peut intervenir dans le cadre d'échange de données génétiques à des finalités d'identification des personnes disparues : Interpol.

Une partie du mandat d'Interpol concerne les enquêtes pénales internationales relevant des cas de disparitions ou de corps non identifiés. L'organisation a mis en place un vaste système d'information dédié aux disparus et accorde une importance particulière à la gestion des données génétiques. Sa base de données ADN date de 2002, mais une base de données génétique dédiée aux disparues a été constituée en 2021 (I-Familia) [2073]. Interpol présente son action comme étant caractérisée par une finalité humanitaire. Il faut noter qu'Interpol est déjà plus largement intervenu à des fins d'identification de victimes de catastrophe, parfois en coopération avec le CICR. Les deux organisations peuvent échanger sur les standards à

---

by the judicial authority."ROMANO, Serena, "The Italian legal framework for the management of missing persons and unidentified dead bodies, and the rights of the relatives", OIM, September 2016https://missingmigrants.iom.int/sites/g/files/tmzbdl601/files/publication/file/Mediterranean-Missing-Italian-legal-memo.pdf

[2071] « Lorsque les États membres souhaitent recourir au cadre Prüm II pour rechercher des personnes disparues et identifier des restes humains, ils devraient adopter des mesures législatives nationales pour désigner les autorités nationales compétentes à cet effet et pour fixer les procédures, conditions et critères spécifiques à cet effet. En ce qui concerne les recherches de personnes disparues en dehors du domaine des enquêtes pénales, les mesures législatives nationales devraient clairement indiquer les motifs humanitaires pour lesquels une recherche de personnes disparues peut être effectuée. Ces recherches devraient respecter le principe de proportionnalité. Les motifs humanitaires devraient inclure les catastrophes naturelles ou d'origine humaine ainsi que d'autres motifs tout aussi justifiés, tels que les soupçons de suicide. » Résolution législative du Parlement européen du 8 février 2024 sur la proposition de règlement du Parlement européen et du Conseil relatif à l'échange automatisé de données dans le cadre de la coopération policière («Prüm II»), modifiant les décisions 2008/615/JAI et 2008/616/JAI du Conseil et les règlements (UE) 2018/1726, 2019/817 et 2019/818 du Parlement européen et du Conseil (COM(2021)0784(COR1) – C9-0455/2021 – 2021/0410(COD) https://www.europarl.europa.eu/doceo/document/TA-9-2024-0073_FR.html

European Parliament "Police co-operation: MEPs adopt law on more efficient data exchanges", News, Press Release 08/02/2024 https://www.europarl.europa.eu/news/en/press-room/20240202IPR17321/police-co-operation-meps-adopt-law-on-more-efficient-data-exchanges

[2072] "We have concerns, therefore, about the inclusion of identifying missing persons or identifying unknown remains. Whilst missing persons and unknown remains may have links to serious cross-border crimes, there are also many circumstances where they will not. The indiscriminate inclusion of 'missing persons and unidentified human remains' (Article 2) in Prüm II thus lacks a specific legal basis. Its broad scope and lack of specificity also creates serious risks of over-use and abuse." »nous sommes donc préoccupés par l'inclusion de l'identification des personnes disparues ou de l'identification des dépouilles inconnues. Si les personnes disparues et les dépouilles inconnues peuvent avoir un lien avec des crimes transfrontaliers graves, il existe également de nombreuses circonstances où ce n'est pas le cas. L'inclusion sans discernement des « personnes disparues et des restes humains non identifiés » (article 2) dans le projet de loi Prüm II n'a donc pas de base juridique spécifique. Son large champ d'application et son manque de spécificité créent également de sérieux risques de sur-utilisation et d'abus ». EDRI, "Respecting fundamental rights in the cross-border investigation of serious crimes A position paper by the European Digital Rights (EDRi) network on the European Union's proposed Regulation on automated data exchange for police cooperation ("Prüm II")", September 2022https://edri.org/wp-content/uploads/2022/10/EDRi-position-paper-Respecting-fundamental-rights-in-the-cross-border-investigation-of-serious-crimes-7-September-2022.pdf

[2073] Interpol, « INTERPOL unveils new global database to identify missing persons through family DNA », 21/06/2021 https://www.interpol.int/News-and-Events/News/2021/INTERPOL-unveils-new-global-database-to-identify-missing-persons-through-family-DNA

« I-Familia : identifier les personnes disparues dans le monde entier par la recherche ADN en parentalité », Forenseek, 09/02/2022 https://www.forenseek.fr/i-familia-identifier-les-personnes-disparues/

appliquer en la matière. Et c'est à Interpol qu'une famille d'un exilé peut s'adresser en cas de demande d'enquête pour disparition. Un de nos enquêtés nous résume la procédure à suivre : *« Si Interpol est impliqué, c'est une demande du pays, si une famille manque quelqu'un, elle doit se rendre à l'ambassade de son pays ou à la police pour établir un profil ADN, ou un formulaire de personne disparue. C'est la première étape, il y a toujours un acteur officiel. La Grèce, par exemple, ne peut accepter aucun échantillon d'ADN provenant de l'étranger et émanant d'une organisation autre que la police, l'ambassade ou le ministère des Affaires étrangères. La famille doit donc accepter de rencontrer les autorités. Dans la plupart des cas, c'est Interpol qui est impliqué dans l'échange d'informations. Mais par exemple en Afrique, en Érythrée, la famille compte sur les ONG pour faire ce travail (…). Les autorités ne sont pas concernées.* »[2074] En outre Interpol coopère avec l'ICMP depuis 2007[2075]. Interpol et l'ICMP ont pu organiser des réunions courant 2019 sur l'opportunité d'échanges de données génétiques de migrants dans le cadre d'enquêtes sur des personnes déclarées disparues notamment via le projet Flyway d'Interpol[2076]. Ce projet relève toutefois d'une approche sécuritaire : la mort des migrants et leur disparition ne sont plus dues aux politiques répressives des États, mais aux réseaux criminels et aux passeurs[2077].

Et il est évident pour certains de nos enquêtés que l'implication d'Interpol inquiète et fait écho à la criminalisation des exilés dont les empreintes alimentent les bases de données biométriques pléthoriques[2078]. Le mandat policier d'Interpol laisse craindre une réutilisation potentielle de son implication pour servir des objectifs sécuritaires *: « Donc faisons, moi je suis Interpol. Un acteur qui a intérêt à gérer la migration mondiale, qui m'empêcherait d'utiliser la nécropolitique pour faire de la biopolitique ?* » [2079] Citons aussi un coordinateur des opérations de médecine légale du CICR qui remarque que « si Interpol a confirmé sa volonté de contribuer à combler le fossé entre les deux principales sources de données d'identification, à savoir les autorités policières locales et les organisations humanitaires telles que le CICR ou l'Organisation internationale pour les migrations (OIM), certains problèmes subsistent. Pour Interpol, les informations doivent être collectées par la police, qui est formée à cette tâche,

---

[2074] If Interpol is involved it is a request from the country, if a family is lacking somebody, they have to go to an ambassy of their country or a police to profile DNA, or missing person form. That 's in the initial step, there is always an official actor. For example the Grece, can't accept any DNA sample from abroad from any organization other than police, or ambassy, or foreign affair ministry. So a family must agree to see authorities. So Interpol is involved in intermediaire. The ambassy can be involved. In most case, it is interpol which is involved in the sharing of information. But for example in Africa, Erythrea, family rely on NGO, to do that work, the Red Cross. Erythrea the best solution is to use red cross network to share information. Authoroties are not in the picture; it is not possible to use the interpol network, or the ambassies, whitout risking. This is the biggest issue." Entretien n°23, identification des morts n°2, 17/03/2020

[2075]ICMP, "Co-operation agreement between the International commission on missng persons (ICMP)an The international criminal police organization- Interpol", 2007 https://www.icmp.int/wp-content/uploads/2014/08/cooperation-agreement-icmp-and-interpol.pdf

[2076] ICMP, "ICMP and INTERPOL Convene Expert Meeting On DNA Analysis and Missing Migrants",21/11/2019
https://www.icmp.int/press-releases/icmp-and-interpol-convene-expert-meeting-on-dna-analysis-and-missing-migrants/
Le projet FLYWAY, amorcé en 2017, est une initiative d'INTERPOL visant à lutter contre la traite des êtres humains et le trafic de migrants en Afrique de l'Ouest et du Nord.

[2077] PIQUET, Agathe, « Europol et la "sécuritisation" des migrations irrégulières », *Migrations Société*, 2016/3 (N° 165), p. 131-150. 10.3917/migra.165.0131. https://www.cairn.info/revue-migrations-societe-2016-3-page-131.htm

[2078] WIENROTH, M., AMELUNG, N., "Crisis', Control, and Circulation: Biometric Surveillance in the Policing of the 'Crimmigrant Other'." *International Journal of Police Science and Management*, 2023, *25*(3), p. 297-312. https://doi.org/10.1177/14613557231184696
AMELUNG, Nina, "'Crimmigration Control' across Borders: The Convergence of Migration and Crime Control through Transnational Biometric Databases." *Historical Social Research / Historische Sozialforschung*, vol. 46, no. 3, 2021,p. 151–77. https://www.jstor.org/stable/27075121

[2079] Entretien n°36, identification des morts n° 8, 21/05/2020

plutôt que par le commun des mortels, afin de protéger les données. Pour le CICR, il est important que les informations soient collectées dans le but d'enquêter sur le sort des personnes disparues et sur le lieu où elles se trouvent. » [2080] L'instrumentalisation des « notices rouges » est régulièrement dénoncée[2081]. Il existe peu de littérature sur le sujet des « notices jaunes »[2082] et des « notices noires »[2083] dans un contexte de migration. Citons simplement un exemple documenté par Amnesty International. L'organisation a en effet alerté sur une tentative de rapatrier sur la base d'une notice jaune d'Interpol une exilée qui cherchait à fuir sa famille du fait de persécutions contre son activisme sur des enjeux LGBT[2084].

L'usage massif de données génétique pour l'identification de migrants ouvre évidemment une perspective biopolitique et fait écho aux modalités de surveillance policière des exilés [2085].L'implication d'acteurs comme Interpol et la place des données de type ADN fait craindre un potentiel croisement entre logique humanitaire (l'identification des corps, leurs rapatriements pour les familles) et policière (la surveillance des migrations). Ainsi la chercheuse Christina Oelgemöller met en regard la gestion de la migration illégale et celle des disparus et l'invisibilisation des morts : « La gestion des migrations fait appel à la technologie pour le contrôle des frontières et la gestion de l'identité, tandis que le nouveau régime des personnes disparues fait appel à la police scientifique et à la technologie de l'ADN. » [2086]Filippo Furri et Carolina Kobelinsky imaginent ainsi un scénario dystopique: chaque candidat à l'exil pour conjurer l'anonymat de la mort, devrait laisser ses données biométriques en amont, d'où un vaste fichage des vivants pour éviter la disparition post-mortem[2087].

---

[2080]"while Interpol has confirmed its willingness to help bridge the gap between the two main sources of identification data, i.e., local police authorities and humanitarian organizations like the ICRC or the International Organisation for Migration (IOM), some challenges still remain. For Interpol, information should be collected by the police who are trained in the task, rather than the common man, in order to safeguard the data. For the ICRC, it is important that information is collected for the purposes of investigating the fate and whereabouts of the missing." ICRC, « Missing migrants: Forensic experts from the Asia-Pacific region emphasize information-sharing », 24/08/2017https://www.icrc.org/en/document/missing-migrants-forensic-experts-asia-pacific-emphasize-upon-information-sharing

[2081] "Misuse of Interpol's European Parliament, Red Notices and impact on human rights – recent developments", directorate-general for external policies policy department,January2019 https://www.europarl.europa.eu/RegData/etudes/STUD/2019/603472/EXPO_STU(2019)603472_EN.pdf
"Dismantling the Tools of Oppression: Ending the Misuse of INTERPOL", Fairtrail, January 2022 https://www.fairtrials.org/app/uploads/2022/01/Dismantling-the-tools-of-oppression.pdf

[2082] Des notices dédiées aux disparus

[2083] Des notices dédiées aux corps non identifiés

[2084] Amnesty International, « Lebanon: imminent involuntary repatriation of a refugee victim of Interpol abuse », 25/12/2021https://www.amnesty.org.au/lebanon-imminent-involuntary-repatriation-of-a-refugee-victim-of-interpol-abuse/

[2085]SMITH, L. A. « The missing, the martyred and the disappeared: Global networks, technical intensification and the end of human rights genetics ». *Social Studies of Science*, 2017, *47*(3), 398-416. https://doi.org/10.1177/0306312716678489
MACHADO, Helena, GRANJA, Rafaela, *Genetic surveillance and crime control, social, cultural and political perspectives*, Routledge, 2022, 406 p.
"missing people, DNA analysis and identification of human remains A guide to best practice in armed conflicts and other situations of armed violence, Protecting Genetic Privacy in Biobanking through Data Protection Law" ICRC, 2009 https://www.icrc.org/en/doc/assets/files/other/icrc_002_4010.pdf
HALLINAN, DARA, *Protecting Genetic Privacy in Biobanking through Data Protection Law,* Oxford University Press, 2021, 320 p.
TUAZON, Oliver, "Universal forensic DNA databases: acceptable or illegal under the European Court of Human Rights regime?", *Journal of Law and the Biosciences*, Volume 8, Issue 1, 2021, https://doi.org/10.1093/jlb/lsab022
TUAZON O.M, ZWENNE G.J., "DNA Profile Data and Right to Privacy", In: WILLEMSEN C. (Ed.) *Four decades of information technology and innovation: academics and experts look back and forward at the developments in their field.* 2021 P.19-27.

[2086]« migration Management uses technology in its border control and identity management,whilst the newly evolving missing persons regime uses forensic and DNA technology. » OELGEMÖLLER, C."The Illegal, the Missing: an Evaluation of Conceptual Inventions", *Millennium*, 2017, *46*(1), p.24-40. https://doi.org/10.1177/0305829817708812

[2087] KOBELINSKY, Carolina, FURRI, Filippo, *Relier les rives, sur les traces des morts en Méditerranée*, Paris : La Découverte, 2024, 194 p.

Le recours aux données génétiques impliquerait donc, dans de nombreux cas, de rentrer dans une logique d'enquête policière et d'interagir avec des acteurs des forces de l'ordre. Cela ne va évidemment pas sans risques pour les familles, comme nous le fait remarquer un médecin légiste : « *lorsque vous établissez le profil d'un échantillon d'ADN, celui-ci peut être envoyé au laboratoire de la police. C'est la principale préoccupation. Pouvons-nous faire confiance aux autorités pour ne pas utiliser ces données à d'autres fins ? En Italie, un accord a été signé avec cinq pays pour partager les données ADN afin d'identifier les terroristes. Avec le Nigeria, la Tunisie, le Maroc, l'Italie, etc., et bien sûr, si un parent disparaît et que l'Italie établit un profil ADN, comment pouvons-nous savoir que l'ADN n'est utilisé qu'à des fins d'identification et qu'il n'est pas partagé avec d'autres pays pour voir si la personne est morte ou si elle figure sur la liste des terroristes, ou, etc., etc. Quel type de données partagez-vous ? Et comment protéger ces données pour s'assurer qu'elles ne seront pas utilisées à d'autres fins ? Car vous pouvez mettre la famille en danger*. »[2088]

Que faire alors ? Comment minimiser de tels risques ? Certains enquêtés surlignent qu'il est à minima important d'informer les familles sur les procédures « *Il faut expliquer aux familles comment fonctionne le système et quels sont les risques. Certaines familles peuvent être prêtes à prendre plus de risques que d'autres quant à l'utilisation des informations, sachant ce qui est en jeu. Elles cherchent désespérément l'être aimé. Mais il est important qu'elles puissent prendre des décisions en connaissance de cause et les réexaminer au fur et à mesure que l'enquête progresse*. »[2089] Et effectivement, d'après un enquêté, certains exilés ne seraient pas prêts à prendre le risque de contacter des acteurs policiers pour retrouver une personne potentiellement décédée : « *moi à plusieurs reprises j'ai pu entendre directement ou indirectement, pourquoi je devrais moi aller à la police pour parler d'une personne qui est morte ? Est-ce que ça vaut la… le prix, les risques ?* » [2090]

Donc pour que le travail d'identification puisse avoir lieu, il est nécessaire de pouvoir garantir une gestion sécurisée de l'information et préserver une séparation entre la dimension « policière » et la dimension « humanitaire » de l'investigation. Comme le déclare un enquêté : « *en Italie, tout le protocole avec Cattaneo[2091], part du présupposé que tu vas tout faire avec de l'ADN, alors que toutes les informations ne sont pas mobilisées pour collecter les familles, pour faire les matching ante-mortem, post-mortem, il faut aller les chercher, et si tu veux aller les chercher avec le ministère des Affaires étrangères et Interpol, les familles, elles ont pas*

[2088] "When you profile a DNA sample, it can go to the police lab. It is the main concern. Can we trust the authorities not to use these data for other purposes? In Italy they signed an agreement with 5 countries to share DNA data to identify terrorists. With Nigeria, Tunisia, Marocco, Italy, etc. and of course if someone is missing a relative, and Italy profile DNA, how do we know that DNA is only use for identification purpose and not share with other countries to see if the person is dead or is in the terrorist list, or etc. , etc. So what kind of data do you share? And how to protect these data to be sure that it wont be use for other purpose? Because you can put the family in danger." Entretien n°23, identification des morts n° 2, 17/03/2020

[2089]« It has to be explained to families how the system works, what the risks are. Some families may be willing to take more risk about the use of information than others, knowing what is at stake. They are looking desperately for loves one. But it is important that they can make informed decisions and review as the investigation progresses » Entretien, identification des morts n°2, 20/03/2020

[2090] Entretien n°36, identification des morts n°8, 21/05/2020

[2091] Cristina Cattaneo, directrice d'un laboratoire de médecine légale de Milan (le Labanof), impliquée dans l'identification des morts en mer méditerranée.

*particulièrement envie de ça, il faut trouver un moyen de les contacter de façon plus souple, moins agressive, plus en confiance, chose que malheureusement la perspective policière n'a pas toujours* »[2092] Pour l'enquêté, ce rôle de « part feu » pourrait être incarné par le CICR : « *L'ICRC est le seul acteur qui peut faire… coupe-feux. Tu as une série de barrières et de coupe-feux. L'État peut dialoguer avec l'ICRC, car l'ICRC protège les données d'un usage détourné de ces données, que l'État pourrait faire de ces données. Après tu as les acteurs intermédiaires vis-à-vis des personnes de la migration, qui doivent créer un lien de confiance, et dire OK si nous on collecte des informations concernant des victimes, chez toi, moi je mets un filtre, pour qu'il y ait un vecteur unique pour faire arriver des informations, et pour avoir la garantie de la part de l'ICRC que les données collectées collatérales soient protégées et ne soient pas utilisées par des institutions, des États, à des finalités autres* » [2093] Le CICR surligne d'ailleurs l'importance du rôle d'ONG de la société civile pour garantir une gestion transparente des potentielles bases de données génétiques [2094] . Et l'organisation propose effectivement d'explorer la possibilité de servir d'intermédiaire pour gérer les échanges d'information entre les différents acteurs impliqués dans l'identification des morts[2095].

Théoriquement, les familles pourraient donc directement contacter le CICR pour lui confier des informations sensibles. Mais dans les faits, la circulation de l'information est beaucoup moins directe et passe par une nébuleuse d'acteurs et de collectifs. Tout d'abord, les familles elles-mêmes ne sont pas nécessairement informées des organisations à contacter, d'où le fait que certaines ONG, comme Boat4people, servent de relai en leur indiquant la marche à suivre : « *les activistes et les chercheurs ont essayé de donner aux familles et à tous les niveaux d'intermédiaires possibles, c'est-à-dire tous ceux qui les accompagnent, pourraient se présenter dans le scénario, des instruments pour aller vers des institutions qui pourraient les aider à faire leurs recherches, donc aider, aider pour que les autres les aide*.» [2096]

Ensuite, les membres d'ONG impliqués dans l'identification des morts vont eux-mêmes passer par un réseau d'ONG et permettre une circulation informelle de l'information, et rapprocher le CICR des familles : « *les acteurs informels, parce qu'ils sont moins contraints par des raisons juridiques, par des protocoles, etc., et parce qu'ils connaissent beaucoup mieux la dynamique et la situation de la migration, les réseaux informels, genre c'est plus facile de chercher, de façon informelle, quitte à passer ensuite de façon plus formelle, tu voix il y a des associations*

---

[2092] Entretien n°36, identification des morts n°8, 21/05/2020

[2093] Entretien n°36, identification des morts n°8, 21/05/2020

[2094] « The entity responsible for maintaining forensic biobanks and DNA profile databases should operate independently, albeit under the responsibility of the State and ensure civil society involvement. International human rights anfd international humanitarian law organizations can also be involved. With a view to ensuring a clear and transparent sample management policy, this entity must be regularly audited by an independent body duly competent in the field of genetics. »
"Guidelines for the use of forensic genetics in investigations into human rights and international humanitarian law violations", ICRC, December 2019
CICR, "Le processus d'identification forensique : une approche intégrée", 2022 https://www.icrc.org/fr/publication/4590-forensic-human-identification-process-integrated-approach

[2095]« The ICRC is exploring the possibility to act as a data orchestrator for data gathered by different states and organizations. It would allow to cleanse, analyze and classify this data in order to generate relevant answers in relation to the living and the dead. "CICR, "Counting the dead, how registered deaths of migrants in the southern European sea border provide only a glimpse of the issue", November 2020 https://missingpersons.icrc.org/sites/default/files/2022-11/COUNTING-THE-DEAD-FINAL.pdf

[2096]Entretien n°36, identification des morts n°8, 21/05/2020

*en France, en Italie, qui se positionne juste après les activistes, qui eux peuvent aller voir les institutions, c'est un travail de couture. J'ai une famille qui cherche, qui délègue un contact dans un autre pays, qui contacte une association, qui a des contacts avec une autre association, qui peut faire arriver l'information à une croix rouge française, ou à certaines personnes de la Croix rouge internationale pour que ça s'active*. « [2097] Ce même enquêté réfléchit à la manière dont peut être impliquée la diaspora dans le travail informel de collecte d'information. Mais cette étape de recherche est délicate, en raison de situations administratives complexes des membres de la diaspora.

Or ce travail de couture entre réseaux plus informels et organisations humanitaires est fondé sur la confiance. Et le principe de confidentialité joue un rôle essentiel dans la construction de cette dernière. Cela contrevient l'idée que la protection des données peut être perçue comme freinant le travail de couture et de transmissions d'organisation. Certes, de petites structures ne savent pas nécessairement comment partager de façon sécurisée les informations dont elles disposent avec les grosses ONG en raison d'un manque de maitrise des démarches juridiques. Un enquêté nous avoue ainsi que : « *j'ai peut-être des informations sur une famille dans laquelle le CICR est également impliqué et nous ne pouvons pas échanger d'informations, parce qu'il y a des obstacles en raison de la politique de protection des données qu'ils ont. C'est pour les grandes organisations, entre les petites organisations, c'est plus simple, par exemple si je veux partager des informations avec une autre ONG, je leur envoie simplement un e-mail et je leur dis OK, je suis à la recherche de cet homme ou de cette femme, est-ce que vous avez des informations, c'est plus informel*. »[2098]

Mais à contrario, la protection des données peut être considérée comme une précondition de la possibilité d'une recherche (et non pas un obstacle). Un enquêté nous raconte ainsi qu : « *la Croix rouge de Catane a refusé de partager des données de santé avec le ministère de la Santé, des données de migrants qui étaient accueillis à Mineo, dans le centre d'accueil. Moi quand j'ai un acteur comme l'ICRC ou la Croix rouge de Catane qui me donne des garanties, au niveau de la théorie et au niveau de la pratique. Je peux dire OK, allez-y, vous pouvez faire confiance, et donc je peux participer à créer un régime de confiance qui participe de la circulation informelle de l'information. Pourquoi les gens, s'il y a un naufrage, à Lampedusa… pourquoi ils contactent la croix rouge de Catane, et pas la croix rouge d'Agrigente ou la Croix rouge nationale italienne ? Pourquoi ils viennent nous voir, pour que l'on contacte l'ICRC ? Pourquoi ils vont voir l'ICRC ? Parce qu'il y a une doxa, un avis, des personnes en migration, qui savent qui est un acteur de confiance, et qui ne l'est pas*. »[2099]

---

[2097] Entretien n°36, identification des morts n°8, 21/05/2020

[2098] « I have maybe information about a family that ICRC is also involved in and we cant exchange information, because there are some obstacles because of data protection policy they have. it is for the big organizations, between smaller organizations, it is more simple for exemple if I want to share information to another NGO I am just emailed them and said ok I am looking for this man or for this woman do you have some information it is more informal. » Entretien n°23, identification des morts n°2, 17/03/2020

[2099] Entretien n°36, identification des morts n°8, 21/05/2020

§4 — Enquêtes des proches et risques numériques

Enfin, il ne faut pas oublier que les familles peuvent elles-mêmes mener leurs propres enquêtes. Cela peut se faire de façon conjointe aux organisations humanitaires comme le CICR ou de façon indépendante. Or les circuits de partages d'informations sont encadrés clairement selon une série de principes fixé par le CICR et le DIH. Traditionnellement, c'est aux familles de contacter l'organisation humanitaire qui va mener les différentes recherches afin de retrouver la trace des disparus. Le CICR communique ensuite le résultat des enquêtes aux proches. Et notons même que dans des cas bien spécifiques, le CICR ne transmettrait pas systématiquement l'ensemble des informations de l'enquête aux familles. Selon la chercheuse Anjli Parrin, le CICR pourrait pour des raisons de confidentialité ne pas délivrer tous les éléments sur la cause de la mort d'une personne, surtout dans des contextes conflictuels, impliquant plusieurs parties[2100]. Donc, les familles, dans ce cas, ne participent pas directement au processus de recherche. A contrario, des membres de l'armée ukrainienne ont pu directement envoyer aux familles des photographies des corps de soldats aux familles russes afin qu'elles puissent les identifier. Cela implique de passer outre le canal du CICR et du service RFL[2101]. Ajoutons que les réseaux sociaux facilitent le contournement des méthodologies traditionnelles de recherche des disparus. Les proches des défunts et disparus peuvent emprunter les réseaux de solidarités des exilés, contactés potentiellement via Facebook ou d'autres canaux. D'ailleurs, on assiste plus généralement à un phénomène de « crowdsourcing » des investigations[2102]. On a effectivement vu naitre ces dernières années des collectifs de personnes privées se lançant dans la recherche de personnes disparues, en passant ou non par les réseaux sociaux[2103]. Ces derniers permettent de relayer des informations, mais il est possible aussi d'exploiter les nombreuses traces que tout à chacun laisse sur les réseaux. Certaines enquêtes sur des personnes déclarées disparues peuvent ainsi avoir recours à des méthodes proches du renseignement en source ouverte (OSINT). L'usage

[2100] « the ICRC may collect information on the circumstances of death, and is mindful of the importance of this for the search for individuals, and for identification processes. However, the ICRC usually does not provide information about the cause, manner and circumstance of death to families in the cases in which it does get involved" PARRIN, Anjli,"How did they die?": Bridging humanitarian and criminal-justice objectives in forensic science to advance the rights of families of the missing under international humanitarian law", *International Review of the red cross*, n° 923, june 2023https://international-review.icrc.org/articles/how-did-they-die-bridging-humanitarian-and-criminal-justice-objectives-923#footnoteref37_8pckgf1

[2101]« Ni le texte des Conventions de Genève, ni les commentaires y afférents, ni la pratique des Etats ne mentionnent qu'une partie à un conflit armé devrait tendre la main aux parents des personnes décédées ou leur envoyer des photos de leurs cadavres. À l'inverse, les commentaires suggèrent plutôt qu'il incombe au Bureau national d'information ou à l'Agence centrale de recherche de transmettre les informations pertinentes sur le lieu où se trouvent les soldats décédés à leurs parents les plus proches. » "Neither the text of the Geneva Conventions, nor the commentaries thereto, nor relevant state practice mention that any party to an armed conflict should reach out to the relatives of dead persons or send them pictures of their corpses. Conversely, the commentaries much rather suggest that it is the responsibility of the National Information Bureau or the Central Tracing Agency to transmit the relevant information about the whereabouts of deceased soldiers to their next of kin » GRAF, Jan-Philip, NEUMANN, Jannik, « Between accuracy and dignity, legal implication of facial recognition for dead combatants », *Voelkerrechtsblog,* 30/09/2022 https://voelkerrechtsblog.org/between-accuracy-and-dignity/

[2102] GRAY, G., BENNING, B."Crowdsourcing Criminology: Social Media and Citizen Policing in Missing Person Cases", *Sage Open*, 2019, *9*(4). https://doi.org/10.1177/2158244019893700

[2103] COUTARD, Hélène, « Personnes disparues : rencontre avec les enquêteurs de la dernière chance », *Le Monde*, 11/02/2024https://www.lemonde.fr/m-le-mag/article/2024/02/11/personnes-disparues-les-enqueteurs-benevoles-de-la-derniere-chance_6215940_4500055.html

LUS, Bruno, « Sur internet et les réseaux sociaux, l'inlassable traque des personnes disparues », *Le Monde,* 19/10/2018https://www.lemonde.fr/pixels/article/2018/10/19/sur-internet-et-les-reseaux-sociaux-l-inlassable-traque-des-personnes-disparues_5371868_4408996.html

de ce type de technique se banalise progressivement dans le cadre de la documentation établie lors de la violation des droits de l'homme[2104]. Il existe quelques communautés spécialisées dans l'exploitation de ressources ouvertes s'étant dédiées aux cas des disparus[2105]. Des groupes de journalistes et d'activistes ont pu ponctuellement employer de l'OSINT afin de retrouver l'identité d'exilés dont les proches avaient perdu la trace[2106].

Ce dernier cas semble cependant isolé. Il est encore peu question d'OSINT pour les enquêtes sur les morts en migration. Il semblerait que le CICR reste prudent sur l'utilisation des réseaux sociaux, qui n'est mentionnée que très brièvement dans les guides des groupes de travail en médecine légale. On peut par exemple lire que : compte tenu des possibilités qu'offrent les nouvelles technologies, et notamment les « données générées via les médias sociaux, il est aussi essentiel de prendre toutes les mesures requises, de veiller à ce qu'une analyse soit faite au préalable et de s'assurer que les données feront l'objet d'une gouvernance approprié. »[2107] Et il est vrai que les techniques d'OSINT posent un certain nombre d'enjeux en matière de protection des données[2108]. Ces dernières diffèrent selon le type de méthodologie employée, l'OSINT recoupant un large panel de techniques d'enquête, et dont la définition fait encore débat, selon le degré de publicité des données. Enfin, on peut citer d'autres méthodologies se situant à la frontière de l'OSINT, à savoir le logiciel Clearview. Ce dernier est utilisé par le gouvernement ukrainien pour l'identification des soldats morts. Pour rappel, Clearview recourt à l'exploitation de données publique (des images Facebook), mais via un sous-traitant privé, qui réserve théoriquement sa commercialisation aux forces de l'ordre[2109].

Les familles et les particuliers utilisent quant à eux d'autres techniques de recherche sur les réseaux sociaux. En matière d'OSINT, on dispose de peu de documentation sur leurs pratiques. Pour le moment, on peut simplement rapporter un témoignage du groupe de travail sur les disparitions forcées : « le Groupe de travail a reçu des informations sur des cas où, grâce aux

---

[2104] DUBBERLEY, Sam, KOENIG, Alexa, MURRAY, Daragh (eds.), *Digital Witness, Using open source information for human rights investigation, documentation and accountability*, Oxford university press, 2020, 384 p.
MILANINIA, Nema. "using mobile phone data to investigate mass atrocities and the human rights considerations." *UCLA Journal of International Law and Foreign Affairs*, vol. 24, no. 2, 2020, p. 273–316.

[2105] https://www.tracelabs.org/
https://alexislingad.medium.com/osint-investigation-techniques-for-missing-person-cases-trace-labs-316aa1a94de9
https://www.missingpersonshackathon.com.au/

[2106] GLOBAL INVESTIGATION journalism network, "Digging into Disappearances: A Guide to Investigating Missing People and Organized Crime", 07/09/2020https://gijn.org/resource/digging-into-disappearances-a-guide-to-investigating-missing-people-and-organized-crime/
SAPOCH, Jack, BULMANN, May, CHERESHEVA, Maria, LUDKE, Steffen, LJUSTINA, Ivana, VOEGELE, Nicole, OBRADOVIC-WOCHNIK, Jelena, DAVIES, Thom, ISAKJEE, Arshad, ALHAFID, Doraid, TILLACK, Anna, MALICHUDIS, Stavros, SOOS, Oliver, VAN DIJKEN, Klaas, MILONOVIC, Aleksandar, IVANOVA, Camelia, RUBIO BERTRAN, Pat, " Europe's Nameless dead, Lighthouse reports, 01/12/2023 https://www.lighthousereports.com/investigation/europes-nameless-dead/

[2107] CICR, « Le processus d'identification forensique : une approche intégrée », 2022 https://www.icrc.org/fr/publication/4590-forensic-human-identification-process-integrated-approach

[2108] RAHMAN, Zara, IVENS, Gabriela, "Ethics in Open source investigations", in DUBBERLEY, Sam, KOENIG, Alexa, MURRAY, Daragh (eds.), *Digital Witness, Using open source information for human rights investigation, documentation and accountability*, Oxford university press, 2020 p.249

[2109] GAVOIS, Sébastien, "Reconnaissance faciale : Clearview librement utilisée par de nombreux individus", NEXT, 09/03/2020, https://next.ink/brief_article/reconnaissance-faciale-clearview-librement-utilisee-par-de-nombreux-individus/
CLAYTON, James, "How Facial recognition is identifying the dead in Ukraine", *BBC,* 12/04/2022 https://www.bbc.com/news/technology-61055319
ROMERO-MORENO, Felipe, "Facial recognition technology : how it's being used in Ukraine and why it's still so controversial", *The conversation*, 14/06/2022 https://theconversation.com/facial-recognition-technology-how-its-being-used-in-ukraine-and-why-its-still-so-controversial-183171

images de caméras de sécurité en circuit fermé (CCTV) sur le lieu où la personne disparue aurait été emmenée, les proches ou leurs représentants ont retrouvé la plaque d'immatriculation du véhicule utilisé ainsi que son itinéraire postérieur à sa disparition. En croisant ces informations avec les journaux d'appels et les données du téléphone portable de la personne disparue, ils ont recueilli des indications pertinentes sur l'endroit où elle pourrait se trouver. Dans certains cas, des informations similaires ont été obtenues grâce au contenu généré par les utilisateurs (par exemple, des photos ou des vidéos téléchargées sur les médias sociaux). »[2110]Il semblerait, d'après nos diverses recherches, que les familles recourent plutôt aux réseaux sociaux afin de diffuser des avis de recherche et recueillir des témoignages. Des groupes Facebook ont ainsi été créés par les proches, des collectifs de familles, des associations. Jan Bikker rapporte que dès 2010, à la suite du tremblement de terre à Haïti, une page Facebook avait été dédiée à la recherche des disparus. Sur le groupe étaient publiées des photographies des disparus faites de leurs vivants, de leurs effets personnels, ou des données comme des mails, des numéros de téléphone. Dans de rares cas, il peut arriver que des photographies de personnes décédées soient publiées dans des groupes Facebook ou des boucles Telegram[2111].

D'ailleurs, il existe peu de littérature sur les problématiques relatives à la protection des données que pose ce type de pratique. On peut pour notre part faire quelques observations. Tout d'abord, il faut prendre en compte le consentement de la personne concernée, comme le fait remarquer un enquêté : « *On constate également que de nombreuses personnes recherchent des informations sur une personne disparue, ou qu'il y a des publications sur des sites web… l'information est accessible au public et tout le monde peut voir que quelqu'un a disparu. C'est déjà un problème, parce que… (…) Et si cette information est partagée partout sur les médias sociaux par des centaines de personnes. Le problème est… OK, quelle serait mon opinion personnelle… si je suis un migrant, que je voyage dans différents pays et que quelqu'un décide soudain de publier des informations sur moi, sur différents réseaux, même si je n'y consens pas ?* »[2112]

Au-delà du cas des particuliers, le guide de protection de données du CICR recommande de recourir dans ce type de situation à la base légale de l'intérêt vital. Il serait dans l'intérêt de la santé psychique des familles de retrouver leur proche. Il est donc possible que des informations sensibles soient utilisées sans l'accord de la personne concernée. Mais la

[2110]Nouvelles technologies et disparitions forcées Rapport du Groupe de travail sur les disparitions forcées ou involontaires », septembre-octobre 2023 A/HRC/54/22/Add. https://www.ohchr.org/sites/default/files/2024-04/A-HRC-54-22-Add-5-FR.pdf

[2111] PIRONON, Virginie, « En Ukraine, les réseaux sociaux au secours des familles de disparus », *France Inter*, 21/03/2022 https://www.radiofrance.fr/franceinter/en-ukraine-les-reseaux-sociaux-au-secours-des-familles-de-disparus-5211523

D'ISTRIA, Thomas, « En Ukraine, les familles à la recherche de leurs disparus : « je continue d'espérer », *Le Monde*, 28/08/2023 https://www.lemonde.fr/international/article/2023/08/28/je-continue-a-esperer-en-ukraine-les-familles-a-la-recherche-de-leurs-disparus_6186784_3210.html

[2112]« Also what you will find is a lot of people looking for information on a missing person, or there are post on websites… it is publically available everybody can see that somebody is missing. This is already an issue, because… (…) And if this information is shared everywhere on social media by hundreds of people. The issue is… OK what would be my personal opinion… if I am a migrant, I am travelling around different countries and on a soudain somebody decide to post information on me, on different network, even if I don't give my consent to it » Entretienn°23, identification des morts n°2, 17/03/2020

personne conserve le droit d'être informée des circonstances de la publication de données et de la nature de ces dernières : « Un tel prérequis n'est évidemment pas applicable si la personne est décédée, mais en cas de disparition, il est peut-être envisageable que la personne concernée, une fois retrouvée, soit informée des données qui ont été utilisées lors de l'enquête. » [2113] En outre, le médecin légiste Jan Bikker alerte sur différents risques associés à ces pratiques. En effet, la publication de liste de victimes peut être exploitée pour nourrir des arnaques. Des fake news peuvent avoir été publiées sur des groupes de recherche de disparus. Des individus dissimulés sous de faux profils ont pu annoncer qu'un proche a été retrouvé, ou au contraire, que la personne est morte, alors que cela n'est pas le cas[2114]. L'objectif de ce type de publication peut être d'extorquer des sommes d'argent à des familles de migrants, ou faire pression sur eux[2115]. Ainsi un enquêté s'inquiète du fait que : « *Pour la famille, le fait de publier toutes ces informations peut la mettre en danger, par exemple du côté des passeurs ou des autorités qui recherchent quelqu'un. Par exemple, si des informations sur une personne originaire d'Érythrée sont publiées, même la famille peut subir des pressions. » Ce dernier ajoute que : « Pour les enfants disparus, il y a souvent… nous avons des alertes de personnes disparues pour les mineurs non accompagnés par exemple, pour les enfants, elles sont affichées (…) cela pourrait nuire à ces personnes, parce que tout le monde sait qu'un enfant a disparu, d'accord cela peut les mettre en danger, surtout si nous parlons d'enfants*. »[2116] Il va sans dire que les données utilisées par les enquêtes des familles doivent être stockées de façon sécurisée. Or les proches peuvent ne pas avoir les moyens de protéger les informations, comme le fait remarquer le groupe de travail onusien sur les disparitions forcées : « Les proches des personnes disparues utilisent fréquemment les réseaux sociaux ou les applications de messagerie pour rechercher activement leurs proches. Bien que cela puisse faciliter l'établissement du sort des personnes disparues et du lieu où elles se trouvent, on peut se demander si ces données hautement sensibles sont stockées et protégées de manière adéquate et sûre, compte tenu des cas de cyberattaques, d'atteintes à la protection des données et de piratage informatique. »[2117]

Dans ce dernier chapitre, on a tenté de comprendre le travail des médecins légistes et des personnes investies dans l'identification des morts. Au-delà des standards d'enquête, il nous

---

[2113] KUNER, Christopher, MARELLI, Massimo (eds.), Handbook on data protection in humanitarian action, second edition, 2020 https://rm.coe.int/handbook-data-protection-and-humanitarian-action-low/168076662a

[2114] BIKKER, J, "Disaster Victim Identification in the Information Age: The Use Of Personal Data, Post-Mortem Privacy and the Rights of the Victim's Relatives ", 2013 10:1 *SCRIPTed* 57 http://script-ed.org/?p=838
SMITH, Laura, "Tsunami email hoaxer jailed", *The Guardian*, 25/01/2005https://www.theguardian.com/technology/2005/jan/25/indianoceantsunamidecember2004.uknews?INTCMP=ILCNETTXT3487

[2115] *Infomigrants,* "Spain: Network 'profited for years' from families of missing migrants", 14/03/2024https://www.infomigrants.net/en/post/55816/spain-network-profited-for-years-from-families-of-missing-migrant
Bonmatí,Damia, Noticias Telemundo Investiga and Belisa Morillo, Noticias Telemundo Investiga, "Scammers target desperate Latino families whose migrant relatives are missing", *NBC News*, 03/01/2022 https://www.nbcnews.com/news/latino/scammers-target-desperate-latino-families-whose-migrant-relatives-are-rcna10696
PATTEM, Leah, KASSAM, Ashifa, "Missing migrants' families say they were asked to pay hundreds for information on relatives", *The Guardian,* 19/03/2024
https://www.theguardian.com/world/2024/mar/19/missing-migrants-families-say-they-were-asked-to-pay-hundreds-for-information-on-relatives

[2116]Entretien n° 23, identification des morts n° 2, 17/03/2020

[2117]« Nouvelles technologies et disparitions forcées Rapport du Groupe de travail sur les disparitions forcées ou involontaires », septembre-octobre 2023 A/HRC/54/22/Add. https://www.ohchr.org/sites/default/files/2024-04/A-HRC-54-22-Add-5-FR.pdf

a paru important de saisir ce qui motivait leur quête et quelles valeurs éthiques ces derniers mobilisent. Ainsi, pour une partie des acteurs impliqués dans ce travail redonner un nom aux morts permet de leur assurer une dignité. Ils entendent par là qu'il s'agit de fait de les rendre aux vivants, de faire en sorte qu'ils retrouvent une certaine appartenance sociale. Le fait d'être identifié est un des premiers droits restant aux morts duquel découle le fait d'être retourné aux familles, et de bénéficier d'une inhumation correspondant aux normes sociales en vigueur. On a toutefois gardé à l'esprit que ce travail d'identification nécessite de traiter des données très sensibles. Il existe par conséquent une tension entre identification et protection des données. Peu de littérature a été publié sur ce sujet, mais tout le long de ce chapitre, on a pu identifier quelques éléments à retenir. Il est vrai que dans un premier temps le droit de la protection des données semble constituer un obstacle à l'enquête. L'accès à toute une série de données sensible est réservé à un corps professionnel spécifique (forces de l'ordre, médecins légistes). Or, un bon nombre de personnes impliquées dans les enquêtes n'ont pas nécessairement ce statut et proviennent de la société civile. D'où la négociation d'accord pour obtenir un droit d'accès aux données. Autre point crucial en matière de protection des données, les professionnels de l'identification des morts plaident pour une centralisation des bases de données généralement génétiques, ce qui ne va pas sans questionnement éthique, voire méthodologique, d'autant que les bases de données génétiques sont bien souvent gérées par les forces de l'ordre, d'où l'importance de sécuriser les liens entre volet humanitaire et policier de l'enquête. Ceci est nécessaire afin de gagner la confiance des familles et des proches qui sont alors tentés d'enquêter par leurs propres moyens, notamment via les réseaux sociaux. Or ces méthodes d'enquêtes informelles ne sont pas sans risques en matière de protection des données. On peut ainsi conclure ce chapitre en remarquant qu'il est tout autant important de se soucier de la vie privée des morts que de celle des vivants. Rendre un nom et une dignité aux morts ne doit donc pas faire l'économie de la protection des vivants.

## Conclusion générale

Nous voilà arrivées au terme de notre thèse, il nous reste maintenant à parcourir à nouveau les différentes étapes de cette dernière pour en montrer les limites et pour proposer des ouvertures vers de possibles recherches ultérieures.

Nous sommes parties d'un questionnement portant sur les tensions découlant de la numérisation de l'aide. Les nouvelles technologies vont donc de pair avec un certain nombre de risques relatifs à la vie privée, et dans le même temps, elle est considérée comme un moyen d'amélioration de la réponse humanitaire. C'est qu'il existe une sensibilité dans le milieu humanitaire à un certain imaginaire technologique, pouvant être qualifié de technosolutionnisme. Sa diffusion a été favorisée par un rapprochement avec le secteur privé qui s'est fait conjointement à la numérisation de l'aide. L'adoption de NTIC par des ONG s'est traduite par l'entrée d'entreprises dans le secteur humanitaire, détenant des valeurs et des imaginaires a priori étrangers au milieu de la solidarité internationale, contredisant même parfois le système éthique des ONG, mais rencontrant un certain écho au sein du secteur de l'aide du fait d'une appétence pour l'expérimentation numérique : venir au secours d'autrui justifie le fait d'adopter des solutions les plus efficientes possibles. Ce rapprochement entre secteur privé et ONG a pris de nombreuses formes comme des partenariats, des actions de *pro bono*, des actions philanthropiques. Il englobe également une grande diversité d'acteurs. La place des GAFAM y est évidemment majeure. Elle est due à leur position dominante au cœur du numérique, à leur rôle dans la constitution du capitalisme de surveillance, et au sein de la tradition philanthropique américaine. Mais sans minimiser leur place, on a voulu la nuancer. Pour plusieurs raisons. Premièrement, le milieu de la Silicon Valley est traversé par un courant idéologique dont les soubassements théoriques l'éloignent de l'humanitaire. Il existe de fortes affinités entre acteurs de la Silicon Valley et longtermisme, quand bien même sa place reste à prendre en compte à sa juste mesure. Deuxièmement, des entreprises a priori beaucoup plus modestes ont investi différents secteurs du « marché numérique humanitaire ». On pense aux dispositifs d'identité numérique (investis notamment par Mastercard), au marché de la biométrie et à celui de la connectivité de crise (investie par Cisco, ou par Salesforce, nous pouvons noter que la firme de connectivité satellitaire d'Elon Musk, Starlink, y a cependant une influence grandissante, mais encore difficilement quantifiable). On pense aux projets de données massives et de type « data for good » impliquant des compagnies téléphoniques. La première section de la thèse nous a donc permis de faire un panorama de l'implication des entreprises dans le numérique humanitaire, en mettant en évidence trois moments clefs dans cette histoire : la crise migratoire de 2015, le Covid19 et le conflit en Ukraine. Trois crises durant lesquelles les entreprises ont joué un rôle humanitaire en finançant des ONG ou en nouant des partenariats avec ces dernières.

L'imaginaire de l'innovation s'est donc diffusé dans différents espaces du champ de l'humanitaire. Il a été soutenu par des acteurs évoluant au sein de laboratoires d'innovation d'ONG ou d'organisation comme l'ANALP. Il faut toutefois garder en tête que si cet imaginaire a connu un réel succès et s'est traduit par la création de réseaux d'acteurs et de lieux spécifiques, s'il reste soutenu par des fondations et des fonds dédiés, les bailleurs étatiques

resteraient plus prudents en matière de financement de l'innovation. Le modèle de financement de l'humanitaire par projet s'applique mal au temps long de l'innovation, qui nécessite de soutenir les différentes phases de conception d'une technologie jusqu'à sa mise en œuvre. Un bon nombre d'idée d'innovation, de partenariats avec des entreprises privées ne débouchent pas sur des projets pérennes, comme a pu le remarquer Giulio Coppi. Et surtout, pour les chercheurs les plus critiques, cet imaginaire de l'innovation contribuerait à légitimer ce qui relèverait d'expérimentations numériques, un terme qui renvoie à l'héritage colonial du numérique humanitaire. En somme, les théories du capitalisme de surveillance mettent en lumière le caractère extractif du numérique contemporain, fondé sur une économie de la donnée, mais pour ce qui concerne le secteur humanitaire, une part des risques relatifs à l'innovation peuvent être aussi liés à des dynamiques coloniales. Pour mieux comprendre ce point, on a effectué un retour en arrière en revenant sur l'histoire des expérimentations médicale dans les colonies. Ce pas de côté nous a paru nécessaire pour mieux appréhender l'humanitaire comme un « laboratoire numérique ». Selon la littérature existante, les expérimentations médicales reposent sur une construction des personnes comme sujets d'expérience, ainsi que sur l'idée d'une « terra nullius », d'un terrain vierge de droits, laissant toute licence à l'innovation. Mais si l'humanitaire a servi de phase de test pour des technologies telles que la biométrie ou des drones, ce secteur ne peut être réduit à un laboratoire. On peut retenir plusieurs arguments allant dans ce sens.

Premier point, il ne s'agit pas de minimiser l'agence des États locaux, souhaitant réguler les différentes expérimentations ayant lieu sur leur territoire. L'exemple de l'Inde s'opposant à Facebook et à son projet Free Basic est bien connu. On peut aussi penser au cas des drones, leur usage ayant été régulé par le Népal après le tremblement de terre de 2015. Citons aussi le cas du Liberia qui a suspendu un projet de donnée massive mené en réponse à l'épidémie d'Ebola, ce dernier contrevenant à sa législation en matière de protection des données. De manière plus générale, le renforcement du récit de la souveraineté numérique, également parmi les pays du Sud, pourrait nourrir une opposition aux expérimentations d'entreprises occidentales. D'ailleurs, les reconfigurations géopolitiques actuelles pourraient rebattre les cartes, les acteurs du continent africain pourraient être moins favorables aux entrepreneurs occidentaux, et dans le même temps, ils pourraient être plus ouverts à la collaboration avec d'autres collaborateurs, notamment chinois. Ce dernier point reste largement de l'ordre de l'hypothèse et pourrait faire l'objet de recherches ultérieures.

Deuxième limite, il existe au sein de l'humanitaire d'autres imaginaires de l'expérimentation : l'esprit du « Do It Yourself » et des makers pourrait constituer une alternative aux modalités d'innovations verticales, renforçant les inégalités de pouvoir entre bénéficiaires et ONG. Nous avons personnellement, lors de précédentes recherches, visité des espaces alternatifs de bricolage numérique, soit des fablabs humanitaires. Il existe en outre des organisations engagées dans ce sens, comme Werobotics. Cette ONG a fait du drone un outil d'émancipation. Cette expérience n'est évidemment pas dépourvue de limites. Nous avons décrit quelques-unes des inégalités Nord/Sud rémanentes entre Werobotics et ses antennes locales, les Flyinglab. Et si elle prône une approche décoloniale, l'organisation nous semble encore ancrée dans un circuit de financement propre à l'économie de la santé globale. Mais surtout, ce projet n'est pas pleinement émancipé de dépendances technologiques. Ces

dernières ne résultent toutefois pas simplement d'un legs colonial. On a vu que le milieu du drone civil est fortement dominé par des firmes chinoises (comme l'entreprise DIJ).

Quatrième limite, de façon générale, les projets de données ouvertes peuvent constituer des alternatives au modèle extractiviste du technocolonialisme. Cela dit, certaines initiatives de type « data for good » semblent s'éloigner de la défense d'un bien commun informationnel. Le cas de Facebook qu'on a évoqué est particulièrement parlant. La firme propose par exemple de mettre à disposition d'ONG des cartes élaborées à partir de l'exploitation des données des utilisateurs de son réseau. Ce type de « philanthropie informationnelle » risquerait d'aboutir à un accaparement de la définition du bien commun, [2118] tout en posant une série de risques pour les individus en matière de vie privée et en légitimant des firmes dont le modèle plus général repose précisément sur une forme d'extractivisme informationnel.

On a donc mobilisé plusieurs contre-arguments pour nuancer la thèse du technocolonialisme. Notre dernier point concerne évidemment l'entrée en vigueur d'une série de textes de loi comme le RGPD ou l'IA Act ayant, entre autres objectifs, la régulation de l'innovation numérique à l'échelle européenne. Cependant, la démarche de compliance propre au RGPD va de pair avec une responsabilisation des acteurs. Cette approche délègue la gestion des risques numériques à ces derniers. Certes, il existe au sein de l'humanitaire une certaine sensibilité pour un imaginaire technosolutionniste, mais la protection des données n'est pas tout à fait étrangère au secteur en raison de sa proximité avec le milieu médical, en raison de la sensibilité des  données traitées par les ONG.  Il existait un corpus de droit souple relatif à la protection des données au sein du secteur humanitaire antérieur au RGPD. Toutefois, il s'est avéré que les DPO d'ONG manqueraient, durant la rédaction de cette thèse, de moyens humains et financiers. Pour pallier ce manque, des ONG peuvent alors faire le choix de rendre prioritaire la mise en conformité en fonction des missions où le contrôle par les autorités de protection des données est le plus probable, à savoir au siège. Cela implique que la protection des données des bénéficiaires ne bénéficierait pas d'autant de ressources ou que la mise en conformité ne serait (dans certains cas) que formelle.

Pourtant les opérations de gestion de risque ne sont pas tout à fait étrangères aux ONG. Ces dernières sont en effet acculturées aux techniques d'anticipation de menaces diverses ( comme des risques de catastrophes, des risques d'accidents de sécurité). Cela dit la gestion du risque numérique ne semblerait pas être formalisé au sein du secteur. Plutôt que d'outils à utiliser clef en main, les analyses d'impact relatives à la protection des données (AIPD) seraient, quand on a interrogé les DPO, encore en cours de construction pour être déployées sur un terrain de crise. La forme des AIPD connait des variations. Elle dépend notamment des choix des DPO et leur façon d'arbitrer entre les différentes facettes parfois difficilement conciliables de ces outils. Les AIPD peuvent être souhaitées holistiques, inclure différents types de risques, tout en devant être réalisables sur le terrain et sans se limiter à un exercice

[2118] TAYLOR, L. « The ethics of big data as a public good: which public? Whose good? ", *Philos Trans A Math Phys Eng Sci*. 2016 28;374(2083)
TAYLOR, Linnet, BROEDERS, Dennis, "In the name of Development: Power, profit and the datafication of the global South", *Geoforum*, 64. P. 229-237.
MCDONALD, Sean Martin, « Data Reiew Boards: Facebook, data governance and trusts in practice »,*Digital Impact*, 03/04/2018
https://digitalimpact.io/data-review-boards-facebook-data-governance-and-trusts-in-practice/

formel. En outre, le fait de choisir de mener une AIPD dépend aussi du niveau de risque associé à une technologie et/ou à un contexte donné. Mais on a vu que des facteurs plus généraux peuvent entrer en jeu comme la modalité de gouvernance de l'ONG, l'indépendance des différentes antennes en matière de choix technologiques. La multiplication d'application ou d'outils de travail complexifie encore l'exercice de compliance. D'où le choix pour certains DPO de défendre l'idée d'une simplification et d'une réduction du nombre de sous-traitants, d'autant que la négociation de clauses de confidentialité ne suffit pas toujours à réduire les risques associés à ces derniers, surtout dans le cas où les ONG négocient avec de gros fournisseurs ou des GAFAM.

En outre, maitriser les risques numériques passe aussi par le choix de recourir à des outils respectant une démarche de type « privacy by design ». Cette approche est cependant peu discutée au sein du secteur humanitaire. Le CICR a toutefois adopté une stratégie visant à développer des dispositifs en suivant le principe de « privacy by design », selon les contraintes propres à l'humanitaire. Or les bailleurs poussent plutôt pour l'adoption d'outils facilitant la redevabilité et le traçage de l'aide, comme la biométrie. La réponse du CICR aux incitations des bailleurs a donc été d'expérimenter des solutions de type « biométrie privacy by design ». Mais sa réalisation reste suspendue aux ajustements budgétaires d'un secteur en crise. Le numérique permet de gagner en efficience, de faire des économies d'échelle, mais la recherche en matière de « privacy by design » a également un coût qu'il s'agit de défendre en interne dans un contexte de tensions financières.

On est donc revenue sur les modalités de régulation de l'innovation et leurs limites, en souhaitant nuancer l'idée d'un secteur humanitaire relevant d'une zone de « non-droit ». Dans la seconde partie, on a adopté dans un premier temps la démarche contraire. On a en effet fait le lien entre protection des données et principe d'indépendance des ONG face aux souverainetés étatiques. Une partie de la stratégie des ONG est alors de se soustraire au droit et de ménager des exceptions à ce dernier. Nous avons donc étudié l'application des immunités et privilèges à l'espace numérique, mais aussi les mobilisations d'ONG pour négocier des exceptions aux sanctions de mesures de contre-terrorisme.

Pour reprendre notre fil, on est revenue dans notre troisième chapitre sur les négociations entre États et ONG quant à des transferts de données. Ces derniers sont en partie très formalisées. Les humanitaires ont recours à différents outils juridiques comme des accords de siège. Mais les négociations informelles prennent parfois le pas, limitant la portée contraignante des accords et renforçant les inégalités entre ONG. La différence de statut juridique influe sur la possibilité d'opposer une ligne rouge en matière de partage de données. Par exemple, les organisations internationales disposent de privilèges et d'immunités qui leur permettent en théorie de conserver une certaine indépendance par rapport aux requêtes étatiques. Il faut cependant surligner le fait que toutes les organisations internationales n'opposent pas le même positionnement face aux requêtes des gouvernements. Tout dépend d'abord du mandat de l'organisation internationale, comme le montre l'exemple du HCR, qui travaille conjointement aux États, et leur laisse parfois la main en matière de gestion des réfugiés. Quant au CICR, il affiche la confidentialité comme une valeur cardinale. Mais l'organisation est mise au défi par la numérisation de ses opérations, qui rend plus difficile

l'application des privilèges et immunités dans le cyberspace. Ce dernier cas nous a permis d'explorer la façon de protéger les données dans un contexte de triple recomposition de la définition classique de la souveraineté. Elle découle d'un ensemble de textes juridiques ayant un caractère extraterritorial (le Cloud Act), de la fluidité du numérique et de sa faculté à se jouer des frontières traditionnelles des États, notamment pour l'informatique en nuage. Enfin, elle est aussi le fait des privilèges et immunités, qui permettent à une organisation internationale de ne pas appliquer les lois locales d'un État.

Notre cinquième chapitre revient sur les tentatives des ONG pour négocier des exceptions aux mesures de contre-terrorisme et au sanctions en se fondant sur le droit humanitaire. Dans un contexte de guerre contre la terreur, les humanitaires plaident pour un plus grand respect de ce dernier, en vue de garantir l'indépendance, la neutralité et l'impartialité des ONG. On a mentionné différents espaces de négociation au sein d'institution multilatérale (comme l'ONU et son Conseil de sécurité), ainsi que le mouvement d'opposition d'ONG aux mesures de criblages imposées par des bailleurs de fonds, comme l'USAID ou l'AFD. Ce mouvement d'opposition a semblé, étonnamment, avoir en partie porté ses fruits, ce qui nous a paru surprenant dans un contexte de resserrement du contrôle du secteur associatif. Cette ouverture reste cependant suspendue à sa mise en pratique et à l'évolution du contexte politique national et international.

Ajoutons que les négociations d'ONG humanitaires portant sur les mesures de contre-terrorisme n'ont porté qu'à la marge sur les enjeux de vie privée, et ce en dépit des enjeux relatifs à la protection des données que soulève l'ensemble des mesures de contrôle de financement. Effectivement, des organisations comme Privacy International ou le Comité européen à la protection des données s'inquiètent du caractère disproportionné des règlementations de type LBC/FT. Quant aux humanitaires, ils s'opposent en majeure partie aux mesures de lutte contre le financement du terrorisme pour des motifs opérationnels et en raison des risques d'atteinte au DIH et aux principes de neutralité et d'impartialité de l'aide. Les ONG craignent en outre que les mesures de criblage des bénéficiaires soient perçues comme des opérations de renseignement, entrainant une rupture de confiance à l'égard des acteurs de la solidarité internationale. Cela mettrait alors en danger les humanitaires et ferait obstacle à l'allocation de l'aide. Leur priorité est donc de négocier avec les banques un allégement des mesures de conformité bancaire, quitte à contrevenir aux normes de KYC. Pour ce faire, certaines ONG adoptent alors des solutions aux marges de la légalité. On pense à l'hawala ou à des cryptomonnaies. Ces dispositifs se situent à la frontière du droit, et leur adoption peut se faire au prix d'une certaine insécurité juridique, et ce alors que ces solutions ne permettent pas toujours de garantir la vie privée des bénéficiaires.

Pour conclure ces lignes, nous sommes revenues sur les négociations d'ONG pour obtenir un statut d'exception et remettre en cause la criminalisation des humanitaires construite par différentes institutions centrales dans la lutte contre le financement du terrorisme, comme le GAFI.

Dans notre cinquième partie, on s'est au contraire intéressée aux efforts de régulation du cyberespace pour tempérer les attaques touchant les humanitaires. Ceci n'est pas sans

évoquer la situation des ONG dans les années 1990, lorsqu'elles ont commencé à être ciblées par différents groupes armés non étatiques.

Toutefois, malgré de possibles parallèles, les cyberattaques n'auraient pas encore été, au début des années 2020, catégorisées systématiquement comme des « accidents de sécurité » pour les personnels des ONG. Plusieurs raisons expliquent ceci. Le numérique a beaucoup été utilisé pour assurer la sécurité des humanitaires intervenant sur le terrain. Et contrairement aux attaques se traduisant par des enlèvements ou des assassinats, les cyberopérations n'ont pas nécessairement des répercussions aussi tragiques. Ces dernières peuvent être moins directement palpables, malgré les récits catastrophistes qui peuvent les entourer. Elles ont pu paraitre secondaires aux yeux des « security managers », même si cette perception peut évoluer, face à des enlèvements et assassinats, d'autant qu'elles ne font pas l'objet d'une comptabilisation précise, contrairement aux accidents de sécurité.

Mais si le lien entre la sécurité des humanitaires et les enjeux cyber reste à construire, le CICR insiste sur la nécessité d'assurer la protection des bénéficiaires dans l'espace numérique. Son discours s'inscrit en partie dans une remise en perspective des récits régaliens sur les menaces agitant le cyberespace. Il se traduit par une injonction à remettre la personne au cœur de la cybersécurité. En anglais, on parle ainsi de « human-centric cybersecurity ». Cette terminologie recoupe plusieurs types d'approches, se situant à la frontière entre sécurité humaine et défense des droits de l'homme, et du droit international humanitaire. L'analyse des dommages des cyberattaques doit alors prendre en compte d'autres répercussions que des conséquences strictement économiques ou stratégiques, et élargir le concept de violence. C'est l'angle d'approche qui parait traverser notre troisième partie. Il ressort des différentes thématiques qu'on a abordé une lecture des risques numériques qui les relie à des enjeux opérationnels, la continuité de l'aide. Mais il apparait aussi pour les ONG que les bénéficiaires doivent faire l'objet d'une protection spécifique face à des répercussions numériques de violence d'États (surveillance, répression, etc.). Les doctrines de sécurité humaine peuvent recouper l'approche humanitaire, et notamment la nécessité de protéger les civils. Mais elles s'en distinguent en incluant de façon plus centrale la protection des droits de l'homme (et notamment du droit à la vie privée), alors que le CICR plaide plutôt par une plus grande application du DIH au cyberespace.

Or, le DIH a été conçu initialement pour réguler les affrontements sur un champ de bataille physique et non virtuel. L'appliquer au cyberespace ne va pas de soi et nourri depuis quelques années une vive discussion, à laquelle le CICR a participé. L'organisation a donc construit une certaine doctrine sur ce sujet. Pour rentrer dans le vif du sujet, le CICR a adopté une conception large des cyberattaques, mais il ne considère pas toutes les cyberopérations comme telles. Elles doivent impérativement affecter le fonctionnement d'un système informatique. Et surtout, il existe peu de littérature sur la prohibition d'accès à des données de civils dans le cadre de conflits, hors structures et objets bénéficiant d'une protection spéciale, notamment les données médicales. Et curieusement, la régulation d'activités de renseignement et d'espionnage — qu'il soit numérique ou non — dans le cadre de conflits semble à première vue, sauf erreur de notre part, constituer un angle mort du DIH. Les débats sur les cyberopérations auxquels participe le CICR portent sur d'autres problématiques que la

protection de la vie privée en tant que telle des bénéficiaires et des civils. Toutefois, dans les prises de position de juristes de l'organisation, on note un infléchissement allant dans le sens d'une prise en compte des cyberopérations n'ayant pas d'impact sur la fonctionnalité des dispositifs numériques. C'est en tout cas le positionnement d'autres juristes qui invitent à choisir un autre cadre juridique que le DIH et revenir au droit de la protection des données ou aux droits de l'homme.

A ce stade, on peut rappeler que notre critique de la conception biopolitique de l'aide suit deux lignes : une première ligne est reliée à la régulation de l'innovation que propose le RGPD, une deuxième ligne est relative à la défense des droits des bénéficiaires, comme l'autodétermination informationnelle par exemple. Toujours est-il que les crises peuvent être interprétées comme des moments de suspension du droit commun, notamment parce qu'elles se déroulent dans des espaces où les souverainetés étatiques sont fragilisées, du moins contestées, entre autre par des groupes armés qualifiés de terroristes. On a pu aussi aborder des espaces hors des frontières territoriales classiques (comme le cyberespace). Mais ces espaces d'exception ne sont pas complétement vides de droits : la lutte contre le terrorisme va de pair avec un lourd régime de sanction, dont les ONG désirent s'exempter. En outre, d'un autre point de vue, les États tentent aussi (avec plus ou moins de succès) d'apprivoiser le cyberespace, processus auquel le CICR prend part, en participant aux débats concernant la manière d'y appliquer le droit humanitaire international.

Pour les ONG, les bénéficiaires ne sont toutefois pas simplement des objets de protection, ils peuvent être considérés en tant que sujets de droit. C'est pour cela qu'on a pensé s'appuyer sur la notion de « dignité », qui est a priori moins mise en avant dans l'actualité médiatique et scientifique que ceux de souveraineté et de colonialité. On s'est pourtant rendue compte qu'elle occupe une place importante dans l'architecture éthique des humanitaires et dans le droit de la protection des données, notamment parce qu'elle est liée à la notion d'autodétermination informationnelle, qui est au cœur de la tradition juridique allemande. Et en creusant le concept de dignité, on a réalisé qu'une série d'échos s'opère entre les principes humanitaires et un corpus normatif construit par des acteurs défendant l'autodétermination informationnelle. La notion de souveraineté contenait aussi cette idée de contrôle de l'information, mais elle était rattachée à une autre tradition théorique, proche des sciences politiques. Alors que la notion de dignité est nourrie par la philosophie morale, la bioéthique et la philosophie du droit. Elle nous a ainsi permis surtout de mettre en tension vulnérabilité et autonomie, en nous appuyant sur différents auteurs rattachés aux théories du « Care ».

Cette tension est manifeste au sujet de ce qui semble relever d'un « paradoxe du consentement » au sein de l'humanitaire. En effet, on a pu constater que le consentement reste la base légale la plus utilisée et la plus valorisée. Recueillir ce dernier permettrait de se conformer à une série de valeurs essentielles de l'action humanitaire. Or il apparait qu'elle n'est pas tout à fait adaptée au contexte de crise. Un premier type de limite est relative à la temporalité de l'humanitaire, à savoir l'urgence. Une deuxième difficulté que rencontrent les DPO est relative au caractère éclairé du consentement et à la nature de l'information communiquée aux personnes concernées. En tout cas, il est clair qu'un facteur semble déterminant en matière de consentement : le degré de littératie numérique ainsi que

l'existence, ou non, d'une fracture numérique. Effectivement, pour un bon nombre de DPO, les bénéficiaires manquent de connaissance sur les NTIC. Cependant, il faut impérativement rappeler qu'il est difficile pour tout à chacun d'avoir une vision complète des flux de données transitant à travers nos ordinateurs et smartphone. Et certes il est indéniable qu'il existe une forte dépendance des bénéficiaires à l'égard des ONG. Ces dernières tentent d'assurer leur survie et remplir des besoins essentiels (nourriture, santé, éducation, etc.). Mais dans le même temps, les ONG n'auraient pas toujours ménagé des espaces de refus à un traitement de donnée, ce qui nécessiterait de construire une alternative à la quantification de l'aide.

On a donc esquissé un panorama des différentes difficultés associées à la collecte du consentement, ainsi qu'à la difficulté d'y renoncer. Le consentement fait écho à une série de valeurs faisant sens pour les humanitaires. Et si recourir à la base légale de l'intérêt légitime est alors présenté comme une forme de pragmatisme, cela va de pair avec le risque d'aboutir à une forme de « paternalisme ». Pour le chercheur spécialisé en éthique médicale Alexandre Jaunet, une solution serait de passer d'un modèle du consentement fondé sur l'autonomie exclusive de l'individu à un modèle s'appuyant sur la confiance des personnes concernées. Il s'inspire alors des travaux de la philosophe Annette Baier. Elle s'inscrit dans une perspective proche des théories du care, et qui a mené une réflexion sur la façon de construire une relation éthique entre personnes inégales en dépassant le modèle du consentement libre. En somme, les malades ne pourraient tout à fait consentir à l'acte médical ( en raison des inégalités structurelles entre médecins et patients), mais ils délégueraient plutôt leur confiance au personnel de soin. Néanmoins, cela suppose selon Alexandre Jaunet une forte responsabilité. Or pour les humanitaires, la confiance est au cœur de la relation d'aide et permet de se faire accepter sur le terrain par les populations locales. Massimo Marelli a pu ainsi répéter que cette dernière doit se retrouver dans l'espace numérique. Néanmoins, si Alexande Jaunet lie confiance et professionnalisme, on a largement évoqué (cf. chapitre 2) le caractère encore inachevé de la professionnalisation des usages numériques et les difficultés des humanitaires (ainsi que des DPO) à appréhender la complexité des flux informationnels propre au milieu numérique. D'où la nécessité de trouver des espaces de formations communs, d'apprentissage du numérique[2119], comme des fablabs humanitaires par exemple.

Or, les projets de blockchains qu'on a décrits partaient d'un principe contraire : ils reposaient (pour la plupart d'entre eux) sur un dispositif technologique sans prendre en compte d'emblée dans le projet les enjeux de littératie numérique. Ou bien ces derniers étaient résolus en déléguant en partie la gestion des dispositifs d'identité, au risque de s'éloigner de l'idéal initial d'autodétermination informationnelle, ce dernier étant conditionné à un usage individuel des dispositifs techniques. Plus généralement, une piste de réflexion concerne la façon de dépasser la lecture libérale et individualiste de la notion de dignité, et de mettre l'accent moins sur la maitrise individuelle du numérique que sur des modalités de gestion des données collectives et des formes de gouvernance des données reposant sur l'idée de commun, en

[2119] CASSWELL, Jenny, "The essential role of digital literacy in contexts of forced displacement", Forced migration review, 2024, issue 73 https://www.fmreview.org/digital-disruption/casswell/
The Effects of a Gender-Sensitive, Safety-Prioritizing Digital Literacy Training for Women in Yemen, International Refugee rescue, 2024, https://gbvresponders.org/wp-content/uploads/2024/04/Digital-Literacy-Learning-Brief-1.pdf

prenant garde à de possibles « appropriation » de cet idéal par des entreprises privées (cf. chapitre 2).

En tout cas, il s'agirait de trouver des cas où la notion de dignité n'est pas nécessairement interprétée dans un sens individuel. On se souvient de l'interprétation qu'en donnent Cynthia Fleury et Norman Ajari, plus politique et mettant l'accent sur des formes de résistances collectives. Il ne s'agirait plus de s'intéresser au consentement individuel, mais à des mobilisations collectives contre la nature extractive du numérique humanitaire. Or à notre connaissance (mis à part le cas des houthis au Yémen qu'on a déjà évoqué), la plupart des recherches portant sur le numérique humanitaire mettent l'accent, à notre connaissance, sur les effets de dominations et moins sur les cas de résistance, individuelle ou collective[2120], de pratique de « contre-surveillance » de la part des bénéficiaires[2121], ou de détournement de dispositifs techniques.

Il nous semble qu'on retrouve cette dimension collective de la notion de dignité au sujet des morts. Ces derniers étant triplement des parias, en tant qu'exilés, en tant que morts et cadavres dépourvus d'identité. Ainsi, pour une partie des acteurs impliqués dans l'identification des morts, leur redonner un nom permet de leur assurer une dignité, voire de lutter contre leur invisibilisation liée à leur criminalisation. Il s'agit de les rendre aux vivants, de faire en sorte qu'ils retrouvent une certaine appartenance sociale. L'identification est un des premiers droits restant aux morts duquel découle le fait de pouvoir être retourné aux familles, et de bénéficier d'une inhumation correspondant aux normes sociales en vigueur (les morts anonymes étant des morts qui « dérogent »). On a toutefois gardé à l'esprit que ce travail d'identification nécessite de traiter des données très sensibles. Il existe par conséquent une tension entre identification et protection des données. Peu de littérature a été publiée sur ce sujet, mais tout le long de ce chapitre, on a pu identifier quelques points à retenir : l'accès par la société civile à des bases de données protégées par le secret médical ou par le droit de la protection des données ; la centralisation des bases de données généralement génétiques, qui soulève un bon nombre de questionnements éthiques, voire méthodologiques ; l'implication des forces de l'ordre dans les enquêtes, et l'importance de cloisonner les volets humanitaires et policiers de l'investigation ; la nécessité d'assurer la confiance des familles, qui peuvent également mener leurs propres investigations, passant bien souvent par les réseaux sociaux, ceci sans le consentement des personnes disparues (leur sort n'étant pas encore éclairci), et en dépit de différents risques en matière de protection des données, qui ne sont pas encore documentés de façon approfondie.

Notre travail se base sur des entretiens, et par le choix d'un cadrage large sur le numérique humanitaire, ce qui ménage la possibilité de poursuivre les recherches et prolonger certains sujets qu'on a évoqués. Certains points pourraient être approfondis en ayant recours à de l'observation directe. Elles permettraient d'approfondir la description des différents groupes

[2120] WELLES, Amanda, " Digital refugee resistance, power, representation and algorithmic censorship", FMR 73, Digital disruption and displacement,May 2024

[2121] KYAW, NYI NYI, "Digital counter-surveillance by refugees from Myanmar in Thaildand", FMR73, Digital disruption and dispalcement, May 2024

d'acteurs qu'on a pu identifier : les DPO, les informations managers officiers, les ingénieurs, les médecins, etc. Cela permettrait de leur donner un peu plus de « corps » et pouvoir décrire plus finement leurs pratiques et leurs stratégies. Plusieurs pistes s'ouvrent alors, entre le fait de poursuivre avec un angle transversal, ou de traiter et creuser des sujets plus spécifiques. Au sujet du consentement par exemple, un travail de terrain permettrait de mieux mettre en évidence les interactions et les dynamiques de pouvoir entre les bénéficiaires et les humanitaires.

Toutefois, en dépit de son angle généraliste, qui était fondée sur l'idée d'acquérir une première vue transversale du numérique humanitaire, notre sujet étant soumis aux évolutions technologiques et géopolitiques actuelles, il est très probable que de nouvelles dimensions de ce dernier apparaissent au fil du temps. Faire de la prospective à ce sujet est difficile, cela constitue peut-être d'un truisme, mais le contexte actuel est pour le moins incertain. Toujours est-il que du fait de son caractère contemporain, il a été difficile d'inclure au fil du temps toutes les facettes du numérique humanitaire. De surcroit, nos recherches peuvent être prolongées du fait que les pratiques ont pu évoluer depuis le début de notre thèse, puisque nos entretiens couvrent une période allant de la fin de l'année 2019 à environ la moitié de l'année 2023. Mais surtout, on n'a peut-être pas assez accordé d'importance à un sujet qui fait aujourd'hui beaucoup couler d'encre : les intelligences artificielles. Le sujet était resté à l'arrière-plan dans le secteur de la solidarité internationale, quelques chercheurs s'y sont confrontés, comme Sarah Spencer. Mais de son propre aveu, seule une minorité d'humanitaire s'y intéressaient, ce qui a compliqué ses recherches. Et il en a été de même pour nous, puisque le sujet n'a pas été pris en compte dans notre tour d'horizon du numérique humanitaire. La démocratisation de l'IA générative fin 2022 a remis au cœur de l'actualité ce sujet[2122]. Une série de rencontres a eu lieu et des publications ont été mises en ligne depuis fin 2023 et courant 2024[2123]. Le paysage émergeant des IA dans l'humanitaire reste toutefois encore à cartographier. Pour ce faire, il serait nécessaire de déterminer les usages et les acteurs recourant aux différents types d'IA existantes (prédictives, génératives, etc.), en étant attentive aux inégalités entre ONG en fonction de leur capacité à se doter de ce genre d'outils,

---

[2122] Sarah Spencer témoigne de cette montée en puissance du sujet dans l'humanitaire :
« un grand nombre de choses ont changé depuis la publication de Humanitarian AI : the hype, the hope and the future en novembre 2021. À l'époque, seule une poignée d'acteurs humanitaires exploraient le potentiel de l'intelligence artificielle (IA) et de l'apprentissage machine (ML), et ces expériences étaient en grande partie menées par des agences qui disposaient du personnel, des données, de l'argent et/ou des relations avec des entreprises technologiques nécessaires pour le faire. En fait, il s'est avéré difficile d'identifier un nombre suffisant de personnes à interviewer en 2021 pour ce document, qui avaient à la fois un intérêt et une compréhension de base de l'IA et de l'action humanitaire. »
« great deal has changed since Humanitarian AI: the hype, the hope and the future was published in November 2021. At that time, only a handful of humanitarian actors were exploring the potential of artificial intelligence (AI) and machine learning (ML) and these experiments were largely led by agencies that had the requisite staff, data, cash, and/or relationships with technology firms to do so. In fact, identifying a sufficient number of individuals to interview in 2021 for that paper, who had both the interest and a basic understanding of both AI and humanitarian action, proved challenging." SPENCER, W, Sarah, "Humanitarian AI revisited: seizing the potential and sidestepping the pitfalls, Humanitarian Practice Network, 07/05/2024 https://odihpn.org/publication/humanitarian-ai-revisited-seizing-the-potential-and-sidestepping-the-pitfalls/

[2123] Briefing note on artificial intelligence and the humanitarian sector, OCHA, 17/04/2024 https://www.unocha.org/publications/report/world/briefing-note-artificial-intelligence-and-humanitarian-sector
MARGFFOY, Mayra, "AI for humanitarian : A conversation on the hype, the hope, the future", *The New humanitarian*, 05/09/2023 https://www.thenewhumanitarian.org/feature/2023/09/05/ai-humanitarians-conversation-hype-hope-future
RAFTREE,Linda,"Do humanitarians have a moral duty to use AI to reduce human suffering? Four key tensions to untangle", *ALNAP*, 11/06/2024
https://alnap.org/humanitarian-resources/publications-and-multimedia/do-humanitarians-have-a-moral-duty-to-use-ai/
BEDUSCHI, Ana, Harnessing the potential of artificial intelligence for humanitarian action: Opportunities and risks, International Review of the Red Cross, Cambridge Vol. 104, N° 919, (Apr 2022):

et en étant attentive aux nouvelles dépendances à l'égard d'acteurs privés. Se posent aussi des enjeux d'épistémologie : quelle lecture des catastrophes implique le recours aux IA, un conflit peut être prédictible ou non ? On peut aussi réfléchir au sens que prend la redevabilité d'une IA : quelle transparence d'une IA pour les bénéficiaires ? Comprendre la modalité de fonctionnement des IA est d'autant plus nécessaire qu'elles pourraient aussi renforcer des discriminations préexistantes en fonction de biais d'algorithmes. Il est aussi évident que l'application d'un certain nombre de principe éthique humanitaire va poser question. Comment penser une IA qui respecte le principe d'humanité et la dignité des bénéficiaires ? [2124] Il reste en outre à déterminer la spécificité des risques en matière de protection des données [2125], et la modalité d'encadrement de l'innovation, en fonction des standards normatifs et des textes en vigueur, notamment l'IA Act[2126].

Deuxième point, on l'a déjà évoqué plus haut, mais les recompositions géopolitiques vont aussi avoir des effets. On pense à la guerre économique entre les États-Unis et la Chine et la place de cette dernière dans l'écosystème numérique. Pour le moment, l'influence de cette dimension sur le secteur humanitaire est difficile à évaluer (le seul sujet qui nous a paru y être lié concerne les drones civils, qu'on a pu évoquer dans le chapitre 2).

Troisième limite du sujet consiste à avoir mis de côté les bénéficiaires des ONG. Ce choix était dû à notre volonté de nous concentrer sur des acteurs encore peu étudiés, à savoir les DPO. Surtout, des chercheurs et des chercheuses ont déjà travaillé sur les pratiques numériques des exilés, en mettant l'accent sur l'opposition entre surveillance, care et control, empowerment et effets de dominations, une part des recherches s'est intéressée au contraire aux actions de résistance des exilés, ou du moins leur façon de contourner des dispositifs numériques développés par les ONG humanitaires. Et en outre, concernant les droits des bénéficiaires, on s'est concentrée sur les enjeux relatifs au consentement. Il existe donc encore du potentiel de recherche, sur différents droits garantis par le RGPD, comme le droit à l'oubli, ou le droit d'accès aux données. D'ailleurs, une question se pose en matière d'articulation entre le droit à l'oubli des bénéficiaires et les enjeux d'archivage des données des ONG. Eux même font écho au lien entre protection des données et enquêtes historiques ou en lien avec l'établissement de preuve lors d'enquête de violation de droits de l'homme, ou encore à titre historique. Ainsi un enquêté a pu nous faire part de ses interrogations : « *quels sont les droits des individus par rapport à ces données ? Pour quelles raisons on va les archiver ? Maintenant on a les descendants qui reviennent vers nous parce qu'ils veulent des informations sur leurs grands-parents, ou alors ils veulent faire des requêtes pour compensation dans leur pays ; l'Allemagne a mis en place un système de compensation pour les victimes des crimes nazis. Le problème c'est qu'on se retrouve sur le même scénario, les dossiers qu'on a sur la guerre au Liban ce sont des dossiers, qui sont fermés, la guerre au Liban est terminée, les dossiers ne sont plus actifs, mais qui dit que dans 20 ans les personnes ne vont*

[2124] https://www.ai-geopolitics.org/team/massimo-marelli
[2125] MASINDE,B.K., Artificial intelligence,Preventing privacy disasters,*Geoversity*, 14/02/2024 https://www.geoversity.io/stories/1342258/preventing-privacy-disasters/
[2126] MCELHINNEY, Helen, SPENCER W., Sarah, " The clock is ticking to build guardrails into humanitarian AI", *The New humanitarian*, 11/03/2024 https://www.thenewhumanitarian.org/opinion/2024/03/11/build-guardrails-humanitarian-ai

*pas venir vers nous pour avoir des informations ou des compensations si les mécanismes, judiciaires se mettent en place. »*[2127]

Quatrième point, on s'est concentrée sur un secteur, l'humanitaire, ainsi que sur les enjeux de vie privée. Il existe d'autres sujets connexes pouvant encore faire l'objet de belles explorations. Et notre angle d'attaque a été celui de la protection des données, la numérisation de l'aide a renforcé d'autres risques préexistants. On pense aux enjeux de désinformations. Ce sujet a pris de l'ampleur au cours des années précédentes, mais son impact sur l'humanitaire est cependant encore peu abordé dans la littérature scientifique. Quelques articles ont été publiés, notamment dans la recherche anglophone, mais le sujet reste encore à creuser[2128]. Plusieurs questions se posent : le caractère ciblé ou non des campagnes de désinformation envers une ONG, les répercussions de ces dernières sur les dynamiques conflictuelles, sur l'allocation de l'aide et sur la relation que les bénéficiaires nouent à l'égard des ONG. D'où une réflexion possible sur l'articulation entre notion de confiance et de vérité, sur ce qu'elle signifie actuellement pour les humanitaires et les populations secourues, sur la façon dont cette articulation est remodelée par l'évolution contemporaine de la production et la réception de l'information.

[2127] Entretien 44, OI 2, DPO, 03/03/2021

[2128] NANTHINI, S, "Countering disinformation and misinformation in humanitarian relief work", RSIS commentary, n° 127, 07/12/2022
XU, Rachel, "You can't handle the truth: misinformation and humanitarian action", 15/01/2021
https://blogs.icrc.org/law-and-policy/2021/01/15/misinformation-humanitarian/
"How misinformation and disinformation harm ICRC's humanitarian work in Burkina Faso", ICRC, 17/02/2023
https://www.icrc.org/en/document/burkina-faso-how-misinformation-disinformation-harm-humanitarian-action
JAFF, Dilshad,"The surge of spreading harmful information through digital technologies: a distressing realtiy in complex humanitarian emergencies", The Lancet, Volume 11, Issue 6, June 2023
https://www.thelancet.com/journals/langlo/article/PIIS2214-109X(23)00207-3/fulltext
Rumors and misinformation, using social media in Community based protection", chapter 6, UNHCR, February 2022
https://www.unhcr.org/innovation/wp-content/uploads/2022/02/Using-Social-Media-in-CBP-Chapter-6-Rumours-and-Misinformation.pdf
"Managing misinformation in a humanitarian context"Internews, February 2021
https://internews.org/wp-content/uploads/2021/02/Rumor_Tracking_Mods_1-2_Context-Case-Studies.pdf
HARGRAVE, Russell, "Aid groups targeted by fake news, report says", Devex, 14/02/2018
https://www.devex.com/news/aid-groups-targeted-by-fake-news-report-says-92096
"How disinformation campaigns endager lives in Sudan", SMEX, 19/05/2023
https://smex.org/how-disinformation-campaigns-endanger-lives-in-sudan/
BUNCE, Mel, "Humanitarian communication in a post-truth world", Journal of humanitarian affairs, 2019, vol.1, issue 1,
https://www.manchesterhive.com/view/journals/jha/1/1/article-p49.xml
Addressing the impact of mis-/disinformation on civilian, perpectives from peacekeeping and humanitarian practitioners, POC week side event to UN security COncil Open debate on POC, 25/05/2023
https://reliefweb.int/report/world/addressing-impact-mis-disinformation-civilians
Urquhart, M., 2021. Migrants and misinformation: Key themes in Nigeria, Bangladesh and Malaysia.
International Organization for Migration (IOM)., 2021
https://publications.iom.int/system/files/pdf/Migrants-and-Misinformation-Key-Themes.pdf
PEARN, Kristen, VERITY, Andrej, "Mis&Disinformation: handling the 21st century challenge in the humanitarian sector", Digital Humanitarian network, February 2022
https://digitalhumanitarians.com/mis_and_disinformation-handling_the_21st_century_challenge_in_the_humanitarian_sector/

# Bibliographie

## Introduction

## Littérature scientifique

### ARTICLES DE REVUE

AGIER Michel, « La main gauche de l'empire ordre et désordres de l'humanitaire », *Multitudes*, 2003/1 no 11, p. 67-77

AGIER, Michel**,** « Urgence et attente », *Écrire l'histoire*, 16 | 2016, http://journals.openedition.org/elh/1086 ; https://doi.org/10.4000/elh.1086

ARORA, P., "Decolonizing Privacy Studies", *Television & New Media*, *20*(4), 2019, p.366–378. https://doi.org/10.1177/1527476418806092

ATLANI-DUAULT, Laëtitia, DOZON, Jean-Pierre, « Colonisation, développement, aide humanitaire. Pour une anthropologie de l'aide internationale », Ethnologie française, 2011/3 (Vol. 41), p. 393-403. DOI : 10.3917/ethn.113.0393. URL : https://www.cairn.info/revue-ethnologie-francaise-2011-3-page-393.htm

ATTEN M., « Ce que les bases de données font à la vie privée », *Réseaux*, 178-179, 2013, p. 21-53

AUDET, François, « L'acteur humanitaire en crise existentielle : les défis du nouvel espace humanitaire», *Études internationales*, volume 42, numéro 4, décembre 2011, p. 447–472. https://doi.org/10.7202/1007550ar

ÁVILA PINTO Renata, « La souveraineté à l'épreuve du colonialisme numérique », dans : Cédric Leterme éd., *Impasses numériques. Points de vue du Sud,* Paris : Éditions Syllepse, « Alternatives Sud », 2020, p. 25-35.

BACQUE Marie-Hélène, BIEWENER Carole, « l'empowerment, un nouveau vocabulaire pour parler de Participation ? », *Réseau Canopé, «Idées économiques et sociales »*, 2013/3 N° 173, p. 25-32

BAUMAN, Zygmunt, BIGO, Didier, ESTEVES, Paulo, GUILD, Elspeth, JABRI, Vivienne, LYON, David,

CASILLI, Antonio, « Contre l'hypothèse de la « fin de la vie privée » », *Revue française des sciences de l'information et de la communication*, 2013, 3 http://journals.openedition.org/rfsic/630

CASILLI, Antonio, Digital Labor studies go global: toward a digital decolonial turn." International Journal of Communication, 11, 2017, p.3934-3954

COULDRY, Nick, MEJIAS, Ulises, « Le colonialisme des données : repenser la relation entre le big data et le sujet contemporain », *Questions de communication*, 42, 2022, http://journals.openedition.org/questionsdecommunication/29845 ;

COULDRY, Nick, MEJIAS, Ulises, « The decolonial turn in data and technology research: what is at stake and where is it heading? », *Information, Communication & Society*, 2021 DOI: 10.1080/1369118X.2021.1986102

DAHDAH AL, M., QUET, Quet, « Between Tech and Trade, the Digital Turn in Development Policies », *Development*, 2020, 63, p.219–225, https://doi.org/10.1057/s41301-020-00272-y

DOUZET, Frédérick, « La géopolitique pour comprendre le cyberespace », *Hérodote*, 2014/1-2 (n° 152-153), p. 3-21, https://www.cairn.info/revue-herodote-2014-1-page-3.htm

Existing Democracy », *Social Text*, 1990, 25/26, p. 56-80.

FAST, Larissa, « Diverging Data: Exploring the Epistemologies of Data Collection and Use among Those Working on and in Conflict », *International Peacekeeping*, 24 (5), 2017, p.796-732, https://doi.org/10.1080/13533312.2017.1383562

FRASER, Nancy, « Rethinking the Public Sphere: A Contribution to the Critique of Actually

FUCHS, C., « Towards an alternative concept of privacy », *Journal of Information, Communication and Ethics in Society*, vol. 9 n° 4, p. 220-237

GILLESPIE, Marie, OSSEIRAN, Souad, CHEESMAN, Margie, "Syrian Refugees and the Digital Passage to Europe: Smartphone Infrastructures and Affordances", *Social Media+ Society*, 2018, p. 1–12https://journals.sagepub.com/doi/pdf/10.1177/2056305118764440

LAURENT, Catherine, BAUDRY Jacques, BERRIET-SOLLIEC, Marielle, *(et al.)*, « Pourquoi s'intéresser à la notion d' « evidence-based policy » ? », *Revue Tiers Monde*, 2009/4 (n° 200), p. 853-873. https://www.cairn.info/revue-tiers-monde-2009-4-page-853.htm

MACIAS, Léa, « La mise en nombre des réfugiés syriens », *Socio-anthropologie*, 40, 2019, http://journals.openedition.org/socio-anthropologie/5664

MADIANOU, M., "Technocolonialism: Digital Innovation and Data Practices in the Humanitarian Response to Refugee Crises", *Social Media + Society*, *5*(3), 2019. https://doi.org/10.1177/2056305119863146

MEIER, Patrick, « New information technologies and their impact on the humanitarian sector », *International Review of the Red Cross*, Vol. 93, N° 884, décembre 2011, p. 1239-1263. https://international-review.icrc.org/sites/default/files/irrc-884-meier.pdf

MEJIAS, U., COULDRY, N., "Datafication.", *Internet Policy Review*, 8(4)., 2019, https://doi.org/10.14763/2019.4.1428

NISSENBAUM H., « Privacy as Contextual Integrity », *Washington Law Review*, 2004, 79, 1,
p. 119-158.

PANDOLFI, Marelia, CORBET,Alice, « De l'humanitaire imparfait», *Ethnologie française*, 2011, 3 (Vol. 41) p.465-472. 10.3917/ethn.113.0465. halshs-02284815

REY, Bénédicte, « La privacy à l'ère du numérique », *Terminal*, 2012, 110, p. 91-103

SEBASTIEN-YVES, Laurent, « Ce que le Cyber (ne) fait (pas) aux Relations internationales. » *Études internationales*, volume 51, numéro 2, été 2020, p. 209–234. https://doi.org/10.7202/1084457ar

SHRINKHAL, R.,“Indigenous sovereignty” and right to self-determination in international law: a critical appraisal”, *AlterNative: An International Journal of Indigenous Peoples*, *17*(1), 2021,p. 71–82. https://doi.org/10.1177/1177180121994681

SOLOVE, Daniel J., “A Taxonomy of Privacy”, University of Pennsylvania Law Review, vol. 154, no. 3,2006. https://scholarship.law.upenn.edu/penn_law_review/vol154/iss3/1

TAYLOR, Linnet, “What is data justice? The case for connecting digital rights and freedoms globally”, *Big Data & Society*, VL 4, 2017.

WARREN S.D., BRANDEIS L.D., « The Right to Privacy », *Harvard Law Review*, 1890, 4/ 5, p. 193-220

OUVRAGES

AGIER, Michel, *Gouverner les indésirables, des camps de réfugiés au gouvernement humanitaire*, Paris, Flammarion, 2008, 352p.

BENNETT, Colin J. *The Privacy Advocates: Resisting the Spread of Surveillance*, Massachusetts : The MIT Press, 2008,p.288

BOERSMA Kees, FONIO Chiara, *Big data surveillance and crisis management* Routledge studies in surveillance, 2019, p.246

BOERSMA Kees, FONIO Chiara, *Big data surveillance and crisis management* Routledge studies in surveillance, 2019, p.246

COULDRY, Nick, *MEJIAS, Ulises, The Cost of conection*, Palo Alto, Standford University Press, 2019, 352 p.

DAUVIN Pascal, SIMEANT-GERMANOS Johanna, *Le travail humanitaire. Les acteurs des ONG, du siège au terrain.* Presses de Sciences Po, « Académique », 2002, 444p.

DUFFIELD Mark, *Post humanitarianism governing precarity in the digital world*, Cambridge : Polity Press, 2019.

ECKEL, Jan, *The Ambivalence of Good, Human Rights in International Politics since the 1940s,* Oxford : Oxford Studies in Modern european history, 2019, 456 p.

FORSYTHE, D. *The Humanitarians: The International Committee of the Red Cross*, Cambridge University Press, 2005, 374 p.

GILLIOM J., *Overseers of the poor: surveillance, resistance, and the limits of privacy*, Chicago: University of Chicago Press, 2001, 277 p.

GLASMAN Joël, *Humanitarianism and the Quantification of Human Needs. Minimal Humanity*, New York : Routledge, 2020, p.274

GONZÁLEZ FUSTER G., *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Dordrecht: Springer, 2014, 292 p.

HABERMAS, J, *L'espace public: archéologie de la publicité comme dimension constitutive de la société bourgeoise,* Paris : Payot, 1988,324 p.

HOURS Bernard, *L'Idéologie humanitaire ou la spectacle de l'altérité perdue*, Paris: Les Éditions L'Harmattan, 1998,173 p.

MIRCA, Madianou, *Technocolonialism: When Technology for good is harmful*, Cambridge : Polity, 2024, 264 p.

MCDONALD Sean, *Ebola: A Big Data Disaster*, The Centre for internet and society, 2016. https://cis-india.org/papers/ebola-a-big-data-disaster

NISSENBAUM H.F., *Privacy in context: technology, policy, and the integrity of social life*, Stanford : Stanford Law Books, 2010, 304 p.

SANDVIK Kristin, LINDSKOV Jacobsen Katja, (eds), *UNHCR and the Struggle for Accountability, Technology, law and results-based management*, Routledge, Taylor & Francis Group, 2017, 194 p.

SANDVIK, Kristin, *Humanitarian extractivism : the digital transformation of aid*, Manchester University Press, 2023, 168 p.

WESTIN Alan, *Privacy And Freedom*, New York : Atheneum, 1967,487 p.

ZUBOFF, Shoshana, *L'Age du capitalisme de surveillance*, Paris : Zulma, 2020, 864 p.

CHAPITRES D'OUVRAGE

HOURS Bernard, « Les marchandises morales globales ou le blanchiment du capitalisme In : BAUMANN Eveline, BAZIN Laurent , OULD Ahmed Pepita, PHELINAS Pascale, SELIM Monique, SOBEL Richard (dir.). *Anthropologues et économistes face à la globalisation* Paris : L'Harmattan, 2008, p. 77-86.

PÉROUSE DE MONTCLOS, Marc-Antoine. *Le bilan impossible. Limites de l'évaluation et du contrôle* In : *Pour un développement « humanitaire » ? Les ONG à l'épreuve de la critique*, Marseille : IRD Éditions, 2015

RAYMOND, Nathaniel, « Beyond "Do No Harm" and Individual Consent: Reckoning with the Emerging Ethical Challenges of Civil Society's Use of Data ». In : VAN DER SLOOT, Bart, FLORIDI,Luciano, TAYLOR, Linnet, (eds.), *Group Privacy* ; Springer Verlag, 2017

THESES ET MEMOIRES

COLLOMB C., « Un concept technologique de trace numérique », Thèse de doctorat, Sciences de l'information et de la communication, Université de technologie de Compiègne et Université libre de Bruxelles,2016

CONFÉRENCES

ACQUISTI A., GROSS R., « Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook », Proceedings of the 6th International Conference on Privacy Enhancing Technologies,2006, p. 36-58.

Littérature grise

ARTICLES DE JOURNAL

LATONERO Mark, « Stop Surveillance Humanitarianism », *The New York Times*, 11/07/2019.

ARTICLES DE BLOG

BRAUMAN, Rony, “L’Action humanitaire”, CRASH, https://msf-crash.org/fr/publications/acteurs-et-pratiques-humanitaires/laction-humanitaire

DEVIDAL, Pierrick, ""Back to basic" with a digital twist: humanitarian principles and dilemmas in the digital age.", *ICRC Humanitarian Law & Policy*, 02/02/2023, https://blogs.icrc.org/law-and-policy/2023/02/02/back-to-basics-digital-twist-humanitarian-principles/

RAPPORTS

KAURIN, Dragana,” Data Protection and Digital Agency for Refugees”, World Refugee Council Research Paper No. 12 — Mai 2019, https://www.cigionline.org/static/documents/documents/WRC%20Research%20Paper%20no.12.pdf

OCHA UN foundation, vodafone foundation, « Disaster Relief 2.0: The Future of Information Sharing in Humanitarian Emergencies », 2011, https://hhi.harvard.edu/publications/disaster-relief-20-future-information-sharing-humanitarian

Privacy international, “Exposing Surveillance in Humanitarian and Development Initiatives”, May 2018 https://privacyinternational.org/impact/exposing-surveillance-humanitarian-and-development-initiatives

SCHOEMAKER Emrys, CURRION Paul, PON Bryan, « identity at the margins : identification system for refugees », *Caribou digital*, 2018, https://assets.publishing.service.gov.uk/media/5cecedd6ed915d2475aca8c5/Identity-At-The-Margins-Identification-Systems-for-Refugees.pdf

SCHOEMAKER, Emrys, CURRION, Paul, PON, Bryan, « identity at the margins : identification system for refugees », *Caribou digital*, 2018, https://assets.publishing.service.gov.uk/media/5cecedd6ed915d2475aca8c5/Identity-At-The-Margins-Identification-Systems-for-Refugees.pdf

VINCK Patrick, *Humanitarian Technology, World Disasters Report 2013*, International Federation of Red Cross and Red Crescent Societies, 2013, www.ifrc.org/PageFiles/134658/WDR%202013%20complete.pdf

Documents juridiques et droit souple

KUNER, Christopher, MARELLI Massimo, “Handbook on data protection in humanitarian action”, second edition, 2020

GREENWOOD, Faine, HOWARTH, Caitlin, POOL, Danielle, RAYMOND, Nathaniel, SCARNECCHIA , Daniel, “The Signal Code : A Human Rights Approach to information during Crisis”, Harvard Humanitarian Initiative, 2017.

Chapitre 1

## Littérature scientifique

### ARTICLES


AGIER, Michel, « Le biopouvoir à l'épreuve de ses formes sensibles. Brève introduction à un projet d'ethnographie des hétérotopies contemporaines », *Chimères*, 2010/3 (N° 74), p. 259-270. https://www.cairn.info/revue-chimeres-2010-3-page-259.htm

AGIER, Michel, « Penser le sujet, observer la frontière », *L'Homme* , 203-204 | 2012, http://journals.openedition.org/lhomme/23096

AL DAHDAH Marine, « Between Philanthropy and Big Business: The Rise of mHealth in the Global Health Market », *Development and change*, Volume 53, issue 2, 2022, p.376-395.

AL DAHDAH, Marine, « Les géants du numérique au chevet de l'Afrique. Le téléphone portable comme nouvel outil de santé globale », *Politique africaine*, 2019/4 (n°156), p.101-1019, https://www.cairn.info/revue-politique-africaine-2019-4-page-101.htm

ARADAU, Claudia "Experimentality, Surplus Data and the Politics of Debilitation in Borderzones". *Geopolitics*,27(1), 2022, p.26-46

BARDELLI, Nora, « Entre témoignage et biométrie : la production du « réfugié » au Burkina Faso », *Politique africaine*, 2018/4 (n° 152), p. 121-140. https://www.cairn.info/revue-politique-africaine-2018-4-page-121.htm

BLOOM, Louise, ROMY, Faulkner, "Innovation spaces, transforming humanitarian practice in the United nations",Working paper, Refugee studies centre, Oxford, 2015

BLOOM, Louise, BETTS, Alexander, "The two worlds of humanitarian innovation", Working paper, Refugee studies centre, 2013

BOSVIEUX-ONYEKWELU Charles, BOUSSARD Valérie, « Moraliser le capitalisme ou capitaliser sur la morale ? », *Actes de la recherche en sciences sociales*, 2022/1 (N° 241), p. 4-15. https://www.cairn.info/revue-actes-de-la-recherche-en-sciences-sociales-2022-1-page-4.htm

CAMPAGNE, Gérard, CHIPPAUX, Jean-Philippe, GARBA, Amadou, « Information et recueil du consentement parental au Niger », *Autrepart*, 2003/4 (n° 28), p. 111-124. https://www.cairn.info/revue-autrepart-2003-4-page-111.htm

CROSS, Jamie, "The 100th object : solar lighting technology and humanitarian good", *Journal of Material culture*, 0(0) 1-21, 2013 https://pure.manchester.ac.uk/ws/portalfiles/portal/216123131/FULL_TEXT.PDF

DE MONTJOYE, Y-A, HIDALGO, C., VERLEYSEN, M., BLONDEL, V.D. "Unique in the crowd: The privacy bounds of human mobility", *Sci Rep* 3, 2013

DIMINESCU, Dana, « Le Migrant connecté : pour un manifeste épistémologique », *Migrations/Société*, vol.17, n° 102, p. 275-292

DIMINESCU, Dana, NICOLOSI, Guido, « Les risques et les opportunités de la migration « connectée » », *Socio-anthropologie*, 40 | 2019, http://journals.openedition.org/socio-anthropologie/6330

DIJCK VAN, J, « Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology », *Surveillance & Society*, 2014, 12/ 2, p. 197-208

DONGUS, Ariana, "Galton's Utopia. Data accumulation in biometric capitalism spheres", *Journal for Digital Cultures. Spectres of AI*,2019, Nr. 5, p.1–16 https://spheres-journal.org/wp-content/uploads/spheres-5_Dongus.pdf

DUFFIELD, Mark, "The resilience of the ruins: towards a critique of digital humanitarianism", *Resilience*, 4:3, 2016,p. 147-165.

EKDALE, Brian, TULLY, Melissa, "African Elections as a Testing Ground: Comparing Coverage of Cambridge Analytica in Nigerian and Kenyan Newspapers", *African Journalism Studies*, 40:4, 2019, p. 27-43.

GAZI, Theodora, GAZIS, Alexandros," Humanitarian aid in the age of COVID-19: A review of big data crisis analytics and the General Data Protection Regulation." 2021, https://international-review.icrc.org/sites/default/files/reviews-pdf/2021-03/humanitarian-aid-covid-19-big-data-crisis-analytics-gdpr-913.pdf

GALINON-MÉLÉNEC B. (dir.),*L'homme-trace : perspectives anthropologiques des traces contemporaines*, Paris, CNRS-édition,2011, 412 p.

GODIN B., « Making sense of innovation: from weapon to instrument to buzzword »,
*Quaderni,* 2016, 90, p. 21-40.

GRABOYES, Melissa, "Introduction: Incorporating Medical Research into the History of Medicine in East Africa." *The International Journal of African Historical Studies*, vol. 47, no. 3, 2014, p. 379–98, http://www.jstor.org/stable/24393435.

JACOBSEN, K. L. "Experimentation in humanitarian locations: UNHCR and biometric registration of Afghan refugees",2015, *Security Dialogue*, *46*(2), p.144-164.

JACOBSEN, Katja, "Biometric data flows and unintended consequences of counterterrorism", *IRRC* No. 916-917 February 2022 https://international-review.icrc.org/articles/biometric-data-flows-and-unintended-consequences-of-counterterrorism-916#footnoteref16_5yqioe0

KLEIN-KELL, Nathalie, "More humanitarian accountability, less humanitarian access? Alternative ideas on accountability for protection activities in conflict settings", *international Review of the Red Cross*, 2018, 100 (1-2-3),p. 287–313

LOCKHART, Andy, WHILE, Aidan, MARVIN, Simon, KOVACIC, Mateja, ODENDAAL, Nancy, ALEXANDER, Christian, "Making space for drones: the contested reregulation of airspace in Tanzania and Rwanda", *Transactions of the institute of british geographers*, Volume 46, 4, 2021, p.850-865

LEFEVRE, Sylvain A, LANGEVIN, Marie, « Mastercard, sa fondation et l'inclusion financière : une entreprise philanthropique ? », *Revue française de sociologie*, 2020/4 (Vol. 61), p. 587-615, https://www.cairn.info/revue-francaise-de-sociologie-2020-4-page-587.htm

MACASKILL, William, GREAVES, Hilary, "The case for strong longtermism", Global Priorities Institute, GPI Working Paper, n°5-2021

MACIAS, Léa, « Usages expérimentaux des nouvelles technologies par l'action humanitaire : un data colonialisme ? », *Hommes & Migrations*, 2022/2 (n° 1337), p. 11-19. https://www-cairn-info.ezproxy.utc.fr/revue-hommes-et-migrations-2022-2-page-11.htm

MAGALHÃES, João Carlos, COULDRY, Nick, "Taking Away: Big Tech, Data Colonialism, and the Reconfiguration of Social Good", *International Journal of Communication*, 15(2021), p.343–362

MARTIN, Aaron, "Aidwashing Surveillance: Critiquing the Corporate Exploitation of Humanitarian Crise", *Surveillance & Society*, 21 (1), 2023, p.96-102

MEIER Patrick, "New information technologies and their impact on the humanitarian sector », *International Review of the Red Cross*, Vol. 93, N° 884,2011, p. 1239-1263.

NOTHIAS, Toussaint, "Access granted: Facebook's free basics in Africa", *Media, Culture & Society*, *42*(3), p.329-348. https://doi.org/10.1177/0163443719890530

READ, Róisín, TAITHE, Bertrand , MAC GINTY, Roger, "Data hubris? Humanitarian information systems and the mirage of technology", *Third World Quarterly*, 2016, 37:8, p.1314-1331, DOI: 10.1080/01436597.2015.1136208

ROCA,Thomas, LETOUZE, Emmanuel, « La révolution des données est-elle en marche ? Implications pour la statistique publique et la démocratie », Afrique contemporaine, 2016/2 (n° 258), p. 95-111. https://www.cairn.info/revue-afrique-contemporaine1-2016-2-page-95.htm

SANDVIK, Kristin, "African Drone stories", *BEHEMOTH A Journal on Civilization*, 2015, Volume 8 Issue No. 2

SANDVIK, Kristin, « Now is the time to deliver: looking for humanitarian innovation's theory of change », *Int J Humanitarian Action* (2, 8), 2017 https://doi.org/10.1186/s41018-017-0023-2

SANDVIK, Kristin, LINDSKOV JACOBSEN, Katja, MCDONALD, Sean Martin, "Do no harm : a taxonomy of the Challenges of humanitarian experimentation", *International Review of the Red Cross*, 2017, 99 (1), p.319–344.

SCOTT SMITH, Tom, « Humanitarian neophilia: the 'innovation turn' and its implications », *Third World Quarterly*, 37:12,2016 p.2229-2251, DOI: 10.1080/01436597.2016.1176856

SCOTT-SMITH, Tom "The fetishism of humanitarian objects and the management of malnutrition in emergencies", *Third World Quarterly*, 34:5,2013, p. 913-928, 10.1080/01436597.2013.800749

TAYLOR, L. "The ethics of big data as a public good: which public? Whose good? ", *Philos Trans A Math Phys Eng Sci*., 2016, 28, 374(2083)

TAYLOR, L. , MEISSNER, F., “A Crisis of Opportunity: Market-Making, Big Data, and the Consolidation of Migration as Risk”, *Antipode*, 52, 2020, p.270-290

TAYLOR, L., BROEDERS, D., “In the name of development: Power, profit and the datafication of the Global South”, *Geoforum*, 64, 2015, p. 229–237.

TAYLOR, L., SCHROEDER, R, “Is bigger better? The emergence of big data as a tool for international development policy”, *GeoJournal* 80, 2015, p. 503–518 https://doi.org/10.1007/s10708-014-9603-5

TWIGT, Mirjam, “Doing Refugee Right(s) with Technologies? Humanitarian Crises and the Multiplication of “Exceptional” Legal States”, *Refugee Survey Quarterly*, volume 43, Issue 1, 2023, https://doi.org/10.1093/rsq/hdad020

WANG, Ning, ""We Live on Hope...": Ethical Considerations of Humanitarian Use of Drones in Post-Disaster Nepal," in *IEEE Technology and Society Magazine*, vol. 39, no. 3, 2020, p. 76-85, doi: 10.1109/MTS.2020.3012332

WINNER L., « Do Artifacts Have Politics? », *Daedalus*, 1980, (109, 1), p. 121-136

OUVRAGES

AGIER, Michel, *Gérer les indésirables, des camps de réfugiés au gouvernement humain*, Paris : Flammarion, 2008,350 p.

AMIEL, Philippe, *Des cobayes et des hommes : expérimentation sur l’être humain et justice*, Paris, Belles Lettres, 2011,344 p.

CHAMAYOU, Grégoire, *Les corps vils: expérimenter sur les êtres humains aux XVIIIème et XIXème siècle*, Paris : La Découvertez, 2014, 424 p.

CHENEAU-LOQUAY, Annie, LENOBLE-BART, Annie (dir.), *Les médias africains à l’heure du numérique*, L’Harmattan, Netsuds, n° 5, septembre 2010, 133 p.

COOPER, Frederick, STOLER, Ann Laura (eds), *Tensions of Empire: Colonial Cultures in a Bourgeois World*, University of California Press, 1997, 463 p.

CROWCROF, Jon, BOERSMA Kees, FONIO Chiara, *Big data surveillance and crisis management*, London : Routledge studies in surveillance, 2019, 256 p.

DIDIER, Emmanuel, BRUNO, Isabelle, *Benchmarking, l'Etat sous pression statistique*, Paris: éditions la Découverte, Zones, 2013, 250 p.

FEJERSKOV, Adam, *The Global lab : inequality, technology, and the experimental movement*, Oxford University Press, 2022, 224 p.

FERGUSON, James, *The anti-politics machine, development, depoliticization, and bureaucratic power in Lesotho*, Minnesota University press, 1994, 336 p.

FOUCAULT, *Il faut défendre la société, : Cours au collège de France*, Paris, Seuil, 1997, 283 p.

GLASMAN, Joel, *Humanitarianism and the Quantification of human needs, minimal humanity*, London, Routledge, Taylor & Francis Group, 2020, 274 p.

JACOBSEN, Katja, *The politics of humanitarian technology, Good intentions, unintended consequences and insecurity*, Routledge studies in conflict, security and technology,2015,208 p.

LACHENAL, Guillaume, *Le médecin qui voulut être roi. Sur les traces d'une utopie coloniale*, Paris : Seuil, 2017, 353 p

LATOUR Bruno, *Pasteur : guerre et paix des microbes. Suivi de Irréductions,* Paris : La Découverte, « Poche / Sciences humaines et sociales », 2011, 364 p.

LYON, D, *The Electronic Eye: The Rise of Surveillance Society*, University of Minnesota Press, 1994, 290 p.

LYON, D, *Surveillance After Snowden*, Cambridge, Mass., Polity Pres, 2015,196 p.

MADIANOU, Mirca, *Technocolonialism : When Technology for good is harmful*,Polity Press, 2024, 234 p. ( à paraitre)

MATTELART A., *La globalisation de la surveillance: aux origines de l'ordre sécuritaire*, Paris : Découverte, 2007,266 p.

MCDONALD, Sean Martin, *Ebola : a big data disaster, privacy, property, and the law of disaster experimentation*, The Censer for internet & society Paper, 2016

MEIER, Patrick, *Digital humanitarians : how big data is changing the face of humanitarian response,* London : Routledge, 2015, 259 p.

MOLNAR, Petra, *The Walls have eyes, Surviving migration in the age of Artificial intelligence*, New Press, 2024, 320 p

ORD, Toby, *The Precipice: Existential Risk and the Future of Humanity*, London : Bloomsbury Publishing Plc, 2020, 480 p.

OWENS, Patricia, "*The Boomerang Effect: On the Imperial Origins of Total War",* Between *War and Politics: International Relations and the Thought of Hannah Arendt*, Oxford University Press, 2007, 232 p.

PETRYNA, Adriana, *When experiments travel, Clinical trials and the global search for human subjects*, Princeton university press, 2009, 272 p.

SANDVIK, Kristin, GABRIELSEN JUMBERT, Maria (ed.), *The Good drone,* Routledge, 2016, 212 p

TILLEY, Helen, *Africa as a living laboratory: empire, development, and the problem of scientific knowledge, 1870-1950*, University of Chicago Press, 2011, 520 p

### CHAPITRES D'OUVRAGES

BARNETT, Michael, "Neoliberalism, Philanthropy, and Humanitarianism", in MITCHELL, Katharyne, PALLISTER-WILKINS, Polly, *The Routledge International Handbook of Critical Philanthropy and Humanitarianism,* London: Routledge,2023, 332 p.

BLANCHARD, Emmanuel, « Conclusion : Les forces de l'ordre colonial, entre conservatoires et laboratoires policiers. » DENYS, C., DENIS V., (dir.). *Polices d'Empires, XVIIIe-XIXe siècles*, Presses Universitaires de Rennes, 2012, p.171-187

BURCHARDT, Marian, UMLAUF, René, "Dreams and realities of infrastructural leapfrogging: airspace, drone corridors, and logistic in African healthcare, in BURCHARDT, Marian, LAAK, Dirk (ed.), *Making spaces through infrastructure : visions, technologies, and tensions*,Berlin: De Gruyter Oldenbourg, 2023, p. 221-240

GALIT, Sarfaty, "Corporate Data Responsibility", in: DICKINSON, Laura, BERG, Edward (ed.) , *Big Data and Armed Conflict: Legal Issues Above and Below the Armed Conflict Threshold*, Oxford University Press, 2022

GOMEZ-TEMESIO, Veronica, LE MARCIS, Frédéric, « Governing lives in the times of global health », *in:* PEDERSEN Lene, CLIGGET, Lisa, (dir.), *The SAGE handbook of cultural anthropology*, SAGE Publications Ltd, 2021, p. 554-578.

GREENWOOD, Faine, "Data Colonialism, Surveillance Capitalism and Drones." *Mapping Crisis: Participation, Datafication and Humanitarianism in the Age of Digital Mapping*, edited by Doug Specht, University of London Press, 2020, p. 89–118.

LATOUR, Bruno, "Give me a laboratory and I will raise the World", in KNORR-CETINA, Karin, MULKAY, Michael (ed.), *Science observed, perspectives on the social study of science*, London: Sage Publication, 1983, p.141-169

MITCHELL, Katharyne, PALLISTER-WILKINS, Polly, "Monopoly Philanthropy and the Humanitarian New World Order", in MITCHELL, Katharyne, PALLISTER-WILKINS, Polly, *The Routledge International Handbook of Critical Philanthropy and Humanitarianism*, Routledge,2023, p.1-6

ZWITTER, Andrej," International Humanitarian and Development Aid and Big Data Governance", in SCHIPPERS, Birgit, *The Routledge handbook to rethinking ethics in international relations, Londo*n : Routledge, 2020, p.428

### THÈSES ET MÉMOIRES

BURNS, R. "Digital Humanitarianism and the Geospatial Web: Emerging Modes of Mapping and the Transformation of Humanitarian Practices",Thesis, Geography, University of Washington, 2015, http://hdl.handle.net/1773/33947

SCHLAEPFER, Isabelle, "Humanitarian technologies as sociotechnical imaginaries, how multi-national companies impact on the idea of humanitarian action through technologies", Doctoral thesis, School of Arts, Languages and Cultures, University of Manchester, 2020, https://pure.manchester.ac.uk/ws/portalfiles/portal/216123131/FULL_TEXT.PDF

### CONFÉRENCES

EAGLE, Nathan, MONTJOYE, Yves-Alexandre, LUIS, Bettencourt, "Community Computing: Comparisons between Rural and Urban Societies Using Mobile Phone Data", *IEEE international conference on computational science and engineering*, 2009, p. 144-150. 10.1109/CSE.2009.91

MAAS, Paige, IYER, Shankar, GROS, Andreas, PARK, Wonhee, MCGORMAN, Laura, NAYAK, Chaya, DOW, Alex, "Facebook disaster maps: aggregate insights for crisis response & recovery",White Paper – Social Media in Crisis

and Conflicts Proceedings of the 16th ISCRAM Conference – València, Spain May 2019 https://idl.iscram.org/files/paigemaas/2019/1912_PaigeMaas_etal2019.pdf

**Littérature grise**

ARTICLES DE JOURNAUX

"How a tide of tech money is transforming charity", *The Economist*, 09/02/2023https://www.economist.com/international/2023/02/09/how-a-tide-of-tech-money-is-transforming-charity

ALY, Heba, "What future for private sector involvement in humanitarianism?", *The New humanitarian*, 23/08/2013 https://www.thenewhumanitarian.org/analysis/2013/08/26/what-future-private-sector-involvement-humanitarianism

APPLEYARD, Bryan, "The charity algorithm : how Silicon Valley philanthropy turned sour", *The Newstatesman*, 16/01/2019. https://www.newstatesman.com/science-tech/2019/01/the-charity-algorithm-how-silicon-valley-philanthropy-turned-sour

BEASLEY, Stephanie, CHENEY, Catherine," Tech entrepreneurs bring new approaches, challenges to philanthropy", *Devex*,24/01/2022 https://www.devex.com/news/tech-entrepreneurs-bring-new-approaches-challenges-to-philanthropy-102174

BEAUTY, Thalia, Associated Press, "Microsoft tops the list of largest private donors to Ulraine with $430 million - but Google also made the cut", *Fortune*, 23/02/2023, https://fortune.com/europe/2023/02/23/ukraine-war-top-private-donors-microsoft-google/

CHENEY, Catherine, "Why a drone startup that launched with a humanitarian focus is switching gears", *Devex*, 07/06/2019 https://www.devex.com/news/why-a-drone-startup-that-launched-with-a-humanitarian-focus-is-switching-gears-95057

CHENEY, Catherine, "Facebook introduces disaster maps", *Devex*, 07/06/2017 https://www.devex.com/news/facebook-introduces-disaster-maps-announces-early-partners-90427

CHENEY, Catherine, "What the Facebook scandal means for "data for good", *Devex,* 06/04/2018, https://www.devex.com/news/what-the-facebook-scandal-means-for-data-for-good-92425

CHENEY, Catherine, "A robotics group offers ideas to 'shift power' to drive localization", *Devex*, 14/04/2022 https://www.devex.com/news/a-robotics-group-offers-ideas-to-shift-power-to-drive-localization-102987

CHIPPAUX, Jean-Philippe, « L'Afrique, cobaye de Big Pharma », *Le Monde diplomatique*, juin 2005https://www.monde-diplomatique.fr/2005/06/CHIPPAUX/12513

CIESIELSKI, Rebeca, ZIERER, Maximilian, "How biometric devices are putting afghans in danger", *Interaktiv, Br24*, 27/12/2022, https://interaktiv.br.de/biometrie-afghanistan/en/index.html

DHUNNA AHMAD, Tazeen, "Refugee hackathons and 3D printing : apps for the world's displaced people", *The Guardian*, 20/06/2017 https://www.theguardian.com/voluntary-sector-network/2017/jun/20/hackathons-3d-printing-prosthetics-technology-world-refugee-day

EBOKO, Fred, "Non, l'Afrique n'est pas, ni de près ni de loin, la cible privilégiée des essais cliniques", *Le Monde*, 08/04/2020https://www.lemonde.fr/afrique/article/2020/04/08/non-l-afrique-n-est-pas-ni-de-pres-ni-de-loin-la-cible-privilegiee-des-essais-cliniques_6035948_3212.html

KIRKPATRICK, Robert, "Data philanthropy is good for business", *Forbes*, 20/09/2011 https://www.forbes.com/sites/oreillymedia/2011/09/20/data-philanthropy-is-good-for-business/?sh=63d8bcaa5f70

KIRKPATRICK, Robert, "A new type of philanthropy : donating data", *Harvard Business Review*, 21/03/2013 https://hbr.org/2013/03/a-new-type-of-philanthropy-don

LEETARU, Kalev, "Are Facebook's disaster maps the Ultimate government surveillance tool in disguise?", *Forbes*,05/05/2019 Are Facebook's Disaster Maps The Ultimate Government Surveillance Tool In Disguise? (forbes.com)

MACAIRE, EYENGA, George, « Drone médicaux, Comment Zipline redéfinit la délivrance des soins de santé en Afrique », *Afrique XXI*, 07/09/2022 https://afriquexxi.info/Comment-Zipline-redefinit-la-delivrance-des-soins-de-sante-en-Afrique

MACASKILL, William, "What is the most effective way to help refugees?", *The Guardian*, 04/09/2015https://www.theguardian.com/commentisfree/2015/sep/04/help-refugees-donations-government-political-action

NOVECK, Beth Simone, "Data Collaboratives: Sharing Public Data in Private Hands for Social Good", *FORBES*,24/09/2015, https://www.forbes.com/sites/bethsimonenoveck/2015/09/24/private-data-sharing-for-public-good/#397107b351cd

ORSINI, Alexis, « Applis, startups, hackathons... quand la tech vient en aide aux migrants », *Numerama*, 18/12/2017, https://www.numerama.com/politique/312100-applis-startups-hackathons-quand-la-tech-vient-en-aide-aux-migrants.html

PARKER, Ben, "Humanitarian Innovation faces rethink as innovators take stock", *The New Humanitarian*, 20/03/2019 https://www.thenewhumanitarian.org/analysis/2019/03/20/humanitarian-innovation-faces-rethink-innovators-take-stock

PREVOST, Thibault, « Ukraine : Airbnb, votre nouvelle ONG préférée », *Arrêt sur images*, *Clic gauche,* 27/03/2022. https://www.arretsurimages.net/chroniques/clic-gauche/ukraine-airbnb-votre-nouvelle-ong-preferee

RAMALINGAM, Ben, "New Ideas can transform aid delivery", *The Guardian*, 22/02/2011, https://www.theguardian.com/global-development/poverty-matters/2011/feb/22/humanitarian-aid-innovation

SEMUELS, Alana, "How Silicon Valley has disrupted philanthropy", *The Atlantic*, 25/07/2018 https://www.theatlantic.com/technology/archive/2018/07/how-silicon-valley-has-disrupted-philanthropy/565997/

SIEGFRIED, Kristy, "Surveillance for good? Facebook tracks disaster victims", *The New humanitarian*, 08/06/2017https://www.thenewhumanitarian.org/special-report/2017/06/08/surveillance-good-facebook-tracks-disaster-victims

THOMPSON,A., Stuart, WARZEL, Charlie," Twelve million phones, one dataset, zero privacy", *The New York Times*, 19/12/2019 https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html

TOBIN, Meaghan, "How facebook discover replicated many of the free basics'mistakes", *Rest of world,* 08/06/2021https://restofworld.org/2021/facebook-connectivity-discover/

WILLE, Belkis, "You don't need to demand sensitive biometric data to give aid. The Ukraine response shows how", *The New humanitarian* 11/07/2023, https://www.thenewhumanitarian.org/opinion/2023/07/11/you-dont-need-demand-sensitive-biometric-data-give-aid-ukraine-response-shows

DAOUD Lisa, WATCH Edmond, « Les technologies de l'information : le cache-misère d'un secteur en manque d'agilité ? », Revue HEM, URD, 26/03/2019. https://www.urd.org/fr/revue_humanitaires/les-technologies-de-linformation-le-cache-misere-dun-secteur-en-manque-dagilite/

ARTICLES DE BLOGS

"Exploring The Mosaic Effect On HDX Datasets", *Centre for humanitarian data*, 20/07/2020, https://centre humdata.org/exploring-the-mosaic-effect-on-hdx-datasets/.

"Facebook data for good population density maps and how they are helping the nonprofit sector", Nethope 29/01/2021https://nethope.org/articles/facebook-data-for-good-population-density-maps-and-how-they-are-helping-the-nonprofit-sector/

"Meta's ongoing efforts regarding Russia's invasion of Ukraine", *Facebook* 26/02/2022. https://about.fb.com/news/2022/02/metas-ongoing-efforts-regarding-russias-invasion-of-ukraine/

BERENS Jos, "Private Sector Data for Humanitarian Response: Closing the Gaps", *Bloombergneweconomy* https://www.bloombergneweconomy.com/news/private-sector-data-for-humanitarian-response/

BERENS Jos, "Private Sector Data for Humanitarian Response: Closing the Gaps", Bloombergneweconomy https://www.bloombergneweconomy.com/news/private-sector-data-for-humanitarian-response/

GLASMAN, Joel, « L'invention de l'impartialité: historique d'un principe humanitaire, entre raison juridique, stratégique et algorithmique », CRASH, MSF, 18/11/2020 https://msf-crash.org/fr/linvention-de-limpartialite-histoire-dun-principe-humanitaire-entre-raisons-juridique-strategique

GRAF, Vanessa, "Refugee camps as proving grounds for new technologies : Ariana Dongus, Ars Electronica, 27/08/2018, https://ars.electronica.art/aeblog/en/2018/08/27/ariana-dongus/

GREENWOOD, Faine, "The crucial need to secure the location data of vulnerable populations", *Brookings*, 17/12/2021 https://www.brookings.edu/articles/the-crucial-need-to-secure-the-location-data-of-vulnerable-populations/

MCDONAL, Sean Martin, SANDVIK, Kristin, JACOBSEN, Katja," From principle to practice : humanitarian innovation and experimentation", *Norwegian centre for humanitarian studies, Blog,* 22/12/2017https://www.humanitarianstudies.no/from-principle-to-practice-humanitarian-innovation-and-experimentation/

MCDONALD, Paul, "Understanding updates to your device's location setting", 9/09/2019 https://about.fb.com/news/2019/09/understanding-updates-to-your-devices-location-settings/

MCDONALD, Sean Martin, "Data Reiew Boards: Facebook, data governance and trusts in practice",*Digital Impact*, 03/04/2018, https://digitalimpact.io/data-review-boards-facebook-data-governance-and-trusts-in-practice/

MEIER, Patrick, "Big Data philanthropy for humanitarian response", *Irevolution*, 04/06/2012 https://irevolutions.org/2012/06/04/big-data-philanthropy-for-humanitarian-response/

MOROZOV, Evgeny, » A l'ère numérique, le capitalisme compatissant », *Le Monde diplomatique*, 2 juillet 2016,https://blog.mondediplo.net/2016-07-02-A-l-ere-numerique-le-capitalisme-compatissant

PAWELKE, Andreas, TATEVOSSIAN, Anoush Rima, "Data Philanthropy: Where Are We Now?" *United Nations Global Pulse Blog*, 08/05/2013 https://www.unglobalpulse.org/data-philanthropy-where-are-we-now

PRIVACY INTERNATIONAL, "Buying a smart phone on the cheap? Privacy might be the price you have to pay, 20/09/2019 https://privacyinternational.org/long-read/3226/buying-smart-phone-cheap-privacy-might-be-price-you-have-pay

SMITH Brad, "Using AI to help save lives", Microsoft blog, 24/09/2018. https://blogs.microsoft.com/on-the-issues/2018/09/24/using-ai-to-help-save-lives/

SMITH, Brad, "Digital technology and the war in Ukraine", blog Microsoft, 28/02/2022.https://blogs.microsoft.com/on-the-issues/2022/02/28/ukraine-russia-digital-war-cyberattacks/

SMITH, Brad, "Extending our vital technology support for Ukraine" blog Microsoft, 11/03/2022, https://blogs.microsoft.com/on-the-issues/2022/11/03/our-tech-support-ukraine/

TODD, Benajamin, MacAskill, William, "Is it ever Ok to take a harmful Job in order to do more good? An in-depth analysis", June 2017, https://80000hours.org/articles/harmful-career/

RAPPORTS

"Facebook data for good, Facebook data for good annual report", Facebook, 2020 https://www.crisisready.io/wp-content/uploads/2021/01/Facebook-Data-for-Good-2020-Annual-Report-1.pdf

"How tech is supporting Ukraine", US Chamber of Commerce, technology engagement center, 2022 https://americaninnovators.com/news/how-tech-is-supporting-ukraine/

"Innovation on the frontline: the impact of technology in Ukraine's humanitarian response", 24/02/2023, https://techtotherescue.prowly.com/231267-innovation-on-the-front-line-the-impact-of-technology-in-ukraines-humanitarian-response

"The tierra common, network Resisting data colonialism a practical intervention", *INC Theory on Demand #50*, Institute of Network Cultures, 2023 https://networkcultures.org/wp-content/uploads/2023/12/ResistingDataColonialism_INC2023_TOD50.pdf

BALSARI, Satchit, BUCKEE, Caroline, CHAN, Jennifer, SCHROEDER, Andrew, "the Use of Human Mobility Data in Public Health Emergencies", *Crisis ready*, April 2022 https://www.crisisready.io/wp-content/uploads/2022/06/The-Use-of-Human-Mobility-Data-in-Public-Health-Emergencies.pdf

BETTS Alexander, BLOOM Louise, "Humanitarian innovation: the state of the art", OCHA, 2014 http://www.unocha.org/node/120957.

COPPI, Giulio, "Mapping humanitarian tech exposing protection gaps in digital transformation programmes", AccessNow, February 2024https://www.accessnow.org/wp-content/uploads/2024/02/Mapping-humanitarian-tech-February-2024.pdf

CULWELL CORTES, Alexa, MCLEOD GRANT, Heather, "The giving code, Sillicon Valley nonprofits and philanthropy", Open/impact, 2016 https://openimpact.io/wp-content/uploads/2022/05/GivingCode_full_download_102516.pdf

DAOUD Lisa, WATCH Edmond, « Les technologies de l'information : le cache-misère d'un secteur en manque d'agilité ? », Revue HEM, URD, 26/03/2019. https://www.urd.org/fr/revue_humanitaires/les-technologies-de-linformation-le-cache-misere-dun-secteur-en-manque-dagilite/

FAST, Larissa, WAUGAMAN, Adele, "Fighting Ebola with Information: Learning From Data andInformation Flows in the West Africa Ebola Response", *USAID*, 2016 https://www.usaid.gov/sites/default/files/2022-05/FightingEbolaWithInformation.pdf

GERSTLE, Talia (et al. ), "Assessing the use of call detail records (CDR) for monitoring mobility and displacement",IOM February 2021, https://www.migrationdataportal.org/sites/g/files/tmzbdl251/files/2021-02/IOM_Princeton_CDRReport_Feb2021_web.pdf

GLEIBERMAN, Mollie, "Effective altruism, doing transhumanism better", working paper, 2023, Insitute of development policy, University of Antwerp https://www.openphilanthropy.org/grants/uc-berkeley-ai-safety-research-2018/

GLENNIE, Alex, BENTON, Meghan, "Digital humanitarianism : how tech entrepreneurs are supporting refugee integration", Migration Policy Institute Octobre 2016 https://www.migrationpolicy.org/sites/default/files/publications/TCM-Asylum-Benton-FINAL.pdf

GREENWOOD, Faine, JOSEPH, Dan, "Aid from the air: A review of drone use in the RCRC global network", American Red Cross , 14/08/2020 https://americanredcross.github.io/rcrc-drones/Aid_from_the_Air.pdf

KOMUHANGI, C., MUGO, H., TANNER, L., GRAY, I., "Assessing the promise of innovation for improving humanitarian performance, a 10-year review for the state of humanitarian system report", *Analp*, 16/10/2023, https://www.alnap.org/help-library/assessing-the-promise-of-innovation-for-improving-humanitarian-performance-a-10-year

LETOUZE, Emmanuel, VINCK, Patrick ,KAMMOURIEH, Lanah, “The law, politics and ethic of cell phone data analytics”, *Datapop alliance*, April 2015, https://datapopalliance.org/wp-content/uploads/2015/04/WPS_LawPoliticsEthicsCellPhoneDataAnalytics.pdf

MARCHAND Eleanor, “Internet governance in displacement“, UNHCR Innovation Service, 2020 https://www.unhcr.org/innovation/wp-content/uploads/2020/04/Internet-Governance-in-Displacement_WEB042020.pdf

MOLNAR, Petra, “Technological Testing Grounds Migration Management Experiments and Reflections from the Ground Up”, 2020, EDRI.https://edri.org/wp-content/uploads/2020/11/Technological-Testing-Grounds.pdf

PICUM, "Digital technology, policing and migration - what does it means for undocumented migrants", 2022, https://picum.org/wp-content/uploads/2022/02/Digital-technology-policing-and-migration-What-does-it-mean-for-undocumented-migrants.pdf

Privacy international, ICRC, "The humanitarian metadata problem: doing no harm in the digital era", October 2018 https://reliefweb.int/report/world/humanitarian-metadata-problem-doing-no-harm-digital-era-october-2018

RAMALINGAM, Ben, SCRIVEN, Kim, FOLEY, Conor, “Innovations in international humanitarian action”, *Calpnetwork*, 2009, https://www.calpnetwork.org/wp-content/uploads/2020/01/8rhach3-2.pdf

The Engine Room, “Biometrics in the humanitarian sector, a current look at risks, benefits and organisational policies”, July 2023 https://www.theengineroom.org/wp-content/uploads/2023/07/TER-Biometrics-Humanitarian-Sector.pdf

UNICEF, “Innovation at UNICEF, From start-up to scale-up”, May 2015. http://archive.unicef.cn/cn/uploadfile/2016/0317/20160317121428604.pdf

VAN RIJ, Armida, “Beyond the UN: Closing the humanitarian funding gap”, Chathamhouse, 08/07/2021 https://www.chathamhouse.org/2021/07/beyond-un-closing-humanitarian-funding-gap

VERHULST, Stefaan, ADITI, Ramesh, ANDREW, Young, ZAHURANEC, Andrew, “Where is Everyone? The Importance of Population Density Data: A Data Artefact Study of the Facebook Population Density Map”, The GovLab, 2021, https://files.thegovlab.org/data-artefact-study-hrsl.pdf

WARNER, Alexandra, “Monitoring humanitarian innovation”, Alnap, 2017, https://www.elrha.org/wp-content/uploads/2017/03/hif-alnap-monitoring-humanitarian-innovation-2017.pdf

## Littérature scientifique

### ARTICLES

CAVOUKIAN, Ann,"Privacy by Design: The 7 Foundational Principles", Toronto, 2010, www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf

DARRIN, Maxime, « Sur les évaluations d'impact dans les politiques numériques », *La Revue européenne des médias et du numérique*, 06/2023 https://la-rem.eu/2023/06/sur-les-evaluations-dimpact-dans-les-politiques-numeriques/

KERMISCH, Céline, « Vers une définition multidimensionnelle du risque. » *VertigO,* volume 12, number 2, september 2012

FAVRO, Karine, « La démarche de *compliance* ou la mise en œuvre d'une approche inversée », *LEGICOM*, 2017/2 (N° 59), p. 21-28. https://www.cairn.info/revue-legicom-2017-2-page-21.htm

FISCHER, Flora, « L'éthique *by design* du numérique : généalogie d'un concept », *Sciences du Design*, 2019/2 (n° 10), p. 61-67.: https://www.cairn.info/revue-sciences-du-design-2019-2-page-61.htm

FLORIDI, Luciano, « The End of an Era: from Self-Regulation to Hard Law for the Digital Industry », *Philos. Technol,* 2021,34,p. 619–622. https://doi.org/10.1007/s13347-021-00493-0

GAUDEMET, Antoine, « Qu'est-ce que la *compliance* ? », *Commentaire*, 2019/1 (Numéro 165), p. 109-114. https://www.cairn.info/revue-commentaire-2019-1-page-109.htm

GELLERT R., « We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences between the Rights-Based and the Risk-Based Approaches to Data Protection », *European Data Protection Law Review* (EDPL), 2016, 2, p. 481 et s

GURSES, Seda, TRONCOSO, Carmela, DIAZ, Claudia, « Engineering Privacy by design », KU Leuven, IBBT, ESAT / SCD-COSIC, 2011 https://software.imdea.org/~carmela.troncoso/papers/Gurses-CPDP11.pdf

HACHEZ, Isabelle, « Balises conceptuelles autour des notions de "source du droit", "force normative" et "soft law" », *Revue interdisciplinaire d'études juridiques* , 2010/2 (Volume 65), p. 1-64. https://www.cairn.info/revue-interdisciplinaire-d-etudes-juridiques-2010-2-page-1.htm

HARDY, Gaelle, "La compliance, une privatisation de la régulation? ", *Revue de droit international d'Assas*, N° 5/ Issue 5, 2022

JASMONTAITE,Lina,KAMARA, Irene, ZANFIR-FORTUNA, Gabriela, LEUCI, Stefano, "Data Protection by Design and by Default: Framing Guiding Principles into Legal Obligations in the GDPR", *European Data Protection Law Review*, Vol. 4, No. 2, 2018

MARELLI, Massimo," The SolarWinds hack : lessons for international humanitarian organizations", *International review of the Red Cross*, Vol 104, number 919, 2022 https://international-

review.icrc.org/sites/default/files/reviews-pdf/2022-06/Selected-Articles-International-Review-of-the-Red-Cross-No-919.pdf

RALLET, Alain, ROCHELANDET, Fabrice, ZOLYNSKI, Célia, « De la *Privacy by Design* à la *Privacy by Using*. Regards croisés droit/économie », *Réseaux*, 2015/1 (n° 189), p. 15-46. https://www.cairn.info/revue-reseaux-2015-1-page-15.htm

ROSSI, Julien, « La structure argumentative d'un demi-siècle de politique européenne de protection des données à caractère personnel », *Politique européenne*, 2023/3 (N° 81), p. 54-85. https://www.cairn.info/revue-politique-europeenne-2023-3-page-54.htm

THELISSON, Eva, « La portée du caractère extraterritorial du Règlement général sur la protection des données », *Revue internationale de droit économique,* 2019/4 (t. XXXIII), p. 501-533. https://www.cairn.info/revue-internationale-de-droit-economique-2019-4-page-501.htm

WANG, Boya, LUEKS, Wouter, SUKAITIS, Justinas, GRAF NARBEL, Vincent, TRONCOSO, Carmela, "Not Yet another digital ID : Privacy-preserving humanitarian aid distribution, 2023, https://doi.org/10.48550/arXiv.2303.17343

ZOMIGNANI BARBOZA, J., DE HERT, P. "Data Protection Impact Assessment : A Protection Tool for Migrants Using ICT Solutions.", *Social Sciences*, 10(12), 2021

OUVRAGES

BERNSTEIN P.L., *Against the gods: the remarkable story of risk*, New York : Wiley, 1998, 400 p.

BECK, Ulrich, *La société du risque. Sur la voie d'une autre modernité,* Paris : Flammarion, 2008, 528 p

BISMUTH, Régis, PASCAL, Hugo (dir.), « Les nouveaux défis de la compliance », *La Revue des juristes de sciences po*, 2019, 140 p.

BOURG, Dominique, SCHLEGEL, Jean Louis, *Parer aux risques de demain, le principe de précaution*, Paris : édition du Seuil, 2001, 144 p.

CASSELLA, S., V. LASSERRE, V., LECOURT, B. (dir.), *Le droit souple démasqué, Articulation des normes privées, publiques et internationales*, Pedone, Paris, 2018, 194 p.

DELMAS-MARTY, Mireille, *Le flou du droit*, PUF, Quadrige, 2004, 390 p.

FRISON-ROCHE, Marie-Anne (dir.), *La juridictionnalisation de la compliance*, Dalloz,2023 504 p.

GELLERT, Raphael, *The Risk-based approach to data protection,* Oxford University press, 2020, 304 p.

HIBOU, Béatrice, *La bureaucratisation du monde à l'ère néolibérale*, Paris : La Découverte, 2012, 144 p.

KERMISCH, Céline, *Le Concept de risque, de l'épistémologie à l'éthique*, Cachan: Lavoisier, 2011, 96 p.

LASCOUMES, Pierre, BARTHE,Yannick, CALLON, Michel, *Agir dans un monde incertain. Essai sur la démocratie technique,* Paris : Seuil, 2001, 368 p.

LE BRETON, David, *La sociologie du risque*, Paris, PUF (Que sais-je ?), 2022, 128 p.

POWER, Michael , *The Audit Society*, Oxford University Press, 1997, 200p.

SODERBERG, Johan, *Hacking capitalism, the Free and open source software movement*, New York, London: Routledge, 2008, 252 p.

VALLUY, Jérôme, *De l'histoire de l'informatique en expansion sociétale...au capitalisme de surveillance et d'influence (1890-2023)*, Terra HN édition, 2023http://www.reseau-terra.eu/IMG/pdf/-30.pdf

WRIGHT, David, DE HERT, Paul (ed.), *Privacy impact assessment*, London : Springer, 2012, 523 p.

### CHAPITRES D'OUVRAGES

BAYA LAFFITE, Nicolas *et al.* , « Gouvernement des risques par l'éthique et par les normes : perspectives critiques sur ces dispositifs et leurs évolutions », In: *Bulletin de veille scientifique*, 2011, n° 12, p. 136-142. https://archive-ouverte.unige.ch/unige:156141

BOUDIA, Soraya, « La genèse d'un gouvernement par le risque », dans : BOURG, Dominique, éd., *Du risque à la menace. Penser la catastrophe*, Paris : Presses Universitaires de France, 2013, p. 57-76.

MENDOZA-CAMINADE, Alexandra. « Le rôle du sous-traitant en matière de données personnelles », dans : TISSEYRE, Sandrine (dir.), *Sécuriser la sous-traitance : quels nouveaux défis ?* , Toulouse : Presses de l'Université Toulouse Capitole, 2019,p.103-115

### THESES ET MEMOIRES

BREHIN, Loïc, « Contrat et protection des données personnelles, étude des articles 26, 28 et 46 du RGPD », mémoire de recherche, droit privé général, 2020, université Paris II-Assas

ROSSI, Julien, « Protection des données personnelles et droit à la vie privée : enquête sur la notion controversée de " donnée à caractère personnel " » Science politique, Université de Technologie de Compiègne, 2020, tel-03155480

SUKAITIS, Justinas, "Building a path towards responsible use of biometrics : a proposal for security and data privacy evaluation of biometric systems", Master Thesis, Science Informatique, EPFL, 2021

### CONFÉRENCES

DEMETZOU, Katerina, " GDPR and the Concept of Risk", in : KOSTA, Eleni; PIERSON,Jo;SLAMANIG, Daniel ;FISCHER HUBNER, Simone;KRENN, Stephan, " Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data", 13th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Vienna, Austria, August 20-24, 2018, p.137-154

littérature grise

### ARTICLES DE JOURNAL

GAVOIS, Sébastien, "La Cnil accusée de ne pas veiller au respect du RGPD", *Next*, 06/02/2024 https://next.ink/126827/la-cnil-accusee-de-ne-pas-remplir-sa-mission-de-veiller-au-respect-du-rgpd/

SOREL, Jean- Marc, « Le rôle de la soft law dans la gouvernance mondiale : vers une emprise hégémonique », *Le Grand continent*, 21/03/2021 https://legrandcontinent.eu/fr/2021/03/21/role-de-la-soft-law-dans-la-gouvernance-mondiale-vers-une-emprise-hegemonique/

PEPIN, Guénaël, "Vie privée: la CNIL veut ménager protection et innovation", *Le Monde*, 24/04/2013https://www.lemonde.fr/technologies/article/2013/04/24/vie-privee-la-cnil-veut-menager-protection-et-innovation_3164958_651865.html

ARTICLES DE BLOG

« Les GAFAM échappent au RGPD, la CNIL complice », *la Quadrature du Net*, 25/05/2021, https://www.laquadrature.net/2021/05/25/les-gafam-echappent-au-rgpd-avec-la-complicite-de-la-cnil/

"The Biometrics Minefield*", InspiRed*, 26/02/2021 https://blogs.icrc.org/inspired/2021/02/26/the-biometrics-minefield/

« Humanitarian Token solution: digital cash assistance that preserves privacy », *InspiRed*, 27/06/2023 https://blogs.icrc.org/inspired/2023/06/27/humanitarian-token-solution-digital-cash-assistance-preserves-privacy/

BABILLO, Maria, "Navigating privacy-enhancing technologies : key takeaways from the inaugural meeting of the global PETS network", *Privacy Forum*, 07/09/2023 https://fpf.org/blog/navigating-privacy-enhancing-technologies-key-takeaways-from-the-inaugural-meeting-of-the-global-pets-network/

GRAF NARBEL, Vincent, SUKAITIS, Justinas, "Biometrics in humanitarian action : a delicate balance", *Humanitarian Law & Policy, ICRC blogs*, 02/09/2021https://blogs.icrc.org/law-and-policy/2021/09/02/biometrics-humanitarian-delicate-balance/

HOSEIN, Gus, NYST, Carly, "Aiding surveillance, an exploration of how development and humanitarian aid initiatives are enabling surveillance in developing, countries", *Privacy International*, October 2013https://privacyinternational.org/sites/default/files/2017-12/Aiding%20Surveillance.pdf

MARELLI, Massimo, "Opening an ICRC delegation for Cyberspace", *EJIL: Talk!,* 09/02/2023 https://www.ejiltalk.org/opening-an-icrc-delegation-for-cyberspace/

RENIERIS, Elizabeth, "Why PETS ( Privacy-Enhancing technologies) may not always be our friends", *Adalovelace Institute*, 29/04/2021 https://www.adalovelaceinstitute.org/blog/privacy-enhancing-technologies-not-always-our-friends/

SANDVIK, Kristin, « The ambivalent juridification of the humanitarian space », *Verfassungsblog,* 31/01/2024 https://verfassungsblog.de/the-ambivalent-juridification-of-humanitarian-space/

SANDVIK, Kristin, LOHNE, Kjersti, "Building a sociology of law for the humanitarian field", 20/08/2017, *Intlawgrrls* https://ilg2.org/2017/08/20/building-a-sociology-of-law-for-the-humanitarian-field/

RAPPORTS

CARTONG, « Les données programmes : le nouvel eldorado de la solidarité internationale ? Panorama des pratiques et besoins des OSC francophones »,14/09/2020 https://cartong.org/sites/cartong/files/2020_Etude_CartONG_Les_Donnees_Programmes_OSC_FR.pdf

DGEFP, AFPA, « Mettre en œuvre le règlement général sur la protection des Données Comprendre et accompagner les entreprises et les salariés sur les enjeux d'emploi et de compétences », 2019, https://travail-emploi.gouv.fr/IMG/pdf/resultats-enquete-dpd-dpo.2.pdf

"Europe's governments are failing the GDPR", *Brave*, 2020 https://brave.com/static-assets/files/Brave-2020-DPA-Report.pdf

« Evolution de la fonction de délégué à la protection des données », étude 2022, Direction de la prospective Afpa. https://travail-emploi.gouv.fr/IMG/pdf/synthese_dpo.pdf

FRION, Louise," Digital commons as alternative systems of value", Science po, May 2022 https://www.sciencespo.fr/public/chaire-numerique/wp-content/uploads/2023/06/15-juin-DIGITAL-COMMONS-policy-brief-Louise-Frion-1.pdf

HAYES, Ben, MARELLI, Massimo, "Reflecting on the International committee of the Red Cross's biometric policy : minimizing centralized databases", 09/2023 https://ainowinstitute.org/wp-content/uploads/2023/09/regulatingbiometrics-hayes-marelli.pdf

HES, R., BORKING, John, "Privacy-Enhancing Technologies: The Path to Anonymity", 1995, Registratiekamer, Information and privacy commissioner / Ontario

LEVALLOIS-BARTH, Claire, KELLER, Jonathan, « Analyse d'impact relative à la protection des données: le cas des voitures connectées », Institut Mines-Telecom, Telecom Paris, 2021, https://cvpip.wp.imt.fr/files/2021/11/FINALRapportRechercheC3S_AIPD_VoituresConnectees_nov2021.pdf

MICHELAKAKI, Christina, BARROS VALE, Sebastiao, "Unlocking Data protection by design & by default: lessons from the inforcement of Article 25 GDPR", *The future of privacy*, May 2023 https://fpf.org/wp-content/uploads/2023/05/FPF-Article-25-GDPR-A4-FINAL-Digital.pdf

Documents juridiques et droit souple

Article 29, "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679", 04/04/2017

CEPD, « Responsabilisation sur le terrain- Partie II : analyses d'impact relatives à la protection des données et consultation préalable », Juillet 2019, https://www.edps.europa.eu/system/files/2021-07/19-07-17_accountability_on_the_ground_part_ii_en_445_fr.pdf

EDPS, Opinion 5/2018, "Preliminary Opinion on privacy by design", 31/05/2018 https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf

EDPS, “Accountability on the ground Part I : records, registers and when to do data protection impact assessments”, February 2018, https://www.edps.europa.eu/sites/default/files/publication/18-02-06_accountability_on_the_ground_part_1_en.pdf

“EDPS survey on data protection impact assessment under article 39 of the Regulation (case 2020-0066)” https://edps.europa.eu/sites/edp/files/publication/20-07-06_edps_dpias_survey_en.pdf

## Chapitre 3

## Littérature scientifique

### ARTICLES

BOON, K. E., MEGRET, F., “New Approaches to the Accountability of International Organizations”, *International Organizations Law Review*, *16*(1), 2019, p.1-10 https://brill.com/view/journals/iolr/16/1/article-p1_1.xml?language=en

DEBUF, Els, “Tools to Do the Job: The ICRC’s Legal Status, Privileges and Immunities”, *International Review of the Red Cross*, Vol. 97, No. 897–898, 2015, p. 321–329

FAST, Larissa,”Governing Data: Relationships, Trust & Ethics in Leveraging Data & Technology in Service of Humanitarian Health Delivery”, *Daedalus* 2023, 152 (2), p. 125–140

HAYES, Ben, “Migration and data protection: doing no harm in an age of mass displacement, mass surveillance and "big data", *International Review of the Red Cross*, 2017, 99 (1),p.179–209. https://international-review.icrc.org/sites/default/files/irrc_99_12.pdf

JACOBSEN, LINDSKOV, Katja, “Biometric data flows and unintended consequences of counterterrorism”, *International review of the Red Cross*, 2021, 103 (916-917),p.619-652 https://international-review.icrc.org/sites/default/files/reviews-pdf/2022-02/biometric-data-flows-and-unintended-consequences-of-counterterrorism-916.pdf

KAURIN, Dragana, “Data protection and digital agency for refugees”, World Refugee Council research paper n°12, may 2019https://www.cigionline.org/static/documents/documents/WRC%20Research%20Paper%20no.12.pdf

KLEIN-KELL, Nathalie, “More humanitarian accountability, less humanitarian access? Alternative ideas on accountability for protection activities in conflict settings”, *international Review of the Red Cross*, 2018, 100 (1-2-3),p. 287–313.

LA ROSA, Anne-Marie, *Chapitre IV. Organisations humanitaires et instances pénales internationales : situation singulière du CICR* In : *Juridictions pénales internationales : La procédure et la preuve*, Genève : Graduate Institute Publications, 2003 https://books.openedition.org/iheid/584?lang=fr

LE BLOND, Stevens, CUEVAS, Alejandro, TRONCOSO-PASTORIZA, Juan Ramon, JOVANOVIC, Philipp, FORD, Bryan, HUBAUX, Jean-Pierre, “On Enforcing the Digital Immunity of a Large Humanitarian Organization”,2018 IEEE Symposium on Security and Privacyhttps://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8418617

MARELLI, Massimo, “Hacking Humanitarians: Defining the Cyber Perimeter and Developing a Cyber Security Strategy for International Humanitarian Organizations in Digital Transformation”, *International Review of the Red Cross* (2020), 102 (913), p.367–387

MARELLI, Massimo, “The law and practice of international organizations’ interactions with personal data protection domestic regulation: At the crossroads between the international and domestic legal orders”, *Computer Law & Security Review*, Volume 50, 2023.

MARTIN, Aaron, SHARMA, Gargi, DE SOUZA Siddharth, Peter, TAYLOR, Linnet, VAN ERD, Boudewijn, MCDONALD, Sean Martin, MARELLI, Massimo, CHEESMAN, Margie, SCHEEL, Stephan, DIJSTELBLOEM, Huub, « Digitisation and Sovereignty in Humanitarian Space: Technologies, Territories and Tensions », *Geopolitics*, V 23/3, 2023, p.1362-1397

MCDONALD, Sean,” From Space to Supply Chains: A Plan for Humanitarian Data Governance”, 2019 https://ssrn.com/abstract=3436179

OUVRAGES

COELHO, Ophélie, *Géopolitique du numérique : impérialisme à pas de géants*, Ivry sur Seine : les éditions de l’Atelier, 2023, 272 p.

GOH, Elaine, SENGSAVANG, Eng (eds), *Recordkeeping in international organization, archives in transition in digital, networked environments*, London : Routledge, 2020, 262 p.

KELLO, Lucas, *Striking back, the end of peace in cyberspace- and how to restore it,* Yale University press, 2022, 183 p.

SANDVIK, Kristin, LINDSKOV JACOBSEN Katja, *UNHCR and the Struggle for Accountability, Technology, law and results-based managemen*t, London: Routledge, 2016, 194 p.

CHAPITRES D’OUVRAGES

BÔMONT, Clotilde, « Maîtriser le cloud computing pour assurer sa souveraineté », in TAILLAT, Stéphane, CATTARUZZA, Amaël, DANET, Didier, *La Cyberdéfense : politique de l’espace numérique*, 2ème édition revue et augmentée, Armand Colin, 2023, p. 134-142

DOMINICÉ, Christian, « La nature et l’étendue de l’immunité de juridiction des organisations internationales », In : DOMINICE, Christian, *L’ordre juridique international entre tradition et innovation*, Genève : Graduate Institute Publications, 1997,p.127-145

KOTKA, T., LIIV, I., « Concept of Estonian Government Cloud and Data Embassies », In: KŐ, A., FRANCESCONI, E. (eds), *Electronic Government and the Information Systems Perspective*, Lecture Notes in Computer Science, vol 9265, Springer, 2015,P.149-162

LUBIN, Asaf, “Data Protection as an International Legal Obligation for International Organizations: The ICRC as a Case Study, in BUCHAN, Russell, LUBIN, Asaf (eds.), *The Rights to Privacy and Data Protection in Times of Armed Conflict*, NATO CCDCOE, 2022 https://ssrn.com/abstract=4115810

PATRICIO GRANÉ, Labat, BURKE, Naomi, "The Protection of Diplomatic Correspondence in the Digital Age: Time to Revise the Vienna Convention?", in : BEHRENS, Paul (eds.), *Diplomatic Law in a New Millennium*, Oxford, 2017,p.204-230 https://doi.org/10.1093/oso/9780198795940.003.0013

THÈSES ET MÉMOIRES

ROBINSON, Nicholas, David," Distributed denial of government, the data embassy and the legal and legal implications of extraterritorial data storage", Doctoral Thesis, University of London, philosophy, September 2020 https://pure.royalholloway.ac.uk/ws/portalfiles/portal/44682853/2020_Robinson_N_PhD.pdf

WALID TAKKOUCHE, Karin, "A new layer of refugee politics at UNHCR biometric technology: Syrian refugee biometric registration by UNHCR in Lebanon", Master Thesis, Master of Arts, Political Studies, American University of Beirut, May 2023https://scholarworks.aub.edu.lb/bitstream/handle/10938/24075/TakkoucheKarin.pdf?sequence=3

CONFÉRENCES

"Managing Cloud computing in the United Nations System", Internet governance Forum, 2017 https://www.intgovforum.org/en/content/igf-2017-day-1-room-xxv-of29-managing-cloud-computing-in-the-united-nations-system

"Conference on Trustworthy and Sovereign Cloud Computing", C4DT, 13/09/ 2023https://c4dt.epfl.ch/c4dt-conference-on-trustworthy-and-sovereign-cloud-computing/

COUTURE S, TOUPIN S, « What Does the Concept of "Sovereignty" Mean in Digital, Network and Technological Sovereignty? », GigaNet: Global Internet Governance Academic Network, Annual Symposium 2017

Littérature grise

ARTICLES DE JOURNAL

« Réfugiés syriens : menace à peine voilée du directeur de la Sûreté contre le HCR », *L'Orient-le Jour*, 06/10/2023 https://www.lorientlejour.com/article/1351598/refugies-syriens-menace-a-peine-voilee-du-directeur-de-la-surete-contre-le-hcr.html

FICHTER, Adrienne, « Le CICR réinvente son avenir cyber, mais pas en Suisse », *Heidi.news*, 01/08/2023 https://www.heidi.news/cyber/le-cicr-reinvente-son-avenir-cyber-mais-pas-en-suisse

POUJOL, Véronique, « L'État renfloue les caisses de Luxconnect », *Reporter*, 29/11/2019 https://www.reporter.lu/luxembourg-secteur-ict-etat-renfloue-les-caisses-de-luxconnect/

RAHMAN, Zara, "The UN's refugee data shame", *The New Humanitarian*, 21/06/2021 https://www.thenewhumanitarian.org/opinion/2021/6/21/rohingya-data-protection-and-UN-betrayal

ROBBIN, Zoe, "Jordan: is the UN's biometric registration for Syrian refugee a threat to their privacy?", *Middle East eye*, 23/10/2022https://www.middleeasteye.net/news/jordan-syrian-refugees-un-biometrics-threat-data-privacy

SEYDTAGHIA, Anouch, « Et si la Suisse aidait le CICR et les ONG contre les cyberattaques ? », *Le Temps*, 23/01/2022 https://www.letemps.ch/economie/cyber/suisse-aidait-cicr-ong-contre-cyberattaques

SEYDTAGHIA, Anouch, « Autour du cloud en Suisse, deux visions diamétralement opposées se font face », *Le Temps*,13/07/2023 https://www.letemps.ch/economie/autour-du-cloud-en-suisse-deux-visions-diametralement-opposees-se-font-face

SLEMROD, Annie, "UN experts : Uptick in Houthi obstacles to Yemen aid delivery", *The New humanitarian*, 03/03/2020 https://www.thenewhumanitarian.org/news/2020/02/03/Yemen-Houthis-aid-worker-safety

THOMAS, Elise, "Tagged, tracked and in danger : how the Rohingya got caught in the UN's risky biometric database", *Wired*, 12/03/2018 https://www.wired.co.uk/article/united-nations-refugees-biometric-database-rohingya-myanmar-bangladesh

ARTICLES DE BLOG

BUCHAN, Russell, TSAGOURIAS, Nicholas, "hacking international organizations : the role of privileges and immunities", *Articles of war*, 14/12/2021 https://lieber.westpoint.edu/hacking-international-organizations-privileges-immunities/

Human Right Watch, "UN shared Rohingya data without informed consent", 15/06/2021 https://www.hrw.org/news/2021/06/15/un-shared-rohingya-data-without-informed-consent

Privacy International, "Why we work on refugee privacy", 08/07/2011 https://privacyinternational.org/news-analysis/1322/why-we-work-refugee-privacy

Statewatch, "EU and USA plough ahead with secret discussions on biometric data exchange scheme", 24/08/2023https://www.statewatch.org/news/2023/august/eu-and-usa-plough-ahead-with-secret-discussions-on-biometric-data-exchange-scheme/

WIEWIOROWSKI, Wojciech, "International Organisations Demonstrate Dedication to Data Protection", EDPS, 17 /O7/ 2018 https://www.edps.europa.eu/press-publications/press-news/blog/international-organisations-demonstrate-dedication-data_en

RAPPORTS

BIN SHAFIQUE, Sharid, "Digital ID in Bangladeshi refugee camps : a case study", *The Engine Room*,2020https://digitalid.theengineroom.org/assets/pdfs/%5BEnglish%5D%20Bangladesh%20Case%20Study%20-%20DigitalID%20-%20The%20Engine%20Room.pdf

CHRISTAKIS, Theodore, « Données, Extraterritorialité et Solutions Internationales aux Problèmes Transatlantiques d'Accès Aux Preuves Numériques - Avis Juridique sur L'Affaire Microsoft Ireland (Cour Suprême des Etats-Unis) », 2017, *The White Book: USA v. Microsoft: Quel Impact?*, CEIS & The Chertoff Group White Paper https://ssrn.com/abstract=3081958

DAKSHINIE, Ruwnathika, HIMMICHE, Ahmed, THOMPSON, Henry, TOUGAS, Marie-Louise, PAES, Wolf-Christian, "Final report of the Panel of experts on Yemen",*Security Council*, 27/12/2019 https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2020_70.pdf

FAST, Larissa, "data sharing between humanitarian organisations and donors: toward understanding and articulating responsible practice", NCHS paper, 2022 https://www.humanitarianstudies.no/wp-content/uploads/NCHS-paper-06-April-2022-Data-sharing-between-humanitarian-organisations-and-donors.pdf

Human rights watch, "Deadly consequences, obstruction of aid in Yemen during Covid19", 14/09/2020 https://www.hrw.org/report/2020/09/14/deadly-consequences/obstruction-aid-yemen-during-covid-19#_ftn83

LYNCH, Jennifer, "HART : Homeland Security's Massive New Database Will Include Face Recognition, DNA, and Peoples' "Non-Obvious Relationships", EFF, 07/06/2018 https://www.eff.org/fr/deeplinks/2018/06/hart-homeland-securitys-massive-new-database-will-include-face-recognition-dna-and

RAFTREE Linda, « Case study: Responsible data sharing with governments », *The Cash Learning Partnership*, 03/2021 https://www.calpnetwork.org/wp-content/uploads/2021/03/CaLP-Case-Study-Responsible-Data-Sharing-with-Governments.pdf

RAFTREE, Linda, KONDAKHCHYAN, Anna, "Responsible data sharing with governments", CaLP, 10/03/2021https://www.im-portal.org/help-library/case-study-responsible-data-sharing-with-governments-0

ROBEHMED, Sacha, "The future of Biometrics and digital ID in Lebanon, assessing proposed systems for elections and social assistance*",SMEX*, 2021,https://smex.org/wp-content/uploads/2021/01/210121_SMEX_PI_ElectoralDigitalID_Draft5_EN.pdf

Documents juridiques et droit souple

« Le privilège du CICR de ne pas divulguer des informations confidentielles », *Revue Internationale de la Croix Rouge*, Volume 97, 2015/1 & 2 https://international-review.icrc.org/sites/default/files/12-cicr-97-2015_1-2-memorandum.pdf

ICRC's Directorate, "Access to information policy", 2019, https://www.icrc.org/sites/default/files/document_new/file_list/access-information-policy.pdf

EDPB, "United Nations, Impact of the European Union's data protection regulations on the Activities of UN system Organizations", 14/05/2020https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/2020.05.14_letter_to_edpb_chair_with_un_comments_on_guidelines_2-2020.pdf

EDPS," Government access to data in third countries", 2021 https://edpb.europa.eu/system/files/2022-01/legalstudy_on_government_access_0.pdf

EDPS, « Lignes directrices sur l'utilisation des services d'informatique en nuage par les institutions et les organes de l'Union européenne », 16/03/2018 https://www.edps.europa.eu/sites/default/files/publication/18-03-16_cloud_computing_guidelines_fr.pdf

European data protection supervisor, Transfers internationaux,https://www.edps.europa.eu/data-protection/data-protection/reference-library/international-transfers_fr

EDPB, “Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence”, July2019https://edpb.europa.eu/sites/default/files/files/file2/edpb_edps_joint_response_us_cloudact_annex.pdf

“Advisory opinion on the rules of confidentiality regarding asylum information”, UNHCR, 2005,https://www.refworld.org/jurisprudence/amicus/unhcr/2005/en/93151

« Doctrine sur l’approche confidentielle du Comité international de la Croix- Rouge (CICR) Moyen spécifique du CICR pour obtenir des autorités étatiques et non étatiques le respect du droit », *Revue internationale de la croix rouge*, vol 94, 2012/3 https://international-review.icrc.org/sites/default/files/ricr-887-confidentiel.pdf

Council of the European Union,” Applicability of the General Data Protection Regulation to the activities of the International Committee of the Red Cross”, Brussels, 25/03/2015 https://data.consilium.europa.eu/doc/document/ST-7355-2015-INIT/en/pdf

Council of the European Union, “Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Applicability of the General Data Protection Regulation to the activities of the International Committee of the Red Cross (ICRC)”, 12/05/2015

OIM, « Privilèges et immunités, comité permanent des programmes et des finances », douzième session, 13-14 mai 2013 https://www.iom.int/sites/g/files/tmzbdl486/files/2019-01/SCPF_96_7.pdf

## Chapitre 4

### Littérature scientifique

#### ARTICLES

ALTMAN, Jonathan, CACHAY, Brenda, MILLER, Zach, MORNEAU, Clare, MOSCOSO, Nico, ORIENTALE, Steven, "Using data to understand the impact of AML/CFT sanction on the delivery of aid : the perspective of Nonprofit organizations", January 2021

AMICELLE Anthony, « *Policing* & *big data*. La mise en algorithmes d’une politique internationale », *Critique internationale*, 2021/3 (N° 92), p. 23-48. https://www-cairn-info.ezproxy.utc.fr/revue-critique-internationale-2021-3-page-23.htm

AMICELLE Anthony, FAVAREL-GARRIGUES Gilles, « La lutte contre l’argent sale au prisme des libertés fondamentales : quelles mobilisations ? », *Cultures & Conflits*, 2009/4 (n° 76), p. 39-66. https://www.cairn.info/revue-cultures-et-conflits-2009-4-page-39.htm

AMICELLE, Anthony, CHIFFELLE, Jaquet, OLIVIER, David, « La traçabilité, une technique de stigmatisation? Retour sur la problématisation de l'«hawala» dans le contexte antiterroriste », *Revue Internationale de Criminologie et de Police Technique et Scientifique*, 2015, LXVIII.p. 338-353.

ANTOULY, Julien, « La résolution 2664 du Conseil de sécurité : une étape historique vers une meilleure protection des activités humanitaires », *La Revue des droits de l'homme*, Actualités Droits-Libertés, http://journals.openedition.org/revdh/16070

ANTOULY, Julien, « Quels sont les effets de la lutte contre le terrorisme sur l'humanitaire? », *Alternatives humanitaires*, n°18, 12/11/21 https://www.alternatives-humanitaires.org/fr/2021/11/12/quels-sont-les-effets-de-la-lutte-contre-le-terrorisme-sur-laction-humanitaire/

BIGO,Didier, "La Mondialisation de l'(in)Sécurité? Réflexions sur le champ des professionnels de la gestion des inquiétudes et analytique de la transnationalisation des processus d'(in)sécurisation." *Cultures et Conflits*, no. 58, 2005, p. 53–100

BIGO, Didier**,** « Le "*nexus*" sécurité, frontière, immigration : programme et diagramme », *Cultures & Conflits*, 84 , 2011, p.7-12

BOUCHET-SAULNIER, Françoise, "How counterterrorism throws back wartime medical assistance and care to pre-Solferino Times", *IRRC* n°916-917, February 2022https://international-review.icrc.org/articles/how-counterterrorism-throws-back-wartime-medical-assistance-to-pre-solferino-times-916

BREWCZYŃSKA, Magdalena, KOSTA, Eleni, « From the Fight Against Money Laundering and Financing of Terrorism Towards the Fight for Fundamental Rights: Role of Data Protection » Tilburg Law School Research Paper nr. 2/2023, https://ssrn.com/abstract=4328464

BURTON, Jo, ""Doing no harm" in the digital age: what the digitalization of cash means for humanitarian action, *International review of the Red Cross*, n°913, 2021

https://international-review.icrc.org/articles/doing-no-harm-digitalization-of-cash-humanitarian-action-913

CARNABY, E., HALLWRIGHT, J. "Complexities of implementation: Oxfam Australia's experience in piloting blockchain. », *Frontiers*, Volume 2 - 2019

COHEN, Neal, HASTY, Robert, WINTON, Ashley, "Allocations of the USAID partner vetting system and state department risk analysis and management system under European union and united kingdom data protection and privacy law, counterterrorism and humanitarian engagement project, research and policy paper", march 2014

Counterterrorism and Humanitarian Engagement Project, "Partner Vetting in Humanitarian Assistance: An Overview of Pilot USAID and State Department Programs", Research and Policy Paper, November 2013 https://archive.blogs.harvard.edu/cheproject/files/2013/10/CHE-Project-Partner-Vetting-in-Humanitarian-Assistance-November-2013.pdf

DURANA, Gabrielle, « Démocratiser la finance ? Les désillusions de la cryptomonnaie », *Esprit*, 2023/5 (Mai), p. 47-55. https://www.cairn.info/revue-esprit-2023-5-page-47.htm

FRASHER, Michelle, "Data protection and the EU's anti-money laundering regulation", IAPP, 23/11/2021 https://iapp.org/news/a/data-protection-and-the-eus-anti-money-laundering-regulation/

GILLARD, Emanuela-Chiara, GOSWAMI, Sangeeta, VAN DEVENTER, Fulco, "Screening of final beneficiaries - a red line in humanitarian operations. An emerging concern in development work", *International Review of the Red Cross*, n° 916-917, February 2022 https://international-review.icrc.org/articles/screening-of-final-beneficiaries-a-red-line-in-humanitarian-operations-916

JUTEL, Olivier, « Blockchain humanitarianism and crypto-colonialism », *Patterns,* Volume 3, Issue 1, 2022, https://www.sciencedirect.com/science/article/pii/S2666389921003056

LENFANT, François, VAN BROEKHOVEN, Lia, VAN LIERDE, Frank, « Les conséquences de la guerre contre le terrorisme sur le monde des ONG », *Cultures & Conflit*s, n° 76, 2009, http://journals.openedition.org/conflits/17779

MALLARD, G., SABET, F.,SUN, J."The Humanitarian Gap in the Global Sanctions Regime: Assessing Causes, Effects, and Solutions", *Global Governance: A Review of Multilateralism and International Organizations*, *26*(1), p.121-153. https://doi.org/10.1163/19426720-02601003

MARTIN, Aaron, "Mobile Money Platform Surveillance", *Surveillance & Society*, 17(1/2), 2019, p.213-222.

MAXWELL, Winston, BERTRAND, Astrid, VAMPARYS, Xavier, "Are AI-based Anti-Money Laundering (AML) Systems Compatible with European Fundamental Rights?", ICML 2020 Law and Machine Learning Workshop, Jul 2020, Vienne, Austria.

MCLEAN, Duncan, HOFMAN, Michiel, « Droit international humanitaire, souveraineté des États et érosion du consensus humanitaire : la fin de l'humanitarisme? », *Alternatives humanitaires*, n°23, juillet 2023

MICHELETTI, Pierre, « L'humanitaire au risque de l'empêchement : quelles analyses pour quelles stratégies correctives? », *Alternatives humanitaires*, n°16, 2021 https://www.alternatives-humanitaires.org/fr/2021/03/25/lhumanitaire-au-risque-de-lempechement-quelles-analyses-pour-quelles-strategies-correctives/

MICHIEL, Hofman, "Humanitarians in the age of counter terrorism: rejected by rebels, coopted by States", *Alternatives humanitaires*, n°7, 2018

O'LEARY, Emma, "Politics and principles : the impact of counterterrorism measures and sanctions on principled humanitarian action, *International review of the red cross*, n°916-917, February 2022 https://international-review.icrc.org/articles/politics-and-principles-the-impact-counterterrorism-measures-on-principled-humanitarian-action-916

PARAGI, Beata, "Opacity or transparency? Screening by NGOS in the context of Aid work", NCHS paper, 2023. https://www.humanitarianstudies.no/wp-content/uploads/NCHS-paper-10-April-2023-Opacity-or-transparency.pdf

QUINTEL, T. « Data protection rules applicable to Financial Intelligence Units: still no clarity in sight », *ERA Forum* 23, p.53–74,2022.

VAN BROEKHOVEN, Lia, GOSWAMI, Sangeeta, “Can stakeholder dialogues help solve financial access restrictions faced by non-profit organizations that stem from countering terrorism financing standards and international sanctions?”, *IRRC* n° 916-917, february 2022

### OUVRAGES

BIERSTEKER, Thomas, ECKERT, Sue, *Countering the financing of terrorism*, London : Routledge Taylor & Francis Group, 2008,360 p.

BIERSTEKER, Thomas, ECKERT, Sue, TOURINHI, *Targeted sanctions*, Cambridge university press, 2016,405 p.

FAVAREL-GARRIGUES Gilles, GODEFROY Thierry, LASCOUMES Pierre (dir.) , *Les sentinelles de l’argent sale. Les banques aux prises avec l’antiblanchiment*, Paris, La Découverte, « Cahiers libres », 2009, 312 p.

PARAGI, Beata, *Screening by international aid organizations operating in the Global South, mitigating risks of generosity*, Palgrave McMillan, 2024, 200 p.

PEROUSE DE MONTCLOS, Marc-Antoine, *L’aide humanitaire, l’aide à la guerre ?,* Paris : Editions complexes, 2001,208 p.

### CHAPITRES D’OUVRAGES

AMICELLE, Anthony, “Migrant remittances in the face of securitization”, In T. BASARAN, T, GUILD (eds.), *Global Labour and the Migrant Premium : The Cost of Working Abroad*, New York : Routledge,2018, p 101-110.

FAVAREL-GARRIGUES, Gilles, GODEFROY, Thierry, LASCOUMES, Pierre, « 6. Le développement des instruments informatiques », dans : FAVAREL-GARIGUES, Gilles, THIERRY, GODEFROY, LASCOUMES, Pierre (dir), *Les sentinelles de l’argent sale. Les banques aux prises avec l’antiblanchiment*, Paris, La Découverte, « Cahiers libres », 2009, p. 141-157

FAVAREL GARRIGUE, Gilles, GODEFROY, Thierry, LASCOUMES, Pierre, “Tools and securitization, the instrumentation of AML/CFT policies in French Banks”, In: HELGESSON, Karin Svedberg, MORTH Ulrika (ed), *Accountability and risk management, transforming the public security domain*, London: Routledge, Taylor & Francis Group, 2012, 192 p

### RAPPORTS DE RECHERCHE

“An Analysis of Contemporary Counterterrorism-related Clauses in Humanitarian Grant and Partnership Agreement Contracts, Counterrorism and humanitarian engagement project”, Harvard, May 2014, https://archive.blogs.harvard.edu/cheproject/files/2013/10/CHE_Project_-_Counterterrorism-related_Humanitarian_Grant_Clauses_May_2014.pdf

### CONFERENCES

« Terrorisme, contreterrorisme et droit international humanitaire », 17e colloque de Bruges, 20-21 octobre 2016, Collège d’Europe, CICR, https://www.coleurope.eu/sites/default/files/uploads/page/collegium_47_v7.pdf

BEECHWOOD international, “Hawala and humanitarian aid risks, mitigation and options in Syria”, Chatham house workshop, Istanbul 14-15 December 2015.

Littérature grise

ARTICLES DE JOURNAL

« La traçabilité de l'aide humanitaire débattue devant le Conseil d'État », *le Monde*, 16/03/2022 https://www.lemonde.fr/societe/article/2022/03/16/la-tracabilite-de-l-aide-humanitaire-debattue-devant-le-conseil-d-etat_6117709_3224.html

« Les lois antiterroristes exposent les ONG humanitaires à la paralysie », *Le Monde*, 17/01/2020. https://www.lemonde.fr/idees/article/2020/01/17/les-lois-antiterroristes-exposent-les-ong-humanitaires-a-la-paralysie_6026151_3232.html

BRABANT, Justine, FOUCHARD, Anthony, "L'État tente d'imposer le traçage des bénéficiaires de l'aide humanitaire", *Disclos*e, 01/10/2021 https://disclose.ngo/fr/article/etat-renforce-controle-aide-humanitaire

CURRIER, Cora, "Lawyer and scholars to lexisnexis, Thomson Reuters : stop helping ICE deport people", *The Intercept*, 14/11/2019 https://theintercept.com/2019/11/14/ice-lexisnexis-thomson-reuters-database/

CUTTS, Mark, "Why the UN Security Council must vote for Syria aid access now", *The New Humanitarian*,05/07/2022https://www.thenewhumanitarian.org/opinion/2022/07/05/Why-the-UN-Security-Council-must-vote-for-Syria-aid

ELLIOTT, Vittoria, PARKER, Ben, "Balancing act: anti-terror efforts and humanitarian principle, a conversation on how counter terrorist laws impede aid work", *The new humanitarian*, 26/11/2019, https://www.thenewhumanitarian.org/feature/2019/11/26/balancing-act-anti-terror-efforts-and-humanitarian-principles

FOLLOROU, Jacques, « En Afghanistan, les talibans utilisent des ONG pour contourner les sanctions », *Le Monde*, https://www.lemonde.fr/international/article/2023/10/25/en-afghanistan-les-talibans-utilisent-des-ong-pour-contourner-les-sanctions_6196390_3210.html?utm_source=pocket_reader

HOOPER, Simon, « Charities warned that sending aid to Syria's Idlib could be a "terror offence", *Middle East Eye*, 08/12/2018
https://www.middleeasteye.net/news/charities-warned-sending-aid-syrias-idlib-could-be-terror-offence

MATHIS, Jérôme, « Avec sa cryptomonnaie, Facebook veut concurrencer les services de transfert d'argent en Afrique », *le Monde*, 01/09/2019 https://www.lemonde.fr/afrique/article/2019/09/01/avec-sa-cryptomonnaie-facebook-veut-concurrencer-les-services-de-transfert-d-argent-en-afrique_5505189_3212.html

PARKER, Ben, "Des applications louables pour Bitcoin?", *The New humanitarian*, 13/01/2016 https://www.thenewhumanitarian.org/fr/report/102069/des-applications-louables-pour-bitcoin

SCHAHILL, Jeremy, DEVEREAUX, Ryan, "Blacklisted", *The Intercept*, 23/07/2014 https://theintercept.com/2014/07/23/blacklisted/

THEILER, Zach, "How vague money laundering and counter-terror rules slow aid", *The New humanitarian*, 23/05/2023 https://www.thenewhumanitarian.org/analysis/2023/05/23/how-vague-money-laundering-and-counter-terror-rules-slow-aid

ARTICLES DE BLOG

“Event summary: the future of Fatf recommendation 8 : for financial integrity and for civil society”, *Charity and Security*, 16/10/2023 https://charityandsecurity.org/news/event-summary-the-future-of-fatf-recommendation-8-for-financial-integrity-and-for-civil-society/

« L’humanitaire sanctionné ?, Une interview avec Thierry Mauricet sur les conséquences des mesures anti-terroristes sur les transferts bancaires des ONG », *Défis humanitaires*, 30/11/2020 https://defishumanitaires.com/2020/11/30/mauricet-transferts-bancaires-humanitaire/

BOINET, Thierry, « Monsieur le Président de la République, protégeons l’aide humanitaire qui est en danger ! », *Défis humanitaires*, 30/11/2020 https://defishumanitaires.com/2020/11/30/edito-47-alain-boinet/

CHARNY, R., Joel, "Counter-terrorism and humanitarian action : the perils of zero tolerance”, *War on the rocks*, 20/03/2019 https://warontherocks.com/2019/03/counter-terrorism-and-humanitarian-action-the-perils-of-zero-tolerance/

HUVE, Sophie, MOULIN, Guillemette, FERRARO, Tristan, "Unblocking aid : the EU's 2023 shift in sanctions policy to safeguard humanitarian efforts”, *Humanitarian law& policy*, 23/01/2024 https://blogs.icrc.org/law-and-policy/2024/01/23/unblocking-aid-eu-2023-sanctions-policy-humanitarian-efforts/

KASSEM, Ramzi, MIGNOT-MAHDAVI, Rebecca, SULLIVAN, Gavin,” watchlisting the world : digital security infrastructures : informal law, and the "global war on terror", *JustSecurity,* 28/10/2021https://www.justsecurity.org/78779/watchlisting-the-world-digital-security-infrastructures-informal-law-and-the-global-war-on-terror/

PARAGI Beata, « The ambiguous politics of screening NGOs as actors in the counterterrorism game? », *Norwegian center for humanitarian studies*, 8/02/22, https://www.humanitarianstudies.no/the-ambiguous-politics-of-screening/

PARAGI, Beata, "Opacity or transparency? Screening by NGOs in the context of aid work", Norwegian centre for humanitarian studies, 08/03/2023https://www.humanitarianstudies.no/resource/opacity-or-transparency-screening-by-ngos-in-the-context-of-aid-work/

PEJIC, Jelena, HERBET, Irénée, RODENHAUSER, Tilman, “ICRC engagement with non-state armed groups : why and how”, *humanitarian law Policy ICRC blog*, 04/03/2021 https://blogs.icrc.org/law-and-policy/2021/03/04/icrc-engagement-non-state-armed-groups/

TRISKO, DARDEN, Jessica, “Humanitarian assistance has a terrorism problem. Can it be resolved?”, *War on the Rocks*, 03/01/2019 https://warontherocks.com/2019/01/humanitarian-assistance-has-a-terrorism-problem-can-it-be-resolved/

RAPPORTS

“Exploring blockchain and mobile money in the northwest of syrian assessment of current and potential utility of alternative tools in minimising money transfer challenges and aid duplication”, AFNS, IMMAP, 2023 https://afns.org/volumes/doc/Blockchain-and-Mobile-Money-in-Northwestern-Syria.pdf?v=1695478374

« Principes sous pression, l'impact des mesures antiterrorisme et de prévention/ lutte contre l'extrémisme violent sur l'action humanitaire basée sur les principes », Conseil norvégien pour les réfugiés , 2018https://www.nrc.no/globalassets/pdf/principles-in-practice/principles-under-pressure-french.pdf

« Guide pour l'action humanitaire basée sur les principes, gérer les risques liés à la lutte anti-terroriste », NRC, 2020,https://www.nrc.no/globalassets/pdf/reports/toolkit/nrc_risk_management_toolkit_principled_humanitarian_action_french.pdf

CALLAMARD, Agnes, "Saving lives is not a crime, Report of the Special Rapporteur of the Human Rights Council on extrajudicial, summary or arbitrary executions "(A/73/314), 6/08/2018

Calpnetwork, "cash feasibility assessment", Cash working group, North West Syria, 2020 https://www.calpnetwork.org/wp-content/uploads/ninja-forms/2/IOM_CFA_external_final_compressed.pdf

DARTER, Kimberly," Partner Vetting, Independant assessment : insufficient justification for a global rollout, Interaction", December 2016 https://www.interaction.org/wp-content/uploads/2020/02/Independent-Partner-Vetting-Assessment_FINAL.pdf

DE GEOFFROY, Véronique, CATTEAU, Thomas, FOIN, Thomas, GRUNEWALD, François, « bilan des engagements de la stratégie humanitaire de la république française 2018-2022 : une aide humanitaire plus efficace face aux crises de demain ? », Groupe URD, Janvier 2023 https://www.diplomatie.gouv.fr/IMG/pdf/meae_2023_06_01_bilan_shrf_2018_-_2022_urd_cle0c7f11.pdf

DEAN, Roger, "Remittances to syria What Works, Where and How", Norwegian refugee council, 2015 https://www.calpnetwork.org/wp-content/uploads/2020/01/2015-07-nrc-remittances-to-syria-report-final-1.pdf

DODGSON, Kate, GENC, Dilek, "Blockchain for humanity", ODIHPN, 29/11/2017https://odihpn.org/publication/blockchain-for-humanity/

GILLARD, Emanuela-Chiara, "IHL and the humanitarian impact of counterterrorism measures and sanctions", Chatham house, September 2021 https://www.chathamhouse.org/sites/default/files/2021-09/2021-09-03-ihl-impact-counterterrorism-measures-gillard_0.pdf

HAYES, Ben, "On shrinking space, a framing paper", *Transnationalinstitute*, April 2017 https://www.brot-fuer-die-welt.de/fileadmin/mediapool/2_Downloads/Fachinformationen/Analyse/Analysis_68_The_impact_of_international_counterterrorism_on_CSOs.pdf

HAYES, Ben, "The impact of international counter-terrorism on civil society organizations, Understanding the role of the Financial Action task Force", *Brot Fur die Welt*, April 2017 https://www.brot-fuer-die-welt.de/fileadmin/mediapool/2_Downloads/Fachinformationen/Analyse/Analysis_68_The_impact_of_international_counterterrorism_on_CSOs.pdf

https://pilac.law.harvard.edu/mcac-report//front-matter

"Humanitarian action, counterterrorism measures and sanctions in Syria",Diakona International humanitarian law centre, August 2021

https://apidiakoniase.cdn.triggerfish.cloud/uploads/sites/2/2021/08/Diakonia_FactSheets-Sanctions_FullPacket.pdf

GAO, "Report number GAO-11-355 entitled 'Afghanistan : U.S. Efforts to Vet Non-U.S. Vendors Need Improvement", 2011 https://www.gao.gov/assets/a319435.html

ISAACS, Leon, HUGO, Sarah, ROBSON, Gemma, BUSH, Charlie, ISSACS, Poppy, MORE

MARTINEZ, Inigo," Impact of the Regulatory Environment on Refugees' and Asylum Seekers' Ability to Use Formal Remittance Channels", KNOMAD Working paper 33, July 2018, https://www.knomad.org/publication/impacts-regulatory-environment-refugees-and-asylum-seekers-ability-use-formal

LEWIS, Dustin A., MODIRZADEH, Naz K.,BLUM,Gabriella, "Medical Care in Armed Conflict: International Humanitarian Law and State Responses to Terrorism," Harvard Law School Program on International Law and Armed Conflict, September 2015. https://pilac.law.harvard.edu/medical-care-in-armed-conflict-international-humanitarian-law-and-state-responses-to-terrorism

MACKINTOSH, Kate, DUPLAT, Patrick, "Study of the impact of donor counter-terrorism measures on principled humanitarian action", Norwegian Refugee council, July 2013, https://www.nrc.no/globalassets/pdf/reports/study-of-the-impact-of-donor-counterterrorism-measures-on-principled-humanitarian-action.pdf

MCCARTHY, Gilian, "Adding to the evidence, the impacts of sanctions and restrictive measures on humanitarian action", VOICE, March 2021 https://voiceeu.org/publications/adding-to-the-evidence-the-impact-of-sanctions-and-restrictive-measures-on-humanitarian-action.pdf

MSF, "Adding salt to the wound, the experience of MSF frontline workers providing impartial healthcare in counter-terrorism environments", October 2021 https://reliefweb.int/report/afghanistan/adding-salt-wound-experience-msf-frontline-workers-providing-impartial-healthcare

PANTULIA, Sara, MACKINTOSH, Kate, ELHAWARY, Samir, METCALFE, Victoria, "Counter-terrorism and humanitarian action, tension, impact and ways forward", *HPG policy brief*, n°43, October 2011

SCHELLHAMMER, Lean, "Breaking the silence, lessons from humanitarian access negotiations under counter-terrorism legislation in north western Syria", Chaberlin, 2021

SLIM, Hugo, BANFIELD, Rachel, SOULEYMANE ADENHOF, Thierno, BURTON, Jo, "cash transfer programming in armed conflict: The ICRC's experience", ICRC 2018 https://resources.peopleinneed.net/documents/594-4359-002-cash-transfer-programming-upd-1-11-2018-web-1-.pdf

SULLIVAN, Gavin, HAYES, Ben, "Blacklisted : targeted sanctions, preemptive security and fundamental rights", ECCHR, 2010 https://www.ecchr.eu/fileadmin/Publikationen/Blacklisted.pdf

UNHCR, "Cash assistance and access to formal financial services, information on assessing KYC and CCD regulation", 2021 https://www.unhcr.org/sites/default/files/legacy-pdf/616e8d244.pdf

WALKER, Justine, "Risk Management Principles Guide for Sending Humanitarian Funds into Syria and Similar High-Risk Jurisdictions", May 2020, http://files.acams.org/pdfs/2020/The-Risk-Management-Principles-Guide-for-Sending-Humanitarian-Funds-into-Syria-and-Similar-High-Risk-

Documents juridiques et droit souple

"Contribution D'Action contre la Faim, CARE France, Coordination Sud1, la Croix- Rouge française, Electriciens sans Frontières, HAMAP-Humanitaire, Handicap International, La Chaîne de l'Espoir, Médecins du Monde, Première Urgence International, Secours Islamique France, Solidarités International À l'évaluation de la Directive relative à la lutte contre le terrorisme"[Directive (UE) 2017/541 https://www.coordinationsud.org/wp-content/uploads/ONG-francaises_Contribution-a-evaluation-directive-UE-2017-541_VF-1.pdf

"Digital identity", FATF, March 2020https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-on-Digital-Identity.pdf.coredownload.pdf

"EDPB letter to the European Parliament, the Council, and the European Commission on data sharing for AML/CFT purposes in light of the Council's mandate for negotiations", 28/03/2023https://edpb.europa.eu/system/files/2023-04/edpb_letter_out2023-0015_aml_cft_ep_en.pdf

"FATF's recommendation 8 on non-profit organization: a new tool to unfairly and dangerously shrink civil society space", Working group, torture&terrorism, OMCT, SoS-Torture network, 10/07/2019 https://www.ohchr.org/sites/default/files/Documents/Issues/Terrorism/SR/Submissions/OMCT_GA74CT.pdf

"Opinion 12/2021, on the anti-money laundering and countering the financing of terrorism ( AML/CFT) package of legislative proposals", EDPS, 22/09/2021https://edps.europa.eu/system/files/2021-09/21-09-22_edps-opinion-aml_en.pdf

"Partner Vetting System (PVS) Privacy Impact Assessment (PIA)", USAID, 17/01/2017https://www.usaid.gov/sites/default/files/2022-08/Partner_Vetting_System_PVS_PIA_Summary_January_17_2017.pdf

« Normes internationales sur la lutte contre le blanchiment de capitaux et le financement du terrorisme et de la prolifération, les recommandations du GAFI », novembre 2023https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/Recommandations%20du%20GAFI%202012.pdf.coredownload.pdf

Chapitre 5

Littérature scientifique

ARTICLES

COLLOMB Cléo, HERNANDEZ Nicolas, « Les attaques par *ransomwares* comme actes de cyber guérilla. Une approche écosystémique de la menace cyber dans le contexte de la guerre en Ukraine », *Études françaises de renseignement et de cyber*, 2023/1 (N° 1), p. 155-176. https://www.cairn.info/revue-etudes-francaises-de-renseignement-et-de-cyber-2023-1-page-155.htm

COTE, Anne-Marie, BERUBE, Maxime, DUPONT Benoit, « Statistiques et menaces numériques. Comment les organisations de sécurité quantifient la cybercriminalité », *Réseaux*, 2016/3-4 (n° 197-198), p. 203-224. https://www.cairn.info/revue-reseaux-2016-3-page-203.htm

DEIBERT, Ron, "Toward a Human-Centric Approach to Cybersecurity", *Ethics & International Affairs, 32*(4), 2018

DINNISS, Harisson, " The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives", *Israel Law Review*. 2015,48(1), p.39-54.

DONINI, Antonio, MAXWELL, Daniel," from face to face to screen to screen : remote management, effectiveness and accountability of humanitarian action in insecure environments", *International Review of the red cross*, 2013, 95 (890), 383-413, https://international-review.icrc.org/sites/default/files/irrc-890-donini-maxwell.pdf

DORMANN, Knut, "Computer network attack and international humanitarian law", *Cambridge Review of international affairs*, 19/05/2001

DOUZET, Frédérick, GERY, Aude, "Le cyberspace, ça sert, d'abord, à faire la guerre. Prolifération, sécurité et stabilité du cyberspace", *Hérodote*, 2020/2, n°177-178,p.329-350

DUFFIELD, Mark, "Disaster-resilience in the network age access-denial and the rise of cyber-humanitarianism", DISS Working paper, 2013

DUFFIELD, Mark, WADDELL, Nicholas, "Securing Humans in a dangerous world", *International Politics*, 2006, 43 (1-23)

DUNN, CAVELTY, Myriam, "Breaking the cybersecurity dilemma : aligning security needs and removing vulnerabilities", *Sci Eng Ethics* 20, 2014, p.701–715 https://doi.org/10.1007/s11948-014-9551-y

EGLOFF, Florian, SHIRES, James, "The better angels of our digital nature ? Offensive cyber capabilities and state violence", *European Journal of international security,* 2023, 8, p. 130-149.

GEISS, Robin, LAHMANN, Henning, "Protection of data in armed conflict", *International law studies* n°97, 2021 https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2964&context=ils

GISEL, Laurent, RODENHAUSER, Tilman, DORMANN, Knut, " Twenty years on : international humanitarian law and the protection of civilians against the effect of cyber operations during armed conflicts", *International Review_of the red cross*, n°913, 2021

GROSSMAN, Taylor, KAMINSKA, Monica, SHIRES, James, SMEETS, Max, "The Cyber dimension of the russia-ukraine war", *Eurpean cyberconflict research initiative*, april 2023

GUIFFARD Jonathan, « L'Ukraine, un allié essentiel à la protection du territoire numérique américain », *Hérodote*, 2023/3-4 (N° 190-191), p. 63-77. https://www-cairn-info.ezproxy.utc.fr/revue-herodote-2023-3-page-63.htm

KUMAR, Sheetal, " The missing piece in human-centric approaches to cybernorms implementation: the role of civil society", Journal of Cyber Policy, 6:3, 2021, p. 375-393.

LUBIN, Asaf, "The Reasonable intelligence agency", Articles by Maurer Faculty, 3034, 2022https://www.repository.law.indiana.edu/facpub/3034

MAČÁK K., "Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law", *Israel Law Review*. 2015;48(1):55-80.

MAČÁK, K., "Unblurring the lines: military cyber operations and international law", *Journal of Cyber Policy*, *6*(3), 2021, p.411–428.

MARELLI, Massimo, "Hacking humanitarians: Defining the cyber perimeter and developing a cyber security strategy for international humanitarian organizations in digital transformation", *International Review of the Red Cross, 102*(913), 2020, p. 367-387

MASCHMEYER, Lennart, DEIBERT, Ronald J., LINDSAY, Jon R. (2021) “A tale of two cybers - how threat reporting by cybersecurity firms systematically underrepresents threats to civil society”, *Journal of Information Technology & Politics*, 18:1, 2021, p. 1-20

PAVLOVA, Pavlina, “Human rights-based approach to cybersecurity: addressing the security risks of targeted groups”, *Peace Human Rights Governance,* 4(3), Novembre 2020

SANDVIK, Kristin, RAYMOND, Nathaniel, "Beyond the Protective Effect: Towards a Theory of Harm for Information Communication Technologies in Mass Atrocity Response," *Genocide Studies and Prevention: An International Journal*: Vol. 11 : Iss. 1, 2017 p.9-24

SCHMITT, Michael, "Rewired warfare: rethinking the law of cyber attack", International review of the red cross, 96 (893), 2014, p.189-206

SCHMITT, Michael, "Wired warfare 3.0: Protecting the civilian population during cyber operations, "International Review of the Red Cross, 101 (1), 2019,p.333-335

VAUGHN, JOCELYN, “The Unlikely Securitizer: Humanitarian Organizations and the Securitization of Indistinctiveness”, *Security Dialogue*, vol. 40, no. 3, 2009, p. 263–85. http://www.jstor.org/stable/26299791

OUVRAGES

BRADLEY, Miriam, *Protecting civilians in war, the ICRC, UNHCR, and their limitations in internal armed conflicts*, Oxford University Press, 2016, 232 p.

BUCHAN Russell, LUBIN, ASAF (eds), *The Rights to Privacy and Data Protection in Times of Armed Conflict*, Nato Cooperative cyber defence centre of excellence, 2022,318 p.

DELERUE, François, *Cyber Operations and International law*, Cambridge University Press, 2020, 549 p.

DUFFIELD, *Post-humanitarianism: governing precarity in the digital world*, Cambridge : Polity, 2018, 224 p.

EGLOFF, Florian, *Semi-sate actors in cybersecurity*, Oxford University press, 2022, 305 p.

MARANGE, Céline, QUESSARD-SALVAING, Maud (dir), *Les guerres de l’information à l’ère numérique*, Paris, Puf, 2021, 456 p.

SHACKELFORD, S., DOUZET, F., ANKERSEN, C. (Eds.), *Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace*, Cambridge University Press, 2022, 300 p.

CHAPITRES D’OUVRAGES

BEERLI, Monique, WEISSMAN, Fabrice, «Suivez le guide! Les manuels de sécurité et la mise en ordre autoritaire des organisations humanitaires », In : WEISSMAN, Fabrice, NEUMAN, Michael, (ed.), *Secourir sans périr: La sécurité humanitaire à l’ère de la gestion des risques*, Paris : CNRS Editions, 2016, p. 137–154

BRADLEY, Miriam. "Chapter 6: Human security in armed conflict: norms, agendas and actors for protecting civilians", in OBERLEITNER, Gerd, *Research Handbook on International Law and Human Security*”, Cheltenham, UK: Edward Elgar Publishing, 2022,p. 106-124

DANET Didier, « Collapsologie numérique », dans: TAILLAT, Stéphane, CATTARUZZA, Amael, DANET, Didier éd., *La Cyberdéfense. Politique de l’espace numérique,* Paris : Armand Colin, « Collection U », 2018, p. 157-166

DUNN CAVELTY, Myriam, “Cybersecurity and Human Rights”, in: WAGNER, Ben, KATTEMAN, Matthias C., KILLIAN,Vieth (eds),*Research Handbook on Human Rights & Digital Technology*, Cheltenham: Edward Elgarp, p. 73-98

FAST, Larissa, « Securitization », In: DE LAURI, Antonio, *Humanitarianism*, *Keywords,* Leiden : Brill, 2020, p.191-192 https://doi.org/10.1163/9789004431140_089

LUBIN, Asaf, "The duty of constant care and data protection in War", in: DICKINSON A., Laura, BERG, Edward (eds), *Big data and armed conflict: legal issues above and below the armed conflict threshold*, Oxford University Press,2024, p.229-248

LUBIN, Asaf, "The Rights to Privacy and Data Protection Under International Humanitarian Law and Human Rights Law, in: KOLB, Robert, GAGGIOLI, Gloria, KILIBARDA, Pavle, (eds), *Research Handbook on Human Rights and Humanitarian Law: Further Reflections and Perspectives*, Edward Elgar, 2022, p.463-492

O'CONNELL, Mary Ellen, "Data privacy rights : the same in War and Peace", in : BUCHAN, Russell, LUBIN, Asaf ( eds.), *The rights to privacy and data protection in armed conflict*, Nato Cooperative cyber defence centre of excellence, 2022,p.12-29

TAITHE, Bertrand, “Danger, Risk, Security and Protection: Concepts at the Heart of the History of Humanitarian Aid”, in :NEUMAN, Michael, Weissman, Fabrice, (ed.), *Saving Lives and Staying Alive: the professionalization of humanitarian security*, London: Hurst Publishers. 2016, p. 37- 53

THÈSES ET MÉMOIRES

BEERLI, Monique, “Saving the Saviors: An International Political Sociology of the Professionalization of Humanitarian Security”, Thèse de doctorat : Sciences Politiques, Univ. Genève, 2017

CONFERENCES

« Protéger les civils,contre les menaces numériques lors des conflits armés », GEODE, Pôle d’excellence cyber, 21/05/2024

Littérature grise

ARTICLES DE PRESSE

“Red Cross blames hack on Zoho vulnerability, suspect APT attack”, *The Record*, 16/02/2022 https://therecord.media/red-cross-blames-hack-on-zoho-vulnerability-suspects-apt-attack

BALL, James, HOPKINS, Nick, “GCHQ and NSA targeted charities, Germans, Israeli PM and EU chief”, *The Guardian*, 20/12/2013https://www.theguardian.com/uk-news/2013/dec/20/gchq-targeted-aid-agencies-german-government-eu-commissioner

CHRISTINE, Debora Irene, THINYANE, Mamello, « Opinion: Why civil society remains so vulnerable to cyberattacks »,*DEVEX*, 17/11/2021, Devex,https://www.devex.com/news/opinion-why-civil-society-remains-so-vulnerable-to-cyberattacks-102016

CORNISH, Lisa, “New security concern raised for RedRose digital payment system”, *Devex*, 28/11/2017.https://www.devex.com/news/new-security-concerns-raised-for-redrose-digital-payment-systems-91619

ELLIOTT, Vittoria, “Humanitarian organizations keep getting hacked because they can't spend to secure data”, *Rest of the World*, 03/02/2022, https://restofworld.org/2022/humanitarian-organizations-hack/

IGOE, Michael, « The 4 cyberwarfare risks facing aid groups in Ukraine », *Devex*, 17/02/2022 https://www.devex.com/news/the-4-cyberwarfare-risks-facing-aid-groups-in-ukraine-102685

*Le Monde,* « Médecins du monde, Total, Unicef : la surveillance tous azimuts de la NSA », 20/12/2013. https://www.lemonde.fr/technologies/article/2013/12/20/medecins-du-monde-total-unicef-la-surveillance-tous-azimuts-de-la-nsa_4338321_651865.html

LELOUP, Damien, CLAIROUIN, Olivier « Cybersécurité: dans l'humanitaire, la difficile mue des ONG », *Le Monde*, 21/02/2022, https://www.lemonde.fr/pixels/article/2022/02/21/cybersecurite-dans-l-humanitaire-la-difficile-mue-des-ong_6114613_4408996.html

NAKASHIMA, Ellen, SHABAN, Hamza, “Russian Governement hackers target civil society groups after compromising USAID email marketing account”, *Washington Post*, 28/05/2021https://www.washingtonpost.com/national-security/russia-hack-usaid-human-rights-groups/2021/05/28/3e996c42-bfae-11eb-9c90-731aff7d9a0d_story.html

PARKER, Ben, “Dozen of NGOs hit by hack on US fundrasing database”, *The New Humanitarian*, 04/08/2020https://www.thenewhumanitarian.org/news/2020/08/04/NGO-fundraising-database-hack

PARKER, Ben, “EXCLUSIVE : the cyber-attack the UN tried to keep under wraps”, *The New Humanitarian*, 29/01/2020, https://www.thenewhumanitarian.org/investigation/2020/01/29/united-nations-cyber-attack

PARKER, Ben, “Security lapses at aid agency leave beneficiary data at risk”, *The New humanitarian*, 27/11/2017, https://www.thenewhumanitarian.org/investigations/2017/11/27/security-lapses-aid-agency-leave-beneficiary-data-risk

PARKER, Ben, « Dozens of NGOs hit by hack on US fundraising database », *The New Humanitarian*, 04/08/2020https://www.thenewhumanitarian.org/news/2020/08/04/NGO-fundraising-database-hack

SALDINGER, Adva, « USAID hack is 'wakeup call' for aid industry on cybersecurity » *Devex*,04/06/2021, https://www.devex.com/news/usaid-hack-is-wakeup-call-for-aid-industry-on-cybersecurity-100028

SEYDTAGHIA, Anouch, "Les données volées du CICR seraient désormais en vente", *Le Temps*, 22/02/2022 https://www.letemps.ch/monde/donnees-volees-cicr-seraient-desormais-vente

*The New humanitarian*, “From cyber-attacks to bot farms : the top tech threats humanitarians face in Ukraine”, 09/03/2022 https://www.thenewhumanitarian.org/opinion/2022/03/09/from-cyber-attacks-to-bot-farms

WINDER, Davey, “United Nations confirms "serious" cyberattack with 42 core servers compromised”, *Forbes*, 30/01/2020, https://www.forbes.com/sites/daveywinder/2020/01/30/united-nations-confirms-serious-cyberattack-with-42-core-servers-compromised/?sh=71e6d5b1633d

ARTICLES DE BLOG

"Human security in the age of AI: securing and empowering individuals", ICT for Peace foundation, 2018, https://ict4peace.org/wp-content/uploads/2018/12/Digital-Human-Security-Final-DSmlogos.pdf

BROOKING, Emerson, LONERGAN, Erica, "Welcome to cyber realism: parsing the 2023 departement of defense cyber strategy", *War on the rocks*, 25/09/2023 https://warontherocks.com/2023/09/welcome-to-cyber-realism-parsing-the-2023-department-of-defense-cyber-strategy/?utm_source=pocket_saves

FERRARI, Veronica, KUMAR, Sheetal, "A human-centric approach to international cybernorms: Civil society feedback on the UN Open-Ended Working Group on ICTs proposals", Association for progressive communication, 01/12/2020https://www.apc.org/en/news/human-centric-approach-international-cybernorms-civil-society-feedback-un-open-ended-working

GRACE, Rob, "When security risk management and technology collide: getting humanitarian notification systems right", *GISF*, 10/01/2023 https://www.gisf.ngo/blogs/when-security-risk-management-and-technology-collide-getting-humanitarian-notification-systems-right/

JANCARKOVA, Tatana, MACAK, Kubo," Scenario 12: cyber operations against computer data", International Cyber law in practice: interactive toolkit https://cyberlaw.ccdcoe.org/wiki/Scenario_12:_Cyber_operations_against_computer_data

KREB, Brian, "Red Cross hack linked to iranian influence operation?", *Krebson Security*, 16/02/2022https://krebsonsecurity.com/2022/02/red-cross-hack-linked-to-iranian-influence-operation/

MACAK, Kubo, RODENHAUSER, Tilman, GISEL, Laurent, "Cyber-attacks against hospital and the Covid 19 pandemic : how strong are international law protections?", 02/04/2020 https://blogs.icrc.org/law-and-policy/2020/04/02/cyber-attacks-hospitals-covid-19/

MARELLI, Massimo, "Hacking humanitarians: moving towards a humanitarian cybersecurity strategy", ICRC blogs, Humanitarian law&policy, 16/01/2020, https://blogs.icrc.org/law-and-policy/2020/01/16/hacking-humanitarians-cybersecurity-strategy/

MAURER, Peter, "The digitalization of armed conflicts : three humanitarian priorities", CSDS Policy Brief, The Centre for Security, diplomacy and Strategy, 13/06/2022 https://brussels-school.be/sites/default/files/CSDS%20Policy%20brief_2214.pdf

PYTLAK, Allison, "Exploring human -centric cyber security", Humanitarian Disarmament, 06/02/2023, https://humanitariandisarmament.org/2023/02/06/exploring-human-centric-cyber-security/

RODENHAUSER, Tilman, MACAK, Kubo, "Scenario 20: Cyber operations against medical facilities", International cyber law in practice : interactive toolkithttps://cyberlaw.ccdcoe.org/wiki/Scenario_20:_Cyber_operations_against_medical_facilities

RODENHAUSER, Tilman, STAEHELIN, Balthasar, MARELLI, Massimo, "Safeguarding humanitarian organizations from digital threats", Humanitarian law &Policy, ICRC, 13/10/2022 *https://blogs.icrc.org/law-and-*

*policy/2022/10/13/safeguarding-humanitarian-organizations-from-digital-threats/?utm_source=clipboard&utm_medium=text&utm_campaign=The+Homeanitarian_17+Oct_Week+42*

STAEHELIN, Balthasar, "Hacked": la cybersecurité dans le secteur humanitaire, Geneva Policy Outlook, 30/01/2023, https://www.genevapolicyoutlook.ch/hacked-la-cybersecurite-dans-le-secteur-humanitaire/

RAPPORTS

AL ACHKAR, Ziad, "Digital risk: how new technologies impact acceptance and raise new challenges for NGOs", in :GISF, “Achieving Safe Operations through Acceptance: challenges and opportunities for security risk management”, 2021https://www.gisf.ngo/wp-content/uploads/2021/12/Achieving_Safe_Operations_through_Acceptance_challenges_and_opportunities_for_security_risk_management.pdf

AMAREL, Emma, VERITY, Andrej, DU, Jiahui, “Cybersecurity vs humanitarian organization, on a collision course?”, DH, Digital humanitarian network, August 2018.

CALLEJAS, Jorge Flores, AFIFI, Aicha, LOZINSKIY, Nikolay, “cybersecurity in the United nations system organizations”,JIU/REP/2021/3 https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2021_3_english.pdf

Cyberpeace institute, “NGOs serving humanity at risk: cyber threats affecting international Geneva”, November 2023 https://cyberpeaceinstitute.org/wp-content/uploads/CyberPeace_Analytical%20Report_NGO.pdf

Cyberpeace Institute, “Report of expert meeting on the development of a harms methodology”, December 2023, https://cyberpeaceinstitute.org/news/publications/report-expert-meeting-harms-methodology/

DELERUE, François, “Analyse du manuel de Tallinn 2.0 sur le droit international applicable aux cyber-opérations, étude prospective et stratégique”, CEIS, novembre 2017 http://francoisdelerue.eu/wp-content/uploads/2020/01/20171129_NP_F-Delerue_Analyse-Manuel-Tallinn-2-0.pdf

DETTE Rahel, STEETS Julia, SAGMEISTER Elias, “Technologies for monitoring in insecure environment”, Septembre2016https://www.gppi.net/media/SAVE__2016__Toolkit_on_Technologies_for_Monitoring_in_Insecure_Environments.pdf

GROSSMAN, Taylor, KAMINSKA, Monica, SHIRES, James, SMEETS, Max, "The Cyber dimensions of the Russia-Ukraine War", European Cyber Conflict research initiative, April 2023 https://eccri.eu/wp-content/uploads/2023/04/ECCRI_REPORT_The-Cyber-Dimensions-of-the-Russia-Ukraine-War-19042023.pdf

Open-ended working group on developments in the field of information and telecommunications in the context of international security, Final Substantive Report,10/03/2021 https://dig.watch/wp-content/uploads/2022/08/OEWG-Report.pdf

Documents juridiques et droit souple

Cyberpeace institute, “The OEWG “Zero Draft”: The Need For A Stronger Human-centric Approach”,26/02/2021 https://cyberpeaceinstitute.org/news/the-oewg-zero-draft-the-need-for-a-stronger-human-centric-approach/

ICT4PEACE, “Submission by ICT4Peace to the Open-Ended Working Group (OEWG) on security of and in the use of information and communications technologies 2021-2025”, 2022, https://ict4peace.org/wp-content/uploads/2022/01/ICT4PeaceSubOEWGIIJan2022ds-1.pdf

ICRC, “Protecting civilian against digital threats during armed conflict : recommendations to states, belligerents, tech companies, and humanitarian organization”, Final report of the ICRC global advisory board on digital threats during armed conflict, october 2023

Open-ended working group on developments in the field of information and telecommunications in the context of international security, Final Substantive Report,10/03/2021 https://dig.watch/wp-content/uploads/2022/08/OEWG-Report.pdf

## Introduction III partie

### Littérature scientifique

#### ARTICLES

BLOUSTEIN E.J. « Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser », *New York University Law Review*, 1964, 39, p. 962

AGIER Michel, « Penser le sujet, observer la frontière », *L’Homme*,2012, 203-204, p.203-204, http://journals.openedition.org/lhomme/23096

AGIER, Michel, « Le camp des vulnérables. Les réfugiés face à leur citoyenneté niée », *Les Temps Modernes*, 2004/2 (n° 627), p. 120-137 https://www.cairn.info/revue-les-temps-modernes-2004-2-page-120.htm

COLE, Alyson, “All of Us Are Vulnerable, But Some Are More Vulnerable than Others: The Political Ambiguity of Vulnerability Studies, an Ambivalent Critique”,*Critical Horizons*,2016, 17:2, p. 260-277, DOI: 10.1080/14409917.2016.1153896

DANDOY, Arnaud, « L'éthique du care contre l'exceptionnalisme humanitaire », *Alternatives humanitaires*, N°5, 2017 https://www.alternatives-humanitaires.org/fr/2017/07/03/lethique-care-contre-lexceptionnalisme-humanitaire/

DELMAS-MARTY Mireille, « Humanité, espèce humaine et droit pénal », *Revue de science criminelle et de droit pénal comparé*, 2012/3 (N° 3), p. 495-503 https://www.cairn.info/revue-de-science-criminelle-et-de-droit-penal-compare-2012-3-page-495.htm

ENDERS, Christoph, “The Right to have Rights:The concept of human dignity in German Basic Law”, *Revista de Estudos Constitucionais, Hermenêutica e Teoria do Direito* (RECHTD), 2010, 2(1), p. 1-8

FABRE-MAGNAN Muriel, « La dignité en Droit : un axiome », *Revue interdisciplinaire d’études juridiques*, 2007/1 (Volume 58), p. 1-30. https://www.cairn.info/revue-interdisciplinaire-d-etudes-juridiques-2007-1-page-1.htm

FAST, L., « Unpacking the principle of humanity: Tensions and implications», *International Review of the Red Cross, 97*(897-898), 2015, p. 111-131. doi:10.1017/S1816383115000545

FLORIDI, Luciano, "On Human Dignity and a Foundation for the Right to Privacy", https://ssrn.com/abstract=3839298

HENNETTE-VAUCHEZ Stéphanie, « Une dignitas humaine ? Vieilles outres, vin nouveau », *Revue Droits*, 2008/2 (n° 48), p. 59-86. https://www.cairn.info/revue-droits-2008-2-page-59.htm

HINGH de, Anne, "Some Reflections on Dignity as an Alternative Legal Concept in Data Protection Regulation", *German Law Journal*, Vol 19, n°5. https://germanlawjournal.com/wp-content/uploads/Vol_19_No_5_Anne-de-Hingh.pdf

MALGIERI, Gianclaudio, JĘDRZEJ, Niklas, "Vulnerable data subjects", *Computer Law & Security Review*, 2020,Volume 37, p.1-22

MALGIERI, GianClaudio, GONZALEZ FUSTER, Gloria, "The Vulnerable data subject: a gendered data subject?", *European Journal of Law and Technology*, 2022, Vol 13 No. 2

MCKNIGHT HASHEMI, Valérie, « L'identité des victimes et le respect de la dignité humaine : analyse terminologique », *La Revue internationale de la Croix Rouge*, n°876, 2009 https://international-review.icrc.org/fr/articles/lidentite-des-victimes-et-le-respect-de-la-dignite-humaine-analyse-terminologique

MENKE, Christoph, « De la dignité de l'homme à la dignité humaine : le sujet des droits de l'homme », *Trivium*, 2009/3 http://journals.openedition.org/trivium/3303

MESURE Sylvie, « Dignité et société. Approche sociologique et critique », *Raisons politiques*, 2017/2 (N° 66), p. 211-224. https://www.cairn.info/revue-raisons-politiques-2017-2-page-211.htm

ROCHEL, Johan," Connecting the Dots: Digital Integrity as a Human Right", *Human Rights Law Review*, 2021, Volume 21, Issue 2, p.358–383, https://doi.org/10.1093/hrlr/ngaa063

SANDVIK, Kristin "Technology, Dead Male Bodies, and Feminist Recognition: Gendering ICT Harm Theory", *Australian Feminist Law Journal*, 2018, 44:1, p.49-69, 10.1080/13200968.2018.1465371

SÖZER, H., "Humanitarianism with a neo-liberal face: vulnerability intervention as vulnerability redistribution", *Journal of Ethnic and Migration Studies*, 2020 *46*(11), p. 2163–2180. https://doi.org/10.1080/1369183X.2019.1573661

TURNER, Lewis, "The Politics of Labeling Refugee Men as "Vulnerable"", *Social Politics: International Studies in Gender, State & Society*, 2021, Volume 28, Issue 1, p. 1–23, https://doi.org/10.1093/sp/jxz033

OUVRAGES

FERRIS, Elizabeth G, *The Politics of Protection: The Limits of Humanitarian Action*, Washington : Brookings Institution Press, 2011, p.359.

FLEURY, Cynthia, *La Clinique de la dignité*, Paris, Seuil, 2023, 224 p.

GARRAU, Marie, *Politiques de la vulnérabilité*, CNRS Editions, 2018, 370 p.

MACKENZIE, Catriona, ROGERS Wendy, DODDS Susan, (eds), *Vulnerability : New Essays in Ethics and Feminist Philosophy*, Oxford University Press, 2013, 336 p.

MAILLARD, Nathalie, *La vulnérabilité, une nouvelle catégorie morale ?,* Genève : Labor et Fides, coll. « Le champ éthique », 2011, 386 p.

NORMAN, Ajari, *La Dignité ou la mort. Éthique et politique de la race*, Paris : Éd. La Découverte, coll. Les Empêcheurs de penser en rond, 2019,p.257

SLIM, Hugo, *Humanitarian ethics : a guide to the morality of aid in war and disaster*, London : Hurst & Company, 2015, p.224

THOMAS, Hélène, *Les vulnérables : la démocratie contre les pauvres*, Paris, Éditions du Croquant, 2010, 254 p

CHAPITRES D'OUVRAGES

FUH, D. "Human Dignity". In: DE LAURI, Antonio, *Humanitarianism keywords,* Leiden : Brill. 2020 doi: https://doi.org/10.1163/9789004431140_041

LEURS, K., "Resilience and Digital Inclusion: The Digital Re-making of Vulnerability?", In: TSATSOU, P. (eds) *Vulnerable People and Digital Inclusion*, Palgrave Macmillan, Cham. 2022, p.27-46

ROUVROY, A., POULLET, Y., "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy", In: GUTWIRTH, S., POULLET, Y.,

DE HERT, P., DE TERWANGNE, C., NOUWT, S. (eds*), Reinventing Data Protection?,* Springer, 2009,p.45-76

RAPPORTS DE RECHERCHE

MOSEL, Irina, HOLLOWAY, Kerrie, "Dignity and humanitarian action in displacement", HGP Report, March 2019, https://cdn.odi.org/media/documents/Dignity_synthesis_paper.pdf

CONFERENCES

« Protéger la dignité humaine, XXVIIIème Conférence internationale de la Croix-Rouge et du Croissant-Rouge Genève », 2et 6 décembre 2003 https://disasterlaw.ifrc.org/sites/default/files/media/disaster_law/2021-02/Fran%C3%A7ais_Agenda_Final.pdf

European Data Protection Supervisor, "Towards a new digital ethics: Data, dignity and technology" 2015 https://www.edps.europa.eu/data-protection/our-work/publications/opinions/towards-new-digital-ethics-data-dignity-and_en

Chapitre 6

Littérature scientifique

ARTICLES

ACQUISTI, Alessandro, MICHELE, Francine, MBO'O Ida, et ROCHELANDET, Fabrice, « Les comportements de vie privée face au commerce électronique », *Réseaux*, 2011, n°167, p. 105-130

AGIER, Michel**,** « Urgence et attente », *Écrire l'histoire*, 16, 2016, p.175-183 http://journals.openedition.org/elh/1086

BALBONI, P., COOPER, D., IMPERIALI, R. & MACENEITE, M. , « Legitimate interest of the data controller New data protection paradigm: legitimacy grounded on appropriate protection », *International Data Privacy Law,* 2013, 3 (4), p. 244-261

CRAWFORD, Kate, MEGAN, Finn, "The Limits of Crisis Data: Analytical and Ethical Challenges of Using Social and Mobile Data to Understand Disasters", *GeoJournal*, vol. 80, no. 4, 2015, p. 491–502

FERRETTI, Federico, « Data protection and the legitimate interest of data controllers: Much ado about nothing or the winter of rights? »,2014, 51, *Common Market Law Review*, Issue 3, p. 843-868, https://kluwerlawonline.com/journalarticle/Common+Market+Law+Review/51.3/COLA2014063

HUDSON, M., "Think Globally, Act Locally: Collective Consent and the Ethics of Knowledge Production", *Int. Soc. Sci. J.,* 2009, 60, p. 125–133

JAUNAIT Alexandre, « Comment peut-on être paternaliste ? Confiance et consentement dans la relation médecin-patient », *Raisons politiques*, 2003/3 (n° 11), p. 59-79. https://www.cairn.info/revue-raisons-politiques-2003-3-page-59.htm

JEYABALAN, V.; DONNELLE, L.; MEIER, P.; NOUVET, E. "To Obtain Informed Consent or Not to Obtain Informed Consent? Drones for Health Programs in the Grey Zone between Research and Public Health", *Drones,* 2023, *7*, 247. https://doi.org/10.3390/drones7040247

MASURE, Anthony, « Résister aux boîtes noires. Design et intelligences artificielles », Paris, Puf, *Cités*, n° 80, décembre 2019, anthonymasure.com/articles/2019-12-resister-boites-noires-design-intelligences-artificielles

NI AOLAIN, Fionnuala, "Women, Vulnerability, and Humanitarian Emergencies", *Michigan Journal of Gender&Law*, Vol.18-Issue 1, 2011

PARAGI B., ALTAMIMI, A, «Caring control or controlling care? Double bind facilitated by biometrics between UNHCR and Syrian refugees in Jordan », *Society and Economy*, *44*(2), 2022, p. 206-231. https://doi.org/10.1556/204.2021.00027

SANDVIK, K.B., BJORHAUG, I., ESPEGREN, A. GARNIER, A. "Protecting skilled Afghan women: Brain save and the politics of vulnerability", *Global Policy*, 2023, 14, p.5– 15. https://doi.org/10.1111/1758-5899.13166

SANDVIK, Kristin Bergtora, "Technology, Dead Male Bodies, and Feminist Recognition: Gendering ICT Harm Theory", *Australian Feminist Law Journal*, 44:1, 2018, p.49-69, 10.1080/13200968.2018.1465371

SOLOVE, Daniel J., "Privacy Self-Management and the Consent Dilemma", *Harvard Law Review 1880*, 2013, GWU Law School Public Law Research Paper No. 2012-141

SQUIRE, V., ALOZIE, M. " Coloniality and frictions: Data-driven humanitarianism in North-Eastern Nigeria and South Sudan." *Big Data & Society*, 2023, *10*(1). https://doi.org/10.1177/20539517231163171

VARELIUS , J. "On the Prospects of Collective Informed Consent: On the Prospects of Collective Informed Consent", *Journal of Applied Philosophie*, 2008, n° 25, p.35–44.

OUVRAGES

FRAISSE, Genièvre, *Du consentement*, 2017, Paris : édition Du seuil, 144 p

CHAPITRES D'OUVRAGES

DECEW J.W., «The feminist critique of privacy: past arguments and new social understandings », in: ROESSLER B., MOKROSINSKA D. (eds.), *Social Dimensions of Privacy*, Cambridge University Press, 2015, p. 85-103

KAMARA I., DE HERT, P., « Understanding the balancing act behind the legitimate interest of the controller ground: A pragmatic approach », In SELINGER E, POLONETSKY J., TENE O. (Eds.), *Cambridge handbook of consumer privacy*, 2018, p. 321-352

RAYMOND, Nathaniel, « Beyond "Do No Harm" and Individual Consent: Reckoning with the Emerging Ethical Challenges of Civil Society's Use of Data », In: VAN DER SLOOT, Bart, FLORIDI, Luciano, TAYLOR, Linnet (eds.), *Group Privacy*, Springer Verlag,2017.

ROUVROY, A., POULLET, Y., « The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy. », In: GUTWIRTH, S., POULLET,

Y., DE HERT, P., DE TERWANGNE, C., NOUWT, S. (eds),*Reinventing Data Protection ?*, DORDRECHT, Springer, 2009,p.45-76

RAPPORTS DE RECHERCHE

KAURIN, Dragana," Data Protection and Digital Agency for Refugees", World Refugee Council Research Paper No. 12 — Mai 2019, https://www.cigionline.org/static/documents/documents/WRC%20Research%20Paper%20no.12.pdf

SQUIRE V. et. al., "Data and Displacement:Assessing the Practical and Ethical Implications of Data- Driven Humanitarianism for Internally Displaced Persons in Camp-Like Settings", Final Project Report, 2022 www.warwick.ac.uk/datadisplacement

FROST L, KHAN S, VINCK P. ,"Technologies in Humanitarian Settings: Digital Upskilling of Humanitarian Actors", Harvard humanitarian initiative, 2022. https://hhi.harvard.edu/sites/hwpi.harvard.edu/files/humanitarianinitiative/files/digitalcasestudy_5_digitalliteracy_final.pdf?m=1672678941

The Future of Privacy Forum, "Processing Personal Data on the Basis of Legitimate Interests under the GDPR PRACTICAL CASES",2018, https://fpf.org/wp-content/uploads/2018/04/20180413-Legitimate-Interest_FPF_Nymity-2018.pdf

THESES/ MEMOIRES

ROBUSTELLI, Ludovica, « Le droit à l'autodétermination informationnelle en droit européen », thèse de doctorat, Université Grenoble Alpes, Droit européen, 2022

CONFÉRENCES

UTZ ,C., DEGELING, M., FAHL, S., SCHAUB F., HOLZ T., « (Un)informed Consent: Studying GDPR Consent Notices in the Field », Conference on Computer and Communications Security (CCS '19), 2019

Littérature grise

ARTICLES DE BLOG

ICTworks, « How to Add Informed Consent to Your Responsible Data Practices », 15/05/2019 https://www.ictworks.org/informed-consent-responsible-data/

MEIER, "Patrick, Data Protection Protocols for Crisis Mapping", *IRevolution,* 11/04/2013, https://irevolutions.org/2013/04/11/data-protection-for-crisis-mapping/

MESSENGER, Chloe, STELLER Rachael, « Consent to Data Processing in Humanitarian and Development Contexts, Part 2: Beyond Consent », *DAI Global*, 21/01/2021 https://dai-global-digital.com/beyond-consent-why-seeking-consent-for-data-processing-can-be-problematic-in-humanitarian-and-development-contexts.html

RAFTREE, Linda, "Rethinking informed consent in the digital age", *Wait… What ?, 02*/11/2016. https://lindaraftree.com/2016/11/02/rethinking-informed-consent-in-the-digital-age/

RAPPORTS

DIEHM Cade, SMITH Kelsey, ELLIOTT Ame, BULLEN Georgia, "The Limits to Digital Consent: Understanding the risks of ethical consent and data collection for underrepresented communities", *Simply Secure*, October 2021 https://simplysecure.org/resources/The_Limits_to_Digital_Consent_FINAL_Oct2021.pdf

DOWNER, Matthew, "Digital skills development for equitable and dignified humanitarian assistance", in ITU Digital Skills Insights, 2021. https://academy.itu.int/sites/default/files/media2/file/21-00668_Digital-Skill-Insight-210831_CSD%20Edits%206_Accessible-HD.pdf

OEV/2020/002, Office of Evaluation, WFP evaluation Strategic," Evaluation of WFP's Use of Technology in Constrained Environments", Janvier 2022.https://docs.wfp.org/api/documents/WFP-0000136278/download/

Documents juridiques et droit souple

G29, « Lignes directrices sur la transparence au sens du règlement (UE) 2016/679 » 11/04/2018

G29, « Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE », 09/04/2014.

G29, « Lignes directrices sur le consentement au sens du règlement 2016/679 »,10 /04/ 2018.

Chapitre 7

## Littérature scientifique

### ARTICLES


CHEESMAN, Margie, " Self-Sovereignty for Refugees? The Contested Horizons of Digital Identity", *Geopolitics,* 27:1, 2022, p.134-159,

DE FILIPPI, P., LOVELUCK, B. »The invisible politics of Bitcoin: governance crisis of a decentralized infrastructure", *Internet Policy Review*, 5(3),2016, https://doi.org/10.14763/2016.3.427

DE FILIPPI, Primavera, "The Interplay between Decentralization and Privacy: The Case of Blockchain Technologies", *Journal of Peer Production*, 2016, Issue n.7: Alternative Internets https://ssrn.com/abstract=2852689

DE FILIPPI, Primavera, BOURCIER, Danièle, « Réseaux et gouvernance. Le cas des architectures distribuées sur internet », *Pensée plurielle*, 2014/2 (n° 36), p. 37-53. https://www.cairn.info/revue-pensee-plurielle-2014-2-page-37.htm

De MONTJOYE, Yves-Alexandre et al. , «Unique in the shopping mall: On the reidentifiability of credit card metadata », *Science*, 347,2015, p.536-539

FINES SCHLUMBERGER, Jacques-André, « DWEB », *La Revue européenne des médias et du numérique*, 2018 https://la-rem.eu/2018/11/dweb/

FRANKE, MARK, "Refugees' loss of self-determination in UNHCR operations through the gaining of identity in blockchain technology", *Politics, Groups, and Identities*, 2022, 10:1,p. 21-40

JANSSEN, H., SINGH, J, "Personal Information Management Systems", *Internet Policy Review*, *11*(2), 2022 https://doi.org/10.14763/2022.2.1659

LESSIG, Lawrence, « code is law, on liberty in cyberspace », *Harvard Magazine*, janvier 2000

MUSIANI, F., « Network architecture as internet governance », *Internet Policy Review*, 2013, 2(4) https://doi.org/10.14763/2013.4.208

MUSIANI, Francesca, « L'invisible qui façonne. Études d'infrastructure et gouvernance d'Internet », *Tracés. Revue de Sciences humaines*, 2018, V.35, http://journals.openedition.org/traces/8419

NARAYANAN, Arvind, NISSENBAUM, Helen, BAROCAS, Solon, TOUBIANA, Vincent, BONEH Dan, "A critical look at decentralized personal data architectures", https://ar5iv.labs.arxiv.org/html/1202.4503

PORSDAM, Mann, Sebastian, SAVULESCU, Julian, RAVAUD, Philippe, BENCHOUFI, Mehdi,"Blockchain, consent and prosent for medical research", *J. Med ethics*,2021, n°47, p.244-250

REIDENBERG, Joel, " Lex Informatica: The Formulation of Information Policy Rules through Technology ", 76 *Tex. L. Rev.*, 553, (1997-1998)

THYLIN, Theresia, NOVELO DUARTE, María Fernanda, " Leveraging blockchain technology in humanitarian settings – opportunities and risks for women and girls", *Gender & Development*, 27:2, 2019, p. 317-336.

WANG Boya, LUEKS Wouter, SUKAITIS, Justinas, GRAF NARBEL, Vincent, TRONCOSO, Carmela, " Not yet another digital ID: Privacy Presserving Humanitarian Aid Distribution" https://wangboya.org/assets/pdf/icrc-sp-paper.pdf

WANG, Fennie, DE FILIPPI, Primavera, " Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion", *Frontiers in Blockchain*, 2020, v. 2, https://www.frontiersin.org/articles/10.3389/fbloc.2019.00028/full

ZWITTER, Andrej, BOISSE-DESPIAUX, Mathilde, « Blockchain for humanitarian action and development aid », *Journal of international humanitarian action*, 3:16, 2018

ZWITTER, Andrej, GSTREIN, Oskar Josef, "identity and privacy governance", *Frontiers Research Topics*, 2021

CHAPITRES D'OUVRAGES

BODÓ, B., BREKKE, J. K., HOEPMAN, J.-H. « Decentralisation in the blockchain space », *Internet Policy Review*, *10*(2), 2021https://doi.org/10.14763/2021.2.1560

DE FILIPPI, Primavera, « The Interplay between Decentralization and Privacy: The Case of Blockchain Technologies », *Journal of Peer Production*, Issue n.7 : Alternative Internets , 2016

MUSIANI, Francesca, *«* Architecture distribuée/répartie/décentralisée/P2P *»* In :MEADEL, Cecile,

POULLET, Y, DELFORGE, A, « Les blockchains : un défi et/ou un outil pour le RGPD ? » , in : COTIGA, Andra, JACQUEMIN, Hervé, POULLET,Yves (dir.*), Les blockchains et les smart contracts à l'épreuve du droit*, Bruxelles : Larcier , 2020, p. 97-135

RAPPORTS DE RECHERCHE

CHEESMAN Margie, "Digital wallets and migration policy: a critical intersection", *Dot.mig,* 2022https://www.bosch-stiftung.de/sites/default/files/publications/pdf/2022-06/Digital%20Wallets%20and%20Migration%20Policy.pdf

THÈSES ET MÉMOIRES

STATHAKIS, Ioannis, "Critical perspectives on blockchain for humanitarian aid, How does the technology impact procedural fairness and beneficiary data protection?", Master thesis, law&technology, Tilburg University, 2019 https://arno.uvt.nl/show.cgi?fid=149162

TELES HAMIDEH, Jamile, "Between efficiency and do no harm, Blockchain-based innovation in cash and voucher assistance", Master thesis, Marketing, Hanken School of Economics, 2023

Littérature grise

ARTICLES DE PRESSE

DISNEY, Helen, « Healthcare IT needs a dose of medicine, interview with Vasja Bocko, Iryo », *Unblocked*, 07/02/2018

https://un-blocked.co.uk/2018/02/07/healthcare-it-interview-vasja-bocko-iryo/

JUSKALIAN, Russ, "Inside the Jordan Refugee camp that runs on blockchain", *MIT technology review*, 11/04/2018, https://www.technologyreview.com/2018/04/12/143410/inside-the-jordan-refugee-camp-that-runs-on-blockchain/

WONG, Joon Ian, “The UN is using ethereum's technology to fund food for thousands of refugees”, *Quartz*, 03/11/2017https://qz.com/1118743/world-food-programmes-ethereum-based-blockchain-for-syrian-refugees-in-jordan

ARTICLES DE BLOG

CHEESMAN, Margie, "Blockchain for refugees", *Medium*, 08/06/2022, Mediumhttps://medium.com/datasociety-points/blockchain-for-refugees-a46b41594eee

CHRISTOPHER, Allen, “The Path to Self-Sovereign Identity”**,** *Lifewithalacrity,* April 25 2016 http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

RAPPORTS

ANDERSON, Allison, KANE, Seth, “Identities for opportunities,a feasibility study for overcoming the Rohingya's statelessness challenges via blockchain-based digital solutions”, University of Washington, 2018, https://rohingyaproject.com/identities-for-opportunity-university-of-washington/

COPPI, Giulio, FAST, Larissa, “Blockchain and distributed ledger technologies in the humanitarian sector”, HPG Commissioned Report, Overseas Development Institute (ODI), 2019, https://odi.org/en/publications/blockchain-and-distributed-ledger-technologies-in-the-humanitarian-sector/

CURRION, Paul, “Safe passage, options for data portability in the humanitarian sector”, collaborative cash, 2022

UN WOMEN Jordan, UN WOMEN -WFP Blockchain project for cash transfers in refugee campshttps://www.collaborativecash.org/_files/ugd/477045_8adbdc1a90144e67b86f943284d1509b.pdf

Danish Red Cross, Mercy Corps, Hiveonline, « The Next generation humanitarian distributed platform », 2020, https://www.mercycorps.org/sites/default/files/2020-11/The-Next-Generation-Humanitarian-Distributed-Platform-v3.pdf

DUMITRIU, Petru, "Blockchain applications in the United Nations system: toward a state of readiness", Report of the joint inspection unit, 2020https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2020_7_english.pdf

GIZ, "Financial inclusion of refugees in Jordan, knowledge note", November 2022, https://www.giz.de/en/downloads/giz2022-en-financial-inclusion-refugees-jordan.pdf

GSMA, « blockchain for development: emerging opportunities for mobile, identity and Aid »,2017, https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/12/Blockchain-for-Development.pdf

GSMA, « Humanitarian cash and voucher assistance in jordan: a gateway to mobile financial services »,2020, https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/01/Jordan_Mobile_Money_CVA_Case_Study_Web_Spreads.pdf

HENNEBERT, Christine, "Blockchain et identification numérique, restitution des ateliers du groupe de travail « blockchain et identité », octobre 2020

IFRC, “Digital identity an analysis for the humanitarian sector”, 2021,https://static1.squarespace.com/static/5b75620445776e4b290c0d96/t/60a53f8ec37bbe66f938df75/1621442472657/Digital+Identity%E2%80%93An+Analysis+for+the+Humanitarian+Sector+Final.pdf

IFRC, “Kenya Red Cross, DIGID project, user consultation report”, 2020, https://static1.squarespace.com/static/5b75620445776e4b290c0d96/t/603d14c5775eed6fbde2883b/1614615753940/%5BFinal%5D+DIGID+Kenya+User+Consultation+Report.pdf

IFRC, Cash and voucher assistance in migration context, voices of migrants in Kenya, January 2022 https://cash-hub.org/wp-content/uploads/sites/3/2022/03/Cash-in-Migration-Voices-of-Migrants_Kenya-Final.pdf

IFRC, Kenya Red Cross, Gravity, "Gravity-Tykn interoperability proof of concept", June 2021,https://static1.squarespace.com/static/5b75620445776e4b290c0d96/t/619113c163634531ee6365e9/1636897731161/DIGID+Interoperability+Tests.pdf

IFRC, Kenya Red Cross, ICHA, “Dignified identities in cash assistance : lessons learnt from Kenya”, January 2022https://cash-hub.org/wp-content/uploads/sites/3/2022/02/DIGID-Lessons-Learnt-from-Kenya-Jan-2022.pdf

IFRC, Kenya Red Cross, Uganda Red Cross,Dignified identities in humanitarian action : journey and reflection, February 2023https://interoperability.ifrc.org/wp-content/uploads/2023/11/DIGID-Summary-Report-Final.pdf

SLAVIN, Aiden, “Distributed Ledger Identification Systems in the Humanitarian Sector.” Sovrin Foundation, “What Is Self-Sovereign Identity?”,2019 https://sovrin.org/wp-content/uploads/14A-Report.pdf

ZUCCHINI, Giulio, LOISEAU, Camille, CAPATAZ GORDILO, Carlos, ANDUJAR PEREZ, Julian, BLANCO PENALVER, Ana, SCRUBY, Celia, “How blockchain can possibly improve humanitarian action, community engagement, cash transfer & traceability, Red Social Innovation”, March 2023 https://red-social-innovation.com/wp-content/uploads/2023/06/Blockchain_EN.pdf

## Chapitre 8

## Littérature scientifique

### ARTICLES

BABY Sophie, NERARD François-Xavier, « Les objets des disparus. Exhumations et usages des traces matérielles de la violence de masse », *Les Cahiers Sirice*, 2017/2 (N° 19), p. 5-20. https://www.cairn.info/revue-les-cahiers-sirice-2017-2-page-5.htm

BARAYBAR, J.P, “When DNA is not available, can we still identify people? Recommendations for best practice”, *J. Forensic Sci*., 2008 May, 53(3), p.533-40.

BIKKER, J “Disaster Victim Identification in the Information Age: The Use Of Personal Data, Post-Mortem Privacy and the Rights of the Victim’s Relatives “, *Scripted*, 2013 10:1 http://script-ed.org/?p=838

CARAYON Lisa, KOBELINSKY Carolina, « Mourir. Puis disparaître ? », *Plein droit*, 2023/2 (n° 137), p. 3-5. https://www-cairn-info.ezproxy.utc.fr/revue-plein-droit-2023-2-page-3.htm

CASTEX, Lucien, HARBINJA Edina, ROSSI Julien, « Défendre les vivants ou les morts ? Controverses sous-jacentes au droit des données *post mortem* à travers une perspective comparée franco-américaine », *Réseaux*, 2018/4 (n° 210), p. 117-148. https://www.cairn.info/revue-reseaux-2018-4-page-117.htm

CATTANEO, C., TIDBALL BINZ, M., PENADOS, L., PRIETO, J., FINEGAN, O., GRANDI, M., "The forgotten tragedy of unidentified dead in the Mediterranean", *Forensic Science International*, Volume 250, 2015

CATTANEO, C., DE ANGELIS, D., MAZZARELLI, D. et al. "The rights of migrants to the identification of their dead: an attempt at an identification strategy from Italy", *Int J Legal Med*, 137, 2023, p. 145–156 https://www.thelancet.com/journals/langlo/article/PIIS2214-109X(16)30106-1/fulltext

CLAVANDIER, Gaelle, « De nouvelles normes à l'égard des restes humains anciens : de la réification à la personnalisation ? « , *Revue canadienne de bioéthique*, 2019, 2 (3), p.79— 87. https://doi.org/10.7202/1066465ar

CORDNER, S., TIDBALL-BINZ, M., "Humanitarian forensic action – Its origins and future", *Forensic Science International*, 2017, vol.279, p. 65–71

CORDNER, Stephen, MCKELVIE, Helen, "Developing standards in international forensic work to identify missing persons", *RICR* 2002, vol.84, n°848, p.867-884 https://www.icrc.org/en/doc/assets/files/other/irrc_848_cordner.pdf

DIALLO, Alimou, « Politique de l'inanimé : un dispositif informel d'identification des « corps sans vie et sans papiers » au Maroc », *Politique africaine*, 2018/4 (n° 152), p. 141-163. https://www.cairn.info/revue-politique-africaine-2018-4-page-141.htm

DIAZ, Paola Diaz**,** NICOLOSI, Guido, « Corps, identités et technologies "par les nombres" dans l'imaginaire migratoire », *Socio-anthropologie*, 40, 2019, https://doi.org/10.4000/socio-anthropologie.5577

DUBOIS, Olivier, MARSHALL, Katharine, SPARKES MCNAMARA, Siobhan, "Nouvelles technologies et nouvelles politiques : l'évolution de l'action du CICR en faveur des familles séparées", *Revue internationale de la Croix rouge*, Volume 94, 2012/4https://international-review.icrc.org/sites/default/files/20-dubois_marshall_mcnamara_cicr94_fr.pdf

FATTORINI, Paolo, PRESCIUTTINI, Silvano, PREVIDERE, Carlo," Disaster victim identification by kinship analysis: the Lampedusa October 3rd, 2013 shipwreck", *Forensic Science International: Genetics*, Volume 44, 2020,https://doi.org/10.1016/j.fsigen.2019.102156.

FURRI Filippo, KOBELINSKY Carolina, « Donner un nom aux morts en Méditerranée : l'expérience de Catane », *Plein droit*, 2023/2 (n° 137), p. 19-22.

GAGGIOLI, Gloria, "international humanitarian law : the legal framework for humanitarian forensic action", *Forensic Science International*, Volume 282, 2018, p.184-194

GRAY, G., BENNING, B."Crowdsourcing Criminology: Social Media and Citizen Policing in Missing Person Cases", *Sage Open*, 2019, *9*(4). https://doi.org/10.1177/2158244019893700

HELLER, Charles, PECOUD, Antoine**,** « Compter les morts aux frontières : des contre-statistiques de la société civile à la récupération (inter)gouvernementale », *Revue européenne des migrations internationales*, vol. 33 - n°2 et 3 | 2017, http://journals.openedition.org/remi/8732

HORSMAN, Graeme, "Defining principles for preserving privacy in digital forensic examinations", *Forensic science international : digital investigation,* volume 40, 2022 https://www.sciencedirect.com/science/article/abs/pii/S2666281722000191

LE BRETON, David, « Le cadavre ambigu : approche anthropologique », *Études sur la mort*, 2006/1 (nº 129), p. 79-90. https://www.cairn.info/revue-etudes-sur-la-mort-2006-1-page-79.htm

MBEMBE Achille, « Nécropolitique », *Raisons politiques*, 2006/1 (nº 21), p. 29-60. https://www.cairn.info/revue-raisons-politiques-2006-1-page-29.htm

M'CHAREK, A., CASARTELLI, S., "Identifying dead migrants: forensic care work and relational citizenship", *Citizenship Studies*, 2019, 23(7), p.738-757. https://doi.org/10.1080/13621025.2019.1651102

OTTAVY Eva, « Perdre sa vie, mais pas son nom », Plein droit, 2016/2 (n° 109), p. 15-18. https://www.cairn.info/revue-plein-droit-2016-2-page-15.htm

PARSONS, Thomas, HUEL, Rene, BAJUNOVIC, Zlatan, "Large scale DNA identification : The ICMP experience", *Forensic Science International: Genetics,* 38-2019; 236 244

PISCITELLI, Vittorio (et alii.), "Italy's battle to identify dead migrants", *The Lancet*, Volume 4, Issue 8, 2016 https://www.thelancet.com/journals/langlo/article/PIIS2214-109X(16)30106-1/fulltext

POISSON, Dominique, « Que devient le secret médical après le décès d'une personne ? », *Laennec*, 2007/1 (Tome 55), p. 49-58. https://www.cairn.info/revue-laennec-2007-1-page-49.htm

RITAINE, Évelyne, « Migrants morts, des fantômes en Méditerranée », *Rhizome*, 2017/2 (N° 64), p. 16-17. https://www.cairn.info/revue-rhizome-2017-2-page-16.htm

ROSENBLATT, Adam "International Forensic Investigations and the Human Rights of the Dead", *Human Rights Quarterly*, Volume 32, Number 4, November 2010, p. 921-950 https://doi.org/10.1353/hrq.2010.0015

SCHULIAR, Yves, « Les morts judiciaires – le rôle de la Médecine Légale. Le cas particulier de l'identification des victimes de catastrophes », *Études sur la mort*, 2012/2 (n° 142), p. 193-223. https://www.cairn.info/revue-etudes-sur-la-mort-2012-2-page-193.htm

SMITH, L. A., « The missing, the martyred and the disappeared: Global networks, technical intensification and the end of human rights genetics », *Social Studies of Science*, 2017, *47*(3), p. 398-416. https://doi.org/10.1177/0306312716678489

TAZZIOLI, M.,"The politics of counting and the scene of rescue. Border deaths in the *Mediterranean »*, *Radical Philosophy*,n° 92, July/Aug 2015, p. 2–6.

TUAZON, Oliver, "Universal forensic DNA databases: acceptable or illegal under the European Court of Human Rights regime?", *Journal of Law and the Biosciences*, Volume 8, Issue 1, January-June 2021, https://doi.org/10.1093/jlb/lsab022

VAN LAMMEREN, Sylvie, VON KONIG, Florian, “Missing migrants and their families: a call for greater international cooperation”, *Forced migration review*, n°66, March 2021 https://www.fmreview.org/sites/fmr/files/FMRdownloads/en/issue66/vanlammeren-vonkoenig.pdf

OUVRAGES

ANSTETT, Elisabeth, DREYFUS (ed.), Jean-Marc,*Destruction and human remains, disposal and concealment in genocide and mass violence*, Manchester University Press,2014, 263 p.

CAROL, Anne, RENAUDET, Isabelle, *Des morts qui dérogent, à l’écart des normes funéraires, XIXème-XXème siècles*, Presses universitaires de Provence, 2023,250 p.

HARBINJA, Edina*, Digital Death, Digital Assets and Post-Mortem Privacy*, Edinburgh university press, 2022, 272 p.

KOBELINSKY, Carolina, FURRI, Filippo, *Relier les rives, sur les traces des morts en Méditerranée*, Paris : La Découverte, 2024, 200 p.

LAQUEUR, Thomas, *Le travail des morts, une histoire culturelle des dépouilles mortelles*, Paris : Gallimard, 2018, 930 p.

MACHADO, Helena, GRANJA, Rafaela, *Genetic surveillance and crime control, social, cultural and political perspectives*, London : Routledge, 2022, 406 p

SQUIRE, Vicki, *Europe's Migration Crisis, border deaths and human dignity*, Cambridge university press, 2020, 280 p.

CHAPITRES D’OUVRAGES

BARAYBAR, Jose Pablo, CARIDI, Ines, STOCKWELL, Jill, "A forensic perspective on the new disappeared : migration revisited", in : PARRA, Roberto C., ZAPICO, Sara, UBELAKER, Douglas (ed.), *Forensic science and humanitarian action : interacting with the Dead and the Living*, John Wiley & Sons, 2020,p.101-116

CATTANEO, Cristina (et alii.), " the approach to unidentified dead migrants in Italy", in, PARRA, Roberto, ZAPICO, Sara, UBELAKER, Douglas, *Forensic science and humanitarian action : interacting with the dead and the living*, Wiley, 2020, p.559-570

DE BAETS, Antoon, « the posthumous dignity of dead persons, in: PARRA, C., Roberto, UBELAKER, H., Douglas, (ed.), *Anthropology of violent death, theoretical foundations for forensic humanitarian action*, John Wiley &Sons, 2023 P.18

FURRI, Filippo, KOBELINSKY, Carolina, « Les Autres morts. Gestion des corps et présence des morts de la migration dans la ville de Catane », dans BENEÏ, V. , TIJOUX, M. E. (éds.), Racismes, Corps, Attentes : Figures de la migration en contexte contemporain, L’Harmattan, 2021,288 p

KLEISER, Andreas, PARSONS, Thomas J., “Large Scale Identification of the Missing: Experiences and Perspectives of the International Commission on Missing Persons”, in : ERLICH, Henry, STOVER, Eric Stover, WHITE,Thomas (eds), *Silent Witness: Forensic DNA Evidence in Criminal Investigations and Humanitarian Disasters*, Oxford University Press, 2020

M'CHAREK, Amade, BLACK, Julia," Engaging Bodies as Matters of Care Counting and Accounting for Death During Migration", in , CUTTITTA, Paolo, LAST, Tamara (eds.) , *Border Deaths, Causes, Dynamics and Consequences of Migration-related Mortality,* Amsterdam University Press,2020, 174 p.

MIRTO, Giorgia, "*Procedure di gestione delle vittime delle frontiere in Italia",* in CRUA, G., GILETTI, S., PRONO, F. (eds)*, Desaparecidos e migranti nel Mediterraneo e nelle Americhe*, Gruppo Editoriale Bonanno, Acireale-Roma, 2018.

MOON, Claire, "Extraordinary death work: New developments in, and the social significance of, forensic humanitarian action", in PARRA, Roberto C, ZAPICO, Sara C., UBELAKER, Douglas H. (eds.), Humanitarian Forensic Science: Interacting with the Dead and the Living, Chichester: John Wiley and Sons, 2020,p.37-48

MOON, Claire," What remains? Human rights after death", in SQUIRE, Kirsty, ERRICKSON, David, MARQUEZ-GRANT, Nicholas, " *Ethical approaches to human remains : a global challenge in bioarchaeology and forensic anthropology,* Springer nature, 2020, 649 p.

MSF, « Personnes disparues et les morts », *Dictionnaire pratique du droit humanitaire* https://dictionnaire-droit-humanitaire.org/content/article/2/personnes-disparues-et-les-morts/

RAHMAN, Zara, IVENS, Gabriela, "Ethics in Open source investigations", in DUBBERLEY, Sam, KOENIG, Alexa, MURRAY, Daragh (eds.), *Digital Witness, Using open source information for human rights investigation, documentation and accountability*, Oxford university press, 2020 p.249

TIDBALL-BINZ, Morris, HOFMEISTER, Ute, "Forensic archaeology in humanitarian contexts: ICRC action and recommendations", GROEN, Mike, MARQUEZ-GRANT, Nicholas, JANAWAY, Robert (ed.), *Forensic archaeology : a global perspective*, John Wiley & Sons, 2015,p.427-437

WHITE, Thomas, LEE, Steven, "Forensic Genetics, Ethics, Privacy, and Public Policy", in: ERLICH, Henry, STOVER, Eric, WHITE, Thomas (eds), *Silent Witness: Forensic DNA Evidence in Criminal Investigations and Humanitarian Disasters*, New York, Oxford Academic, 2020

RAPPORTS DE RECHERCHE

ATTIA, Ben, et al."Missing Migrants: Management of Dead Bodies in Sicily. Mediterranean Missing", OIM, 2016 https://missingmigrants.iom.int/sites/g/files/tmzbdl601/files/publication/file/Mediterranean-Missing-Italy-report-long.pdf

GRANT, Stefanie, "Dead and Missing migrants : the obligations of european states under international human rights law", IOM, September 2016 https://missingmigrants.iom.int/sites/g/files/tmzbdl601/files/publication/file/Mediterranean-Missing-Legal-Memo-290816.pdf

KERASIOTIS,Vassilis, SPILIOTAKARA,Maria, "Missing and Dead Migrants at Sea: The legal framework in Greece", OIM, September 2016 https://missingmigrants.iom.int/sites/g/files/tmzbdl601/files/publication/file/Mediterranean-Missing-Greek-legal-memo.pdf

ROMANO, Serena, "The Italian legal framework for the management of missing persons and unidentified dead bodies, and the rights of the relatives", OIM, September

2016https://missingmigrants.iom.int/sites/g/files/tmzbdl601/files/publication/file/Mediterranean-Missing-Italian-legal-memo.pdf

### CONFERENCES

FURRI, Filippo, KOBELINSKY, Carolina « Une bureaucratie pour les morts en Méditerranée », communication au colloque *« Tri migratoire » et expériences du blocage : Afrique, Amérique, Europe*, Nice, juin 2021.

## Littérature grise

### ARTICLES DE PRESSE

COUTARD, Hélène, "Personnes disparues : rencontre avec les enquêteurs de la dernière chance", *Le Monde*, 11/02/2024https://www.lemonde.fr/m-le-mag/article/2024/02/11/personnes-disparues-les-enqueteurs-benevoles-de-la-derniere-chance_6215940_4500055.html

LUS, Bruno, "Sur internet et les réseaux sociaux, l'inlassable traque des personnes disparues", *Le Monde*, 19/10/2018https://www.lemonde.fr/pixels/article/2018/10/19/sur-internet-et-les-reseaux-sociaux-l-inlassable-traque-des-personnes-disparues_5371868_4408996.html

JULLIEN, Dorian, « Naufrage en Méditerranée : plus de 2000 hommes, femmes et enfants sont morts ou disparus depuis le début de l'année. Le bilan de 2022 est déjà dépassé », *Le Monde*, 16/08/2023 https://www.lemonde.fr/les-decodeurs/article/2023/08/10/naufrages-en-mediterranee-avec-plus-de-2-000-morts-depuis-le-debut-de-l-annee-le-bilan-de-2022-est-deja-depasse_6185020_4355770.html

« Plus de 2500 hommes, femmes et enfants sont morts ou disparus en Méditerranée en 2023, selon l'ONU », *le Monde avec AFP*, 29/09/2023 https://www.lemonde.fr/afrique/article/2023/09/29/plus-de-2-500-migrants-morts-ou-disparus-en-mediterranee-depuis-le-debut-de-l-annee-selon-l-onu_6191504_3212.html

BOLLAG, Burton, "Help me find my family", *Devex*, 02/05/218https://www.devex.com/news/help-me-find-my-family-92470

SAPOCH, Jack, BULMANN, May, CHERESHEVA, Maria, LUDKE, Steffen, LJUSTINA, Ivana, VOEGELE, Nicole, OBRADOVIC-WOCHNIK, Jelena, DAVIES, Thom, ISAKJEE, Arshad, ALHAFID, Doraid, TILLACK, Anna, MALICHUDIS, Stavros, SOOS, Oliver, VAN DIJKEN, Klaas, MILONOVIC, Aleksandar, IVANOVA, Camelia, RUBIO BERTRAN, Pat, " Europe's Nameless dead, Lighthouse reports, 01/12/2023 https://www.lighthousereports.com/investigation/europes-nameless-dead/

Tribune, collectif, "Migration: "inscrivons l'obligation d'identification des défunts anonymes dans le droit européen", *Le Monde*, 30/08/2023https://www.lemonde.fr/idees/article/2023/08/30/migration-inscrivons-l-obligation-d-identification-des-defunts-anonymes-dans-le-droit-europeen_6187087_3232.html

### ARTICLES DE BLOG

ANGELI, Danai, "The dead, the missing and the bereaved : Is objective 8 still a priority?", 19/05/2021 https://rli.blogs.sas.ac.uk/2021/05/19/the-dead-the-missing-and-the-bereaved-is-objective-8-still-a-priority/

BOLTON, Syd, JARVIS, Catriona, "GCM Commentary : Objective 8 : Save lives and establish coordinated international efforts on missing migrants", 18/10/2018,https://rli.sas.ac.uk/blog/gcm-commentary-objective-8-save-lives-and-establish-coordinated-international-efforts-missing

ICMP, "ICMP and INTERPOL Convene Expert Meeting On DNA Analysis and Missing Migrants",21/11/2019 https://www.icmp.int/press-releases/icmp-and-interpol-convene-expert-meeting-on-dna-analysis-and-missing-migrants/

ICMP, “statement on the issue of missing migrants by representatives of Cyprus, Greece, and Malta at the conclusion of the 2nd meeting of the joint process 13 june 2019” https://www.icmp.int/wp-content/uploads/2019/06/icmp-gr-mm-047-3-doc-joint-statment-2nd-meeting-of-the-joint-process-geconverteerd.pdf

ICMP,”statement on the issue of missing migrants by representatives of Cyprus, Greece, and Malta at the conclusion of the 3 rd meeting of the joint process”, Athens, 19 November 2021 https://www.icmp.int/wp-content/uploads/2021/11/icmp-gr-mm-084-3-doc-statement.pdf

ICMP, Missing Migrants and refugees program https://www.icmp.int/wp-content/uploads/2020/12/Missing-Migrants-Program-Factsheet-English.pdf

ICMP, "Mediterranean States Can Access Forensic Capacity And Expertise to Locate and Identify Missing Migrants", 05/07/2023 https://www.icmp.int/news/mediterranean-states-can-access-forensic-capacity-and-expertise-to-locate-and-identify-missing-migrants/

ICMP, "Act Now to Save Lives and Prevent Migrants From Going Missing", 07/03/2022 https://www.icmp.int/press-releases/20931/

OUVRAGES

CATTANEO, Cristina, *Naufraghi senza volto: dare un nome alle vittime del Mediterraneo*, Milano : Raffaello Cortina Editore, 2018, 198 p.

KOBELINSKY, Carolina, FURRI, Filippo, Relier les rives - sur les traces des morts en Méditerranée, Paris : La Découverte, 2024,196 p.

TERVONEN, Taina, *Au pays des disparus*, Paris: Fayard,2019, 256 p.

RAPPORTS

« Nouvelles technologies et disparitions forcées Rapport du Groupe de travail sur les disparitions forcées ou involontaires », septembre-octobre 2023 A/HRC/54/22/Add. https://www.ohchr.org/sites/default/files/2024-04/A-HRC-54-22-Add-5-FR.pdf

ICRC, “the Missing - The right to know Action to resolve the problem of people unaccounted for as a result of armed conflict or internal violence and to assist their families”, OP/REX 02/522 Update No. 17/2002 https://reliefweb.int/report/world/icrc-update-project-missing-current-developments-no-2

ICRC,“Counting the dead, how registered deaths of migrants in the southern european sea border provide only a glimpse of the issue", November 2020 https://missingpersons.icrc.org/sites/default/files/2022-11/COUNTING-THE-DEAD-FINAL.pdf

ROBINS, Simon, « Analysis of Best Practices on the Identification of Missing Migrants Implications for the Central Mediterranean, central mediterranean route thematic » report series, issue n° 2,2018https://publications.iom.int/system/files/pdf/identification_of_missing_migrants.pdf

"the development of guiding principles for the proper management of the dead in humanitarian emergencies and help in preventing their becoming missing persons: First Expert's Meeting", International Review of the Red Cross, 2019, 101 ( 912), p.1213-1229 https://international-review.icrc.org/sites/default/files/pdf/1602948923/IRC101_3b/S1816383120000223a.pdf

33rd INTERNATIONAL CONFERENCE OF THE RED CROSS AND RED CRESCENT "Restoring Family Links while respecting privacy, including as it relates to personal data protection" Geneva, Switzerland 9–12 December 2019 https://rcrcconference.org/app/uploads/2019/12/RFL-Resolution_12-December-FINAL-at-1430_CLEAN_en.pdf

CICR, « Le processus d'identification forensique : une approche intégrée », 2022 https://www.icrc.org/fr/publication/4590-forensic-human-identification-process-integrated-approach

CICR, « Principes pour légiférer sur la situation des personnes portées disparues par suite d'un conflit armé ou de situation de violence interne : mesures de prévention des disparitions et de sauvegarde des droits et des intérêts des personnes portées disparues et de leur famille », 2002 https://www.icrc.org/fr/doc/assets/files/other/model-law-missing-0209-fre-.pdf

ICRC, "Guidelines on Coordination and Information-Exchange Mechanisms for the Search for Missing Migrants", November 2021 https://www.icmp.int/wp-content/uploads/2021/10/ICRC-Missing-Migrants-Mechanism-Guidelines.pdf

ICRC, Advisory service on international humanitarian law, "Humanity after Life: respecting and protecting the dead", April 2020 https://www.icrc.org/en/document/humanity-after-life-respect-and-protection-dead

ICRC," Restoring family links, Code of conduct on data protection", November 2015, Version 1.0 https://www.icrc.org/en/document/rfl-code-conduct

Last Rights, "The Dead, the Missing and the Bereaved at Europe's International Borders Proposal for a Statement of the International legal obligations of States", May 2017 https://www.ohchr.org/sites/default/files/Documents/Issues/Migration/36_42/TheLastRightsProject.pdf

# Listes des entretiens

| Numéro de l'entretien | nom code entretien | fonction de l'enquêté | durée de l'entretien | modalité | date de l'entretien |
|---|---|---|---|---|---|
| 1 | ONG 1 | DPO | 45 minutes | Visioconférence | 08/11/2019 |
| 2 | OI1 | DPO | 43 minutes | Visioconférence | 08/11/2019 |
| 3 | OI2 | DPO | 42 minutes | téléphone | 18/11/2019 |
| 4 | | consultant DPO | 44 minutes | téléphone | 18/11/2019 |
| 5 | ONG2 | DPO | 56 minutes | Viso | 20/11/2019 |
| 6 | OI3 | Information manager officer | 51 minutes | Visioconférence | 22/11/2019 |
| 7 | OI2 | DPO | 54 minutes | visioconférence | 11/12/2019 |
| 8 | | consultante | 39 minutes | Visioconférence | 18/12/2019 |
| 9 | ONG3 | DPO | 59 minutes | visioconférence | 19/12/2019 |
| 10 | OI3 | information manager officer | 47 minutes | Visioconférence | 06/01/2020 |
| 11 | ONG4 | DPO et archivistes | 1h23 | en présentiel | 13/01/2020 |
| 12 | ONG5 | DPO | 42 minutes | Téléphone | 16/01/2020 |
| 13 | ONG5 | DPO | 45 minutes | Téléphone | 17/01/2020 |
| 14 | | ingénieur | 44 minutes | Visioconférence | 27/01/2020 |
| 15 | | ingénieur | 32 minutes | Téléphone | 26/01/2020 |
| 16 | | ingénieur | 49 minutes | Visioconférence | 30/01/2020 |
| 17 | ONG 6 | DPO juriste | 1H02 | Visioconférence | 31/01/2020 |
| 18 | OI1 | policy officer | 57 minutes | Visioconférence | 04/02/2020 |
| 19 | OI2 | DPO | 3h environ | Présentiel | 04/02/2020 |
| 20 | | Identification morts 1 Activiste | | échanges mails | 20/02/2020 |
| 21 | ONG7 | DPO | 55 minutes | Visioconférence | 27/02/2020 |
| 22 | | Ingénieur | 46 minutes | Visioconférence | 13/03/2020 |
| 23 | | identification des morts 2 médecin légiste | 1H21 | Visioconférence | 17/03/2020 |
| 24 | | identification des morts 3 activiste-juriste | 1H08 | Visioconférence | 20/03/2020 |
| 25 | | dossier médical | 53 minutes | Visioconférence | 26/03/2020 |
| 26 | ONG8 | Ingénieur | 43 minutes | Visioconférence | 31/03/2020 |
| 27 | | identification des morts 4 chercheuse | 54 minutes | Visioconférence | 06/04/2020 |
| 28 | ONG8 | Ingénieur | 1H35 | Visioconférence | 09/04/2020 |
| 29 | ONG9 | Bénévole d'ONG | 47 minutes | Téléphone | 10/04/2020 |

| | | | | | |
|---|---|---|---|---|---|
| 30 | | identification des morts 5 journaliste | 53 minutes | Téléphone | 10/04/2020 |
| 31 | ONG10 | militante | 42 minutes | Téléphone | 12/04/2020 |
| 32 | | identification des morts 6 police | 1H08 | Visioconférence | 30/04/2020 |
| 33 | ONG11 | Bénévole d'ONG | 1h02 | Visioconférence | 05/05/2020 |
| 34 | ONG12 | policy officer | 45 minutes | Visioconférence | 06/05/2020 |
| 35 | OI2 | identification des morts 7 médecin légiste | 1H13 | Visioconférence | 14/05/2020 |
| 36 | | Identification morts 8 chercheur | 1H 22 | Visioconférence | 21/05/2020 |
| 37 | | chercheur | | échanges mails | 24/05/2020 |
| 38 | OI4 | Deputy Head *of* Operations Unit | 45 minutes | Visioconférence | 03/06/2020 |
| 39 | ONG13 | | 48 minutes | Visioconférence | 08/06/2020 |
| 40 | ONG14 | responsable juridique | 56 minutes | Visioconférence | 16/07/2020 |
| 41 | | chercheuse en science de l'information et de la communication | 38 minutes | WhatsApp | 16/09/2020 |
| 42 | | dossier médical | 1h07 | Visioconférence | 22/02/2021 |
| 43 | | dossier médical | 56 minutes | Visioconférence | 03/03/2021 |
| 44 | OI2 | DPO | 57 minutes | Visioconférence | 07/03/2021 |
| 45 | | dossier médical | 48 minutes | téléphone | 15/03/2021 |
| 46 | | dossier médical | 42 minutes | Téléphone | 15/03/2021 |
| 47 | ONG15 | ingénieur | 1h03 | Visioconférence | 18/03/2021 |
| 48 | | dossier médical | 52 minutes | Visioconférence | 26/03/2021 |
| 49 | | dossier médical | 44 minutes | Téléphone | 30/03/2021 |
| 50 | | dossier médical | 47 minutes | téléphone | 06/04/2021 |
| 51 | ONG16 | DPO | 54 minutes | téléphone | 07/04/2021 |
| 52 | | dossier médical | 56 minutes | téléphone | 07/04/2021 |
| 53 | | dossier médical | 1H07 | Visioconférence | 09/04/2021 |
| 54 | | dossier médical | 32 minutes | Téléphone | 09/04/2021 |
| 55 | | dossier médical | 39 minutes | Téléphone | 09/04/2021 |
| 56 | ONG 17 | Coordinatrice de programme | 1H23 | Visioconférence | 13/04/2021 |
| 57 | | dossier médical | 38 minutes | téléphone | 13/04/2021 |
| 58 | ONG18 | Coordinatrice de programme | 1H16 | téléphone | 13/04/2021 |
| 59 | | dossier médical | 44 minutes | Téléphone | 13/04/2021 |
| 60 | | dossier médical | 1H10 | téléphone | 14/04/2021 |
| 61 | | dossier médical | 1H03 | téléphone | 14/04/2021 |
| 62 | | dossier médical | 1H01 | Téléphone | |
| 63 | | dossier médical | 1H13minutes | en présentiel | 15/04/2021 |

| | | | | | |
|---|---|---|---|---|---|
| 64 | | dossier médical | 48 minutes | Téléphone | 15/04/2021 |
| 65 | | dossier médical | 53 minutes | Téléphone | 16/04/2021 |
| 66 | | dossier médical | 1H13 | Téléphone | 19/04/2021 |
| 67 | | dossier médical | 1H04 | Téléphone | 20/04/2021 |
| 68 | | dossier médical | 1h09 | Téléphone | 20/04/2021 |
| 69 | | dossier médical | 48 minutes | Téléphone | 22/04/2021 |
| 70 | | dossier médical | 36 minutes | Téléphone | 23/04/2021 |
| 71 | ONG19 | Coordinatrice de programme | 1h23 | Visioconférence | 24/04/2021 |
| 72 | | dossier médical | 44 minutes | Téléphone | 26/04/2021 |
| 73 | | dossier médical | 59 minutes | Téléphone | 27/04/2021 |
| 74 | | dossier médical | 1H07 | téléphone | 28/04/2021 |
| 75 | | dossier médical | 1H16 | Téléphone | 28/04/2021 |
| 76 | | dossier médical | 49 minutes | Téléphone | 04/05/2021 |
| 77 | | dossier médical | 58 minutes | Téléphone | 07/05/2021 |
| 78 | | dossier médical | 1h02 | Téléphone | 11/05/2021 |
| 79 | | dossier médical | 38 minutes | Téléphone | 14/05/2021 |
| 80 | | dossier médical | 44 minutes | téléphone | 15/05/2021 |
| 81 | ONG14 | responsable juridique | 3H30 environ | en présentiel | 16/08/2021 |
| 82 | ONG6 | DPO juriste | 1h15 minutes | Téléphone (WhatsApp) | 07/10/2022 |
| 83 | ONG1 | DPO | 55 minutes | téléphone (Signal) | 14/10/2022 |
| 84 | ONG 20 | DPO | 53 minutes | Visioconférence | 14/10/2022 |
| 85 | ONG21 | Chargée de coordination d'équipes de bénévoles | 28 minutes | en présentiel | 25/10/2022 |
| 86 | ONG22 | DPO | 33 minutes | Visioconférence | 27/10/2022 |
| 87 | ONG23 | DPO | 1H01 | Visioconférence | 10/11/2022 |
| 88 | ONG24 | DPO | 1H12 | Visioconférence | 15/11/2022 |
| 89 | ONG 25 | DPO | 32 minutes | Visioconférence | 30/11/2022 |
| 90 | ONG 26 | Coordinatrice de programme | 1H33 | Visioconférence | 06/12/2022 |
| 91 | OI2 | DPO | 55 minutes | Visioconférence | 26/05/2023 |
| 92 | ONG 27 | Coordinatrice de programme | 1H33 | Visioconférence | 06/12/202 |
| 93 | OI2 | DPO ingénieur | 1h23 | Visioconférence | 02/06/2023 |
| 94 | ONG28 | dossier médical | 55 minutes | Visioconférence | |
| 95 | ONG5 | Infirmier chargé de la coordination d'un programme médical d'une ONG humanitaire | 33 minutes | en présentiel | 26/07/2023 |

| | | | | | |
|---|---|---|---|---|---|
| 96 | ONG5 | Infirmier chargé de la coordination d'un programme médical d'une ONG humanitaire | 29 minutes | En présentiel | 05/08/2024 |