UNIVERSITÉ PARIS 1
PANTHÉON SORBONNE

MÉMOIRE DE RECHERCHE

UFR 11 – Science politique

Master parcours Développement et Action humanitaire

Silence, on surveille les journalistes.

Ce que le logiciel espion Pegasus dévoile des dangers de la surveillance et des attaques en ligne des reporters, ou les enjeux d'une dépendance structurelle au numérique.

Sous la direction de Monsieur le Professeur Jérôme Valluy

Alexandre Châtel

Année universitaire 2022-2023

L'université Paris I n'entend donner aucune approbation aux opinions émises dans les mémoires. Ces opinions doivent être considérées comme propres à leurs auteurs.

Ce que la recherche fait au journaliste

Je suis devenu journaliste il y a trois ans. Depuis mes débuts au sein d'une rédaction composée de journalistes français et exilés de plusieurs pays du monde, je travaille à participer d'une transformation du discours médiatique sur l'exil et la migration. Formé au sein d'une équipe riche de sa grande diversité de parcours, d'origine, d'expérience, je cherche à aller à contre-courant de pratiques journalistiques parfois encore trop stéréotypées, formatées et qui ne donnent que trop peu la parole aux premiers concernés. Les mots ont un poids, et la diversité est la clef de voute d'une meilleure représentation médiatique de l'actualité.

À ce stade, une mise en garde me semble nécessaire : ceci n'est pas un mémoire sur le logiciel Pegasus, mais un mémoire qui a pour objectif de montrer que Pegasus constitue d'une part, le summum d'une industrie de la surveillance et d'attaques en ligne, et de l'autre, son simple sommet. Ce que je souhaite, c'est de participer à une réflexion sur les transformations parallèles du champ médiatique et de l'information, qui se précarise, qui se numérise, et sur les imbrications inhérentes avec cette économie grandissante de la surveillance. Ce que je souhaite, c'est de défendre la sécurité des journalistes. Ma recherche porte ainsi sur la surveillance des reporters. Je tenterai, parmi d'autres réflexions, de soutenir la nécessité de rompre la frontière sémantique qui sépare bien trop souvent sécurité numérique et physique, et qui pose un voile sur les dangers concrets qu'elle représente.

Il me semble juste d'avertir à ce stade que j'ai été par moments, au cours de ma recherche, partagé entre ma position de journaliste et celle de chercheur. Une position qui me pousse à souhaiter me prouver auprès de mes pairs, de mes confrères et consœurs, de mes amis, essayant ainsi de produire un travail en mesure de faire avancer la question de la sécurité des journalistes. Une ambition difficilement conciliable dans le cadre de l'exercice ici soutenu et qui a créé de nombreux doutes, parfois des frustrations, mais qui ont consolidé le souhait d'une exigence élevée dans la rigueur de mon analyse.

Vous trouverez dans ce mémoire des éléments permettant, je l'espère, de mieux cerner l'ampleur de la société de surveillance dans laquelle nous vivons, des défis qu'elle pose aux cadres analytiques et des dangers qu'elle représente pour la sécurité des journalistes.

Ce mémoire est dédié à mes collègues, à toutes et tous les reporters décédés pour leur investigation, et à la liberté de la presse dans le monde.

Table des matières

Remerciements

*Mes vifs remerciements sont tout d'abord adressés à Monsieur le Professeur **Jérôme Valluy** qui m'a fait l'honneur de diriger ce travail de recherche. Je tiens à lui exprimer ma gratitude et mon profond respect.*

*Je tiens également à remercier Monsieur le Professeur **Gregory Daho**, second membre du jury, du temps et des remarques constructives adressées à l'égard de mon travail.*

*Je souhaite remercier toutes les personnes qui ont accepté d'échanger avec moi dans le cadre de ma recherche, parmi lesquelles : **Elodie Vialle**, **Phineas Rueckert**, **Maxine Singeot**, **Paloma de Dinechin** et **Alicia Arquetoux**. À elles et eux, je les remercie de leurs témoignages et du temps consacrés à alimenter la réflexion sur les enjeux de la surveillance des reporters.*

*Aussi, je souhaite adresser un mot au **Café Les Patios**, situé place de la Sorbonne, et à toute son équipe, qui m'ont accueilli chaque jour durant plusieurs épreuves depuis mon arrivée à Paris il y a quatre ans.*

*Je souhaite enfin adresser une mention spéciale à ma rédactrice en cheffe **Nina Gheddar** qui m'accompagne dans ma formation professionnelle et personnelle depuis plusieurs années. À elle, je lui adresse ma plus grande gratitude et ma plus haute estime.*

Introduction

« Depuis Pegasus, d'un côté les journalistes se disent 'on est tous surveillés' et ils flippent, et de l'autre, 'bon on est tous surveillés' et ils ne font rien. Donc c'est comme un régime, c'est la nouvelle année et vous vous dites 'foutu pour foutu je vais manger des bonbons' ».

Entretien avec Elodie Vialle, chercheuse en sécurité numérique et liberté d'expression à Harvard.

Depuis 2000, 1787 journalistes dans le monde ont été tués dans l'exercice de leur métier[1]. En têtes de liste, l'Irak, la Syrie, le Mexique, l'Afghanistan, l'Inde (voir annexe 2)…Tués, détenus ou disparus, les reporters ont toujours été des cibles stratégiques pour qui veut taire l'information. Aujourd'hui, on compte 533 journalistes emprisonnés dans le monde[2]. Mais combien sont en permanence fichés, suivis ou menacés ? Voilà tout l'objet de la surveillance.

En juillet 2021, le consortium international de seize médias coordonné par Forbidden Stories dévoile le Projet Pegasus, qui révèle l'usage de la technologie espionne Pegasus fabriquée par le groupe israélien NSO et vendue à des gouvernements autoritaires[3]. Exportée sous l'accord du Ministère de Défense israélien, celle-ci permet d'infecter n'importe quel téléphone portable de manière totalement invisible et d'y surveiller les moindres faits et gestes de son utilisateur. Amnesty International et Forbidden Stories ont eu accès à une liste de plus de 50 000 numéros de téléphones marqués d'intérêt par NSO depuis 2016[4]. La liste inclut des centaines de dirigeants d'entreprises, de figures religieuses, d'universitaires, d'employés d'ONGs, d'officiels de gouvernements, de ministres et de présidents. Elle inclut également plus de 180 journalistes, de reporters comme éditeurs en chefs, provenant du *Financial Times*, *CNN*, the *New York Times*, *France 24*, *The Economist*, *Associated Press*, *Reuters*, *Mediapart*[5]…

Les apports de l'enquête sont multiples. Toutefois, le focus sur la plus haute classe politique qui aurait été surveillée, parmi laquelle, le cabinet présidentiel français, pose un voile sur des dangers encore plus pressants quant à la sécurité des reporters d'investigations dans le monde. En ce sens, les contextes nationaux, politiques, socio-économiques et individuels apparaissent bien souvent lissés. La surveillance, au-delà du phénomène, prend diverses formes et surtout provoque des effets très différents selon les pays, et selon la profession exercée.

[1] Reporters Sans Frontières, bilan « Des journalistes détenus, tués, otages et disparus dans le monde », 2022.
[2] Libération, « 533 journalistes emprisonnés dans le monde », le 14 décembre 2022.
[3] Forbidden Stories, « Pegasus : la nouvelle arme mondiale pour faire taire les journalistes », le 18 juillet 2021.
[4] Le Monde, « Projet Pegasus : révélations sur un système mondial d'espionnage de téléphone », le 18 juillet 2021.
[5] The Guardian, "Revealed: leak uncovers global abuse of cyber-surveillance weapon", le 18 juillet 2021.

État de l'art

Ma recherche sur la surveillance des journalistes s'inscrit à la croisée entre deux champs : le champ des études sur la surveillance et le champ du journalisme et de l'information.

Ce que nous disent les études sur la surveillance, à l'image d'Oliver Aïm dans *Les théories de la surveillance*[6], c'est que les territoires de la surveillance s'étendent. Les caméras de surveillance en ville, la géolocalisation, les comptes connectés, les algorithmes, la reconnaissance faciale…La surveillance recouvre désormais toute question qui implique les données, la vie privée, les technologies de l'information et de la communication, les nouvelles formes de l'exercice du pouvoir. D'où l'imposition de la formule « société de surveillance » dont l'origine provient de Michel Foucault qui disait dans *Surveiller et punir*[7] que « notre société n'est pas celle du spectacle, mais de la surveillance ». Le succès de sa notion de « panoptisme » est devenu l'emblème de la surveillance des sociétés modernes. La surveillance doit être pensée comme un phénomène total et le rapport au concept « pan » (« tout » en grec) entretient une relation étroite avec la « panique » : tous surveillés, tous tracés. Le champ des *surveillance studies* voit ainsi le jour avec le travail de David Lyon et Gary T. Max au début des années 2000 et la création de la revue *Surveillance & Society*. En 2001, ce champ définit la surveillance dans la perspective de la sécurité avec un point de départ très politique : les attentats du 11 septembre 2001 et l'entrée des Etats-Unis en guerre contre la terreur, marquée par l'obsession nouvelle d'une information totale. C'est ainsi qu'ils décrivent un « tournant surveillanciel », lorsque la surveillance devient un enjeu à part entière.

Il faut toutefois, à l'image de Florent Castagnino dans *Critique des surveillance studies*[8], accorder une vigilance importante dans la mobilisation de ces-dernières. Les enjeux portés par ce champ proviennent de trois constats : celui du développement des technologies de l'information, du contexte de lutte contre le terrorisme et des inquiétudes grandissantes quant à la protection de la vie privée. L'objet « surveillance » est protéiforme, parfois perçu de manière banale, participative et bien souvent exceptionnelle, il recouvre une multitude de réalités et est difficile à appréhender. Toutefois, l'usage d'un seul terme englobant toutes ces réalités, « surveillance », questionne sa plus-value conceptuelle. Le champ des *surveillance studies*,

[6] Aïm Olivier, *Les théories de la surveillance. Du panoptique aux Surveillance Studies*, Armand Colin, 2020.
[7] Foucault Michel, *Surveiller et punir : Naissance de la prison*, éditions Gallimard, 1975.
[8] Castagnino Florent, *Critique des surveillances studies. Éléments pour une sociologie de la surveillance*, Déviance et Société, 2018.

malgré sa plus grande diversité et son autocritique, considère en effet dans ses approches presque à chaque fois la surveillance comme un danger en soi. Une démarche qui se heurte à une série de constats contemporains : certes, on observe une démocratisation de la surveillance, à partir de bases de données, qui concerne tout le monde ; pourtant, la surveillance devient à la fois plus visible et invisible dans ses effets, et la frontière entre surveillant et surveillé devient floue. De même, le développement des technologies ne doit pas être considéré comme responsable de la surveillance, mais comme la condition de son intensification. Il faut ainsi, en manipulant les *surveillance studies*, prêter attention aux tensions qui traversent ce champ et sur lesquelles nous reviendrons : celle d'une aporie définitionnelle de la surveillance ; celle du caractère technique ou bien stratégique qui lui est conféré ou encore celle de l'ambivalence dans ses effets exclusivement liberticides ou potentiellement positifs.

De cette mise en garde conceptuelle et méthodologique, il convient de penser encore plus globalement la surveillance comme imbriquée dans une économie nouvelle. Pour cela, nous mobiliserons Shoshana Zuboff qui dans *L'âge du capitalisme de surveillance*[9] décrit ce nouvel ordre économique qui « revendique l'expérience humaine comme matière première gratuite destinée à être traduite en données comportementales ». Le capitalisme de surveillance révèle que le tournant numérique n'est pas celui d'un effet pro-social, rapprochant les individus et l'accès au savoir, mais celui d'un objectif commercial. Google, à l'image de General Motors pour la révolution industrielle, en est le précurseur et cela s'est vite étendu à Facebook, puis Microsoft, Amazon et Apple. Ces entreprises ont profité de l'après 11 septembre 2001 et des peurs de chacun pour étendre leur système de surveillance sous couvert de se présenter comme les défenseurs des droits et de l'émancipation, sans frein législatif ou institutionnel. Leur protection tient de trois éléments : l'illisibilité des systèmes, l'ignorance des processus et le sentiment d'inévitabilité de leur action. Pour Zuboff, la notion même de capitalisme de surveillance est encore mal comprise : il s'agit, au-delà du tournant numérique, d'une nouvelle ère du capitalisme qui exploite la technologie à ses fins. Si on retire en effet la technologie, on met très vite à nu les objectifs de ce capitalisme. La critique de Zuboff rejoint l'analyse de Castagnino en ce qu'elle porte directement sur cette économie nouvelle et non directement sur les technologies dont elle se sert : le capitalisme de surveillance n'est pas une technologie mais une logique qui imprègne la technologie. Une logique qui fait le pari réussi de l'extrême dépendance des individus à internet et qui rend insensible au fait d'être surveillés, géolocalisés, analysés ou qui à l'inverse, résigne du fait d'un sentiment d'impuissance face au système.

[9] Zuboff Shoshana, *L'âge du capitalisme de surveillance*, éditions Zulma, 2018.

La surveillance des reporters s'inscrit dans cette ère nouvelle du capitalisme de surveillance. Celle d'une dépendance au numérique dans la profession et par conséquent, celle d'une surexposition structurelle à la surveillance. Comme le montrent en effet Inna Lyubareva et Emmanuel Marty dans leur ouvrage *Vingt-cinq ans d'information en ligne, une exploration des transformations structurelles des médias*[10], depuis les années 2000, les médias ont dû se saisir d'internet et des plateformes intermédiaires (Facebook, Twitter, YouTube) car elles structurent l'accès et la circulation des contenus informationnels en ligne. Le champ socio-professionnel du journalisme s'est modifié. On observe en effet une double dynamique entre les médias qui vont négocier leur place et les médias qui sont natifs de cette ère. La structure de l'espace professionnel apparaît plus dispersée, davantage numérisée et bien souvent, plus précarisée financièrement. De plus, on observe un recours massif des techniques numériques et une personnification des contenus notamment par l'essor du format *live*. Les plateformes apparaissent à la fois comme les nouveaux partenaires incontournables et comme des concurrents qui imposent des règles algorithmiques fondées sur des techniques de marketing, qui viennent ainsi transformer les stratégies éditoriales et l'ensemble du champ journalistique.

Enfin, il est nécessaire de penser la surveillance des journalistes comme une activité qui touche à la fois les pays démocratiques comme autoritaires. À ce titre, Guilhem Giraud, ancien agent du renseignement français[11], montre comment la surveillance des journalistes est devenue une pratique courante dans le monde entier, y compris en Europe. Cette surveillance, malgré les encadrements juridiques, est justifiée par les gouvernements au nom de la sécurité nationale et de la lutte contre le terrorisme. Dans le cas de la France, il explique que depuis la loi du 24 juillet 2015, les services de renseignements sont autorisés à recueillir des données sur les journalistes lorsqu'elles sont susceptibles de compromettre la sécurité nationale. Cette pratique généralisée constitue alors une lourde atteinte à la liberté de la presse et à la vie privée.

Les journalistes se retrouvent ainsi en première ligne d'une dynamique de surveillisation des activités humaines et qui devient presque banale dans leur pratique professionnelle. Celle-ci résulte en une ambivalence dans leur rapport aux plateformes GAFAM (Google, Apple, Facebook, Amazon et Microsoft) : devoir les investir pour élargir leur diffusion d'information, ou tenter de négocier avec celles-ci les droits voisins de leurs contributions. Une chose est sûre, la pratique journalistique est devenue structurellement dépendante de cette économie.

[10] Lyubareva Inna et Marty Emmanuel, *Vingt-cinq d'informations en ligne, une exploration des transformations structurelles des médias*, Revue « Les enjeux de la communication et de l'information », le 26 septembre 2022.
[11] Giraud Guilhem, *Confidences d'un agent du renseignement français*, éditions Robert Laffont, 2022.

Les enjeux de la surveillance des reporters

L'affaire Pegasus illustre très bien le propos de Shoshana Zuboff qui décrit le « sans précédent » de l'économie de surveillance contemporaine. De son exportation à son usage final, Pegasus constitue en effet un exemple parfait de la complexité et technicité de la surveillance moderne, où s'imbriquent ici l'implication du groupe NSO, du Ministère de Défense israélien, des Etats clients et des différentes cibles.

Toutefois, les contextes ne sont pas les mêmes, et les dangers de l'usage d'une telle technologie peuvent être très différents d'un pays à l'autre. C'est le cas du Mexique, premier gouvernement client du groupe NSO, qui avec Pegasus devient au plus haut de sa technologie d'espionnage[12]. Parmi les 50 000 numéros de téléphones retrouvés, plus de 15 000 provenaient du Mexique entre 2014 et 2017, le plaçant de fait comme le pays ayant eu le plus recours à cette technologie espionne. Sous couvert de ce que le gouvernement mexicain dissimule sous le titre de lutte contre la criminalité, l'enquête a révélé que les téléphones de plus de 25 journalistes et activistes mexicains étaient espionnés entre 2015 et 2017[13]. Parmi eux figure la journaliste Carmen Aristeguí, célèbre pour ses investigations sur la corruption, et Cecilio Piñeda, journaliste qui enquêtait sur la corruption au sein de l'Etat de Guerrero. Il a été assassiné quinze jours après avoir été ajouté sur cette liste – si aucun lien direct ne peut être prouvé, il est juste de rappeler que cette technologie permet d'obtenir une géolocalisation en temps réel[14]. Pendant les 70 ans de gouvernance du *Partido Revolucionario Institucional* au XXe siècle au Mexique, la surveillance des politiciens et journalistes a souvent été à l'œuvre, et devait changer à partir de 2000 et l'alternance politique, considérée comme un tournant démocratique[15]. Cette longue liste de téléphones interpelle alors sur le niveau de surveillance pourtant associé à des régimes autoritaires et rappelle que les dangers qu'elle implique sont intimement liés avec le degré de liberté de la presse et de sécurité des reporters assurées par l'Etat.

De plus, la surveillance contemporaine des journalistes doit être pensée comme la conséquence d'une dépendance structurelle – et grandissante – au numérique, à internet et aux plateformes de communication (Facebook, Twitter, YouTube)[16]. Une dépendance qui produit

[12] The Washington Post, "How mexico's traditional political espionage went high-tech", le 21 juillet 2021.
[13] The Washington Post, "Private Israeli Spyware used to hack cellphones of journalists, activists, worldwide", le 18 juillet 2021.
[14] The Washington Post, "Private Israeli Spyware used to hack cellphones of journalists, activists, worldwide", le 18 juillet 2021.
[15] The Washington Post, "How mexico's traditional political espionage went high-tech", le 21 juillet 2021.
[16] Lyubareva Inna et Marty Emmanuel, *Vingt-cinq d'informations en ligne, une exploration des transformations structurelles des médias*, Revue « Les enjeux de la communication et de l'information », le 26 septembre 2022.

un double effet. Elle crée d'une part une surexposition des journalistes à la surveillance de leurs activités et données, et modifie continuellement le champ et la pratique journalistique. De l'autre, par la personnification croissante des contenus, elle crée une plus grande exposition des journalistes aux risques d'attaques numériques et de harcèlement en ligne. Les journalistes sont, et doivent être définis, du fait de cette dépendance, comme une catégorie à risque et dont l'indépendance de leur travail est structurellement compromise.

La surveillance – de plus en plus numérique – a bien souvent comme revers de la médaille, les attaques en ligne. Les dangers en question sont multiples : harcèlement en ligne, menaces, intimidations, usurpation d'identité…En 2017, le Conseil de l'Europe a publié une étude sur le harcèlement à l'encontre des journalistes au sein de ses 47 membres[17] : sur les 940 journalistes interrogés, 40 % auraient subi des formes de harcèlement ayant "affecté leur vie personnelle". Dans 53 % des cas, il s'agissait de cyberharcèlement. Souvent invisibilisés, ceux-ci sont lourds de conséquences : 31 % des journalistes atténuent la couverture des sujets après avoir été harcelés, 15 % les abandonnent, 23 % ne diffusent pas certaines informations, et 57 % ne dénoncent même pas ces violences[18], provoquant ainsi un large phénomène de censure.

Cependant, les journalistes sont inégaux devant ces dangers. Il existe, en effet, une variable de genre, d'ethnie et d'orientation sexuelle dans cette surexposition aux dangers du numérique. Selon le rapport de 2020 de IWMF[19], près de trois femmes journalistes sur quatre (73%) disent avoir déjà expérimenté de la violence en ligne, avec en première forme des menaces de violences physiques (25%) et sexuelles (18%). Une tendance encore plus lourde pour les femmes lesbiennes (85%) ou bisexuelles (88%). Ce constat vient également nourrir l'hypothèse selon laquelle le harcèlement de genre se trouve à l'intersection de l'ethnie et de l'orientation sexuelle. Toute catégorie confondue, plus d'une femme reporter sur deux est victime de violences en ligne, une tendance qui reste bien plus élevée chez les femmes qui s'identifient comme latinos, noires, juives ou d'origine indigène, allant jusqu'à un écart de 37% entre les femmes blanches (61%) et les femmes juives (88%)[20]. En outre, la surveillance fait des journalistes une catégorie à risque, mais vient également creuser des inégalités préexistantes. Les journalistes d'investigation, les femmes racisées et toute minorité perçue sont les principales cibles de cette surveillance et principales victimes de ces attaques.

[17] Conseil de l'Europe, rapport sur la sécurité des journalistes, avril 2017.
[18] Reporters Sans Frontières, « Censure et surveillance des journalistes : un business sans scrupules », Reza Moini, Benjamin Ismail, Elodie Vialle, enquête de 2017.
[19] International Women's Media Foundation, survey of online harassment.
[20] International Center for Journalists and UNESCO, "The Chilling: a global study of online violence against women journalists", 2020.

Par ailleurs, il faut aussi rappeler que les journalistes sont également des cibles d'intérêt car ils occupent une position stratégique dans une société : ils sont le contact rapproché, voire le porte-parole, des sources de l'information. Pour un gouvernement ou un groupe qui souhaite surveiller toute ou partie de sa population, les journalistes tiennent ce rôle par nature ambivalent de relai d'information et de connexion avec les sources de l'information. Dans les cas où celles-ci seraient dissidentes, leur surveillance permet de les atteindre plus facilement. La question de la sécurité des journalistes doit alors se penser de manière indissociable avec la question de la sécurité des sources.

Cependant, il est nécessaire de questionner la prise de conscience collective des enjeux – et dangers – de la surveillance. Entre le contexte financier du champ socioprofessionnel qui se précarise, se numérise[21] et la progression exponentielle des technologies de surveillance[22], les journalistes se retrouvent dans une forme d'ambivalence dans leur rapport à ces dangers : d'un côté, négocier les nouvelles règles du capitalisme de surveillance et des plateformes ; de l'autre, s'y conformer, par résignation ou par manque de moyens.

En outre, les dangers du numérique ne peuvent être pensés de manière individuelle car la précarité et les discriminations à l'œuvre sont des faits sociaux qui s'observent collectivement dans une société. Il faut dès lors opter pour une approche holistique des dangers que la surveillance provoque pour la sécurité des reporters et de leurs sources. La surveillance des journalistes constitue ainsi une atteinte forte aux libertés fondamentales, parmi lesquelles : la vie privée, la liberté d'informer et la liberté de la presse. Pegasus est en effet un outil très puissant pour tout Etat qui souhaite contrôler sa population et en première ligne, ses dissidents. Mais il ne constitue, en fin de compte, qu'une goutte d'eau dans l'océan des technologies de surveillance. Les dangers que cette société de surveillance implique pour les journalistes, pour les sources d'information et pour la profession, résonnent alors avec encore plus d'intensité avec l'interprétation de Shoshana Zuboff qui voit, en somme, la surveillance comme une dépossession des droits humains essentiels[23].

[21] Lyubareva Inna et Marty Emmanuel, *Vingt-cinq d'informations en ligne, une exploration des transformations structurelles des médias*, Revue « Les enjeux de la communication et de l'information », le 26 septembre 2022.
[22] Zuboff Shoshana, *L'âge du capitalisme de surveillance*, éditions Zulma, 2018.
[23] Zuboff Shoshana, *L'âge du capitalisme de surveillance*, éditions Zulma, 2018.

Problématisation

Parallèlement, les territoires de la surveillance et les territoires du numérique s'étendent. En conséquence, la surveillance se complexifie et passe toujours plus par le numérique. Pourtant, malgré les dangers que les technologies de surveillance de plus en plus sophistiquées impliquent, et dont Pegasus est l'illustration, les journalistes continuent d'être dépendants aux plateformes sur lesquelles ils y sont surexposés. Quelles sont alors les dynamiques qui font des journalistes une catégorie dépendante, à risque et surexposée aux dangers de la surveillance et des attaques en ligne ?

Démarche d'enquête et limites méthodologiques

Dans le but de poursuivre cette recherche au sein d'un mémoire plus conséquent consacré aux enjeux de la surveillance des journalistes, j'ai souhaité ici dédier ma recherche à présenter de manière panoramique les enjeux que pose la surveillance contemporaine à la sécurité des journalistes, de leurs sources et de leur travail. Le tout, en partant du logiciel Pegasus afin de montrer qu'il ne constitue que le sommet de l'iceberg des dangers causés par les technologies de surveillance et d'attaques en ligne.

L'une de mes limites tient du fait que je n'ai pas discuter de manière formelle avec des victimes directes de cyberharcèlement pour des enjeux de poids psychologique. De la même manière je n'ai pas pu discuter avec des victimes directes de Pegasus, principalement pour des enjeux de confidentialité étant eux-mêmes des reporters d'investigation : ma démarche a alors été de passer par des canaux d'information proches des victimes, à l'image des reporters Phineas Rueckert et Paloma de Dinechin qui ont participé à l'investigation.

Aussi, j'ai conscience que mes enquêtés et l'analyse de leurs réponses tient d'une variable circonstancielle : chaque journaliste ou chercheur a un point de vue différent car personnel des enjeux de la surveillance. J'ai toutefois préféré faire le choix de privilégier peu d'entretiens afin de prendre le temps de les exploiter à bon escient dans le cadre de cet exercice. Aussi, ma démarche est ma principale limite : à vouloir monter en généralité pour tenter de décrire des tendances qui se retrouvent à la croisée du champ du journalisme et du champ de la surveillance, j'ai tout à fait conscience de l'existence d'une multitude de variables qui viennent complexifier la compréhension de ces enjeux. Variables parmi lesquelles en premier lieu : les contextes nationaux, socioéconomiques, l'État de droit, la liberté de la presse, ou encore les relations financières et politiques entre les médias et le pouvoir public. C'est pourquoi j'ai tenu à aborder une approche holistique des enjeux de la surveillance des reporters.

Outils de recherche

1. **Tableau de reporting** : ici se trouve l'ensemble de mes avancées. Ce document très détaillé m'a servi de carnet de bord tout au long de l'année.

2. **Étude forensique** : vulgarisation du procédé de vérification de la présence d'un virus malicieux basée sur le rapport du Security Lab d'Amnesty International de 2021. Ce rapport documente les traces forensiques laissées sur des appareils IOS et Android infectés par Pegasus, de 2014 jusque juillet 2021.

3. **Cinq entretiens semi-directifs** :

    - **Elodie Vialle** : Journaliste, consultante en sécurité numérique et liberté d'expression et chercheuse à l'université d'Harvard pour échanger sur les dangers de la surveillance, couplés aux changements du champ journalistique.

    - **Phineas Rueckert :** Journaliste à Forbidden Stories, média en charge de l'affaire Pegasus sur laquelle il a été l'un des principaux investigateurs pour revenir sur le déroulé de l'enquête.

    - **Paloma de Dinechin** : Journaliste d'investigation basée au Mexique pour discuter des journalistes mexicains victimes de Pegasus.

    - **Maxine Singeot :** Chargée de projet au pôle soutien chez Reporters Sans Frontières pour revenir sur leurs actions en matière de protection des journalistes contre le harcèlement en ligne.

    - **Alicia Arquetoux :** Étudiante en journalisme, pour discuter des formations en matière de sécurité digitale au sein des écoles de journalisme.

4. **Formation professionnelle** : suivi d'une formation sur « La sécurité numérique des journalistes » assurée par **Laurent Richard**, fondateur du média Forbidden Stories.

Annonce de plan

Dans une première partie, je montrerai en quoi, à travers le cas de l'affaire Pegasus, la surveillance des journalistes est très étendue et met à l'épreuve les cadres analytiques classiques, dans le but de définir et encadrer les enjeux qu'elle constitue (I). Dans une deuxième partie, je développerai les arguments qui, tendanciellement, font que les journalistes sont davantage exposés à la surveillance, aux attaques en ligne et à leurs dangers (II). Dans une troisième partie, je soulèverai une série de questions qui permettent d'apporter des nuances à la compréhension de la surveillance contemporaine des journalistes (III). De manière transversale, je tenterai d'avancer des éléments qui permettent de questionner le rapport même des journalistes à la surveillance dont ils sont la cible.

I.

I. Les contextes dans lesquels s'inscrit la surveillance des journalistes : un enjeu complexe et difficile à encadrer

Dans cette première partie, nous montrerons en quoi la surveillance des journalistes s'inscrit au sein de trois contextes : un contexte politique vaste (A), un contexte sociologique à l'épreuve (B), enfin, un contexte d'une économie de surveillance généralisée (C).

A. La surveillance des journalistes s'inscrit dans un contexte politique vaste : Pegasus, le sommet de l'iceberg des dangers du numérique

En juillet 2021, le Projet Pegasus révèle notamment que le Président Emmanuel Macron, l'ancien Premier Ministre Edouard Philippe ainsi que quatorze autres ministres ont été sélectionnés par les services secrets marocains pour une potentielle surveillance via le logiciel Pegasus[24]. Suivant ces révélations, le Président aurait immédiatement convoqué une réunion d'urgence sur la cybersécurité et engagé des négociations diplomatiques avec le gouvernement israélien, exigeant l'interdiction de surveiller les numéros à code français[25]. Entre crise diplomatique, enjeux de sécurité défense et effet de panique politique…et si la surveillance de la plus haute classe politique par Pegasus cachait un danger encore plus pressant ?

Tout d'abord, il est essentiel de rappeler une chose : Pegasus est une arme militaire et est considéré comme le logiciel espion le plus puissant jamais développé par une entreprise privée[26]. Le groupe NSO, via ce logiciel, peut – par exemple – enregistrer les appels, activer secrètement les caméras ou le micro et enregistrer les conversations, avoir accès aux photos ou encore, localiser en temps direct la position de son utilisateur[27]. Ce logiciel est développé et vendu à des gouvernements par le groupe israélien NSO : il peut infecter des milliards de téléphones, qu'ils soient sur des systèmes opératoires Android (Samsung) comme IOS (Apple). Dans sa première version en 2016 déjà bouleversante, l'infection nécessitait de cliquer sur un lien issu d'un email ou d'un sms malicieux. Aujourd'hui, l'infection se fait en « zéro clic », elle est quasi indétectable, et profite de toutes les failles des applications comme WhatsApp, Imessage, Musique[28], comme l'explique Laurent Richard, fondateur de Forbidden Stories :

[24] France Info, « Pegasus : le gouvernement et toute la classe politique française dans le viseur du Maroc », Elodie Guéguen, le 20 juillet 2021.
[25] Forbidden Stories, « Pegasus : la nouvelle arme mondiale pour faire taire les journalistes », le 18 juillet 2021.
[26] Forbidden Stories, « Pegasus : la nouvelle arme mondiale pour faire taire les journalistes », le 18 juillet 2021.
[27] The Guardian, "What is Pegasus and how does it hack phones?", le 18 juillet 2021.
[28] The Guardian, "What is Pegasus and how does it hack phones?", le 18 juillet 2021.

« *Si vous êtes victime d'une attaque Pegasus, vous ne le saurez jamais, parce que maintenant ce sont des attaques zéro-clic. Il n'y a plus besoin de cliquer sur un SMS et un lien attaché à un SMS qui serait malveillant. En fait, vous dormez, votre téléphone est ciblé, il ne vibre pas, la personne rentre dans votre téléphone, efface la première trace qu'il vient de laisser, et prend le contrôle entier de votre appareil* ».

Laurent Richard, extrait de la formation « Sécurité numérique des journalistes ».

Une fois infecté, le logiciel peut contrôler administrativement le téléphone et ainsi avoir un pouvoir que le propriétaire lui-même n'a pas. Une fois infecté, Pegasus devient un outil de surveillance jour et nuit.

Cependant, il convient de comprendre que la surveillance frappe plus dangereusement les journalistes. En effet, derrière un impact médiatique fort de l'enquête permis par les révélations autour des plus grands politiciens et chefs d'Etats, se cache une autre catégorie de la population, plus fragile et prise pour cible : les reporters d'investigations. Raconter l'histoire des journalistes victimes de Pegasus, c'est le choix que l'équipe du média Forbidden Stories a mené (voir annexe 3). Au sein de cette dernière, Phineas Rueckert, journaliste d'investigation, raconte :

« Notre but c'était pas forcément de se concentrer sur les histoires d'hommes politiques, des grands noms, c'était de vraiment lancer ça à partir des histoires de journalistes, des activistes et défenseurs des droits de l'Homme, des gens qui ont pas beaucoup de voix, et pour qui l'impact allait être plus important ».

Extrait d'entretien avec Phineas Rueckert, le 11 janvier 2023.

Autour d'un café discret près de leur rédaction à Bastille, mon échange avec Phineas Rueckert permet de comprendre la double dynamique ici en jeu lorsqu'il décrit que « l'impact allait être plus important » notamment pour les journalistes. D'une part, que parler de leurs histoires, bien souvent oubliées, mettrait en lumière d'autres récits. C'est précisément tout le projet de Forbidden Stories dont l'ambition est de poursuivre les enquêtes de journalistes assassinés, défendant ainsi que « tuer le messager ne tuera pas le message »[29]. De l'autre qu'en proportion, ce sont majoritairement des journalistes – plus de 180 – qui ont été ciblés.

[29] Forbidden Stories, voir site internet, "About us".

De plus, si de très nombreux journalistes sont surveillés, ils le sont aussi de manière massive. Afin d'en cerner l'étendue, il est intéressant de voir l'étude forensique d'Amnesty International qui retrace la technique de détection du virus au sein d'un téléphone[30]. Après vulgarisation, et en reprenant les exemples de trois journalistes surveillés, nous obtenons des chiffres édifiants.

Nom	Période d'attaques	Nombre d'attaques	Nombre de numéros de téléphones / serveurs différents de provenance	Exemple de message malicieux
Carmen Aristegui	Du 20/11/2014 au 28/07/2016	**70**	**27** numéros de téléphones différents (tous en +52 = numéro national)	**Message malicieux** : « *Hace 5 dias q no aparece mi hija te agradecere mucho q compartan su foto, estamos destrozados es un infierno : http://bit[.]ly/29rnk6c (https://smsmensaje [.]mx/7960742s/)* »
Edwy Plenel	Du 05/07/2019 au 05/09/2019	**25**	**11** serveurs différents	Attaque zéro clic
Lénaig Bredoux	Du 08/07/2019 au 10/07/2020	**44**	**21** serveurs différents	Attaque zéro clic

Vulgarisation réalisée par données croisées[31].

Ce-dernier permet d'observer plusieurs choses : que les attaques (tentatives de *hacking*) sont massives – au nombre de 70 pour la journaliste d'investigation mexicaine Carmen Aristegui ; étendues dans le temps – des mois, voire des années ; et quasi indétectables car proviennent de numéros et/ou serveurs toujours différents. Aussi, ce tableau est révélateur du progrès très rapide de la technologie. Dans sa première version, visible en 2014, l'infection suppose de cliquer sur un lien à travers un message frauduleux, comme ici « Cela fait 5 jours que ma fille

[30] Amnesty International Security Lab, "Forensic Methodology report. How to catch NSO Group's Pegasus", 2021.
[31] Ce tableau a été réalisé en comptant manuellement le nombre de récurrences d'attaques et de numéros de téléphones et/ou serveurs de provenance pour chacun des journalistes ici cités.

a disparu, peux-tu repartager cette photo d'elle, nous sommes bouleversés… ». Mais à partir de 2018, l'infection devient « zéro clic » : invisible, indétectable.

En conséquence, il convient de rappeler en quoi la surveillance des journalistes est un phénomène très dangereux. Par exemple, depuis 2011, le gouvernement mexicain a largement contracté auprès de NSO. Si l'accord initial avait pour fond la lutte contre le terrorisme et les groupes criminels, le New York Times a trouvé des preuves de l'usage détourné de Pegasus[32]. En effet, entre 2014 et 2017, au moins 25 reporters mexicains apparaissent comme cibles de Pegasus[33]. Le gouvernement de l'ex-Président Peña Nieto aurait utilisé de manière massive le malware et les dangers sont clairs : sous sa présidence le Mexique est devenu le pays le plus dangereux où exercer la profession journalistique[34]. Pendant son mandat, l'association Artículo 19 a enregistré 2502 agressions contre des reporters, qui incluent 47 assassinats[35]. Parmi ces-derniers il faut noter celui de Cecilio Piñeda Birto, assassiné le 2 mars 2017 pour ses enquêtes sur la corruption et qui, seulement quelques semaines plus tôt, voyait son numéro de téléphone ciblé par Pegasus. Sans causalité vérifiable, si son téléphone a bien été hacké, alors sa position était connue en permanence. Une chose est sûre, la surveillance Pegasus apparait ainsi comme l'un des outils les plus puissants pouvant faire taire les journalistes et la presse.

Toutefois, malgré son très lourd danger, le logiciel Pegasus s'inscrit au sein d'une économie très vaste et lucrative de la censure. Phineas Rueckert alerte à ce sujet :

> *« La surveillance des journalistes c'est pas que Pegasus, c'est principalement des méthodes moins sophistiquées. C'est la surveillance des réseaux sociaux, c'est le phishing, le hacking, ou encore une attaque digitale pour faire tomber un site ».*
>
> **Extrait d'entretien avec Phineas Rueckert, le 11 janvier 2023.**

Pegasus est un outil certes très puissant, mais il est aussi très couteux et utilisé dans des situations bien précises. La surveillance et les attaques en ligne s'apparentent comme l'apanage des pays répressifs en matière de liberté d'information, voire de liberté de la presse, avec en

[32] The New York Times, "Using texts as lures, governments spyware targets Mexican journalists and their families", le 19 juin 2017.
[33] Aristegui Noticias, « Pegasus Project : Más de 25 periodistas en México de TV, radio, internet y prensa fueron blanco de espionaje », le 18 juillet 2021.
[34] Proceso, "Peña Nieto, el desenfrenado espionaje contra periodistas", le 18 juillet 2021.
[35] Articulo 19, rapport sur « La sécurité des journalistes mexicains », 2018.

première ligne, la Chine, l'Iran, la Syrie ou l'Ouzbékistan qui cherchent à surveiller au plus près possible l'activité des journalistes[36] (voir annexe 1). A ce titre, Laurent Richard raconte :

> « *Ça se fait énormément en Azerbaïdjan par exemple. C'est vraiment une sorte de culture du pays. Mais dans plein d'autres pays, c'est faire chanter les journalistes. Donc souvent les journalistes peuvent être surveillés. C'était le cas d'une journaliste star d'Al Jazeera, présentatrice d'un magazine. Et ils vont vouloir vous hacker parce qu'ils veulent trouver du contenu personnel, une photo, une vidéo, pour pouvoir ensuite vous faire chanter et du coup pour pouvoir vous nuire ou vous dire clairement que vous devriez stopper là votre investigation. Et donc c'est aussi évidemment pour pouvoir discréditer publiquement le ou la journaliste ensuite* ».
>
> **Laurent Richard, extrait de la formation « Sécurité numérique des journalistes ».**

Au moins une trentaine de pays dans le monde auraient ainsi mis en place des armées de trolls, des commentateurs payés par les autorités pour faire taire la dissidence en ligne[37]. Pegasus doit ainsi se comprendre comme une seule goutte d'eau dans l'océan des technologies de surveillance où l'on compte plus de 65 entreprises privées[38].

[36] Reporters Sans Frontières, « Censure et surveillance des journalistes : un business sans scrupules », 2017.
[37] Freedom House, rapport "Freedom of the Net" avec l'Université d'Oxford, 2017.
[38] Laurent Richard, formation en « Sécurité numérique des journalistes », le 16 mars 2023.

B. La surveillance des journalistes s'inscrit dans un champ controversé : comment définir le concept surveillance à l'aune des progrès du numérique ?

La notion de surveillance est progressivement devenue un objet théorique autonome issu de travaux pionniers et de rencontres interdisciplinaires. Pour le cerner, nous pouvons retenir trois leçons préliminaires d'Olivier Aïm permettant d'appréhender la notion de surveillance[39]. La première, que la surveillance se déploie dans des « agencements » ; puis, que la surveillance touche toujours à un moment donné le corps des individus, y compris via des dispositifs numériques ; enfin, que la surveillance tend vers un fonctionnement quadrillé et stratifié, puisque c'est la diversité de la population qui est son objectif référentiel. Michel Foucault, dans *Surveiller et Punir*, pose les bases du champ des théories surveillancielles[40] : pour lui, la surveillance est une action permettant de discipliner les corps de manière systémique, permis par le passage d'une souveraineté monarchique à une souveraineté bureaucratique. Gilles Deleuze propose toutefois une nouvelle lecture de Michel Foucault dans les années 1980[41]. Il met en effet en question l'enjeu de l'enfermement et affirme que le temps disciplinaire est passé, précisément parce que la surveillance est sortie de ses confinements stricts, au profit de la logique ouverte et continue du « contrôle ». De ce fait, la surveillance des individus, parce qu'elle est exponentielle, devient pour le champ des *surveillance studies* un objet en soi.

Cependant, la surveillance apparaît comme étroitement liée à la question de l'Etat. La surveillance est en effet fortement corrélée à des questionnements politiques de natures diverses : la déviance, la pénalité, la prison, le contrôle social, les normes, le travail policier, l'identification des populations, le fichage des individus, les discriminations, la gouvernance des villes, l'espace public, la vie privée… Comme le montre Anthony Giddens, la surveillance doit se penser comme un outil favorisant la construction de l'Etat Nation[42]. Dans son analyse de la construction de l'Etat Nation, il considère que le pouvoir est devenu administratif, reposant sur la collecte de données sur les individus. Déterminée par le principe de contrôle, l'information constitue l'une des clefs de compréhension de l'émergence de ce modèle politique. La gestion informationnelle de la population met au centre de son activité la surveillance pratique de pouvoir. Il définit à ce titre dans *The Nation-State and Violence*, publié en 1985, la surveillance comme principal outil de l'Etat Nation pour gouverner la population

[39] Aïm Olivier, *Les théories de la surveillance. Du panoptique aux Surveillance Studies*, Armand Colin, 2020.
[40] Foucault Michel, *Surveiller et punir : Naissance de la prison*, éditions Gallimard, 1975.
[41] Deleuze Gilles, *Foucault*, 1986.
[42] Giddens Anthony, *The Nation-State, and Violence,* 1985.

en tant que « mobilisation du pouvoir administratif »[43]. La surveillance apparaît ici comme l'effet des pratiques de rationalisation dans son sens wébérien. Pour Anthony Giddens, de même que pour Gilles Deleuze, la surveillance tient ainsi non pas de la discipline, mais du contrôle. Une chose est sûre, elle est un moyen de pouvoir.

C'est dans cet objectif de dévoiler la caractère éminemment politique de la surveillance que les précurseurs des *surveillance studies* ont tenté d'éclairer les citoyens sur ces menaces. Mais quel bilan peut-on en tirer ? Ce champ se structure autour de l'émergence d'une « nouvelle surveillance » indexée aux nouvelles technologies et au processus d'« informatisation » des sociétés modernes, nous dit Olivier Aïm[44]. Pourtant, selon Florent Castagnino, trois grandes tensions traversent encore les *surveillance studies*[45]. La première, celle d'une aporie définitionnelle : la surveillance se trouve en effet dans une position ambivalente, entre vouloir lui conférer un caractère banal et universel ou bien politique et social spécifique, qui serait constitutif des sociétés contemporaines. La deuxième, que les études sur la surveillance sont enfermées dans une vision normative qui s'attache à étudier quasi exclusivement ses effets négatifs. La troisième, que le rapport à la technique est entendu de sorte à concevoir la surveillance comme un phénomène politique dangereux en soi parce que technologique. Face à ces débats, Elodie Vialle, alerte ainsi sur la technophobie des recherches sur la surveillance :

> *« Il y a en effet une technophobie due à une méconnaissance (…) de tout ce qu'on met derrière surveillance, et il faut bien la définir. Aujourd'hui il y a tout un pan de techniques de surveillance numérique qui passent sous notre radar ».*
>
> **Extrait d'entretien avec Elodie Vialle, le 9 janvier 2023.**

En tant que journalistes, chercheurs, il reste encore à intégrer à nos recherches sur la surveillance la dimension profondément numérique qui imprègne la surveillance contemporaine. La surveillance des journalistes s'inscrit effectivement au sein d'une « surveillisation des sociétés »[46], mais elle est le plus souvent un effet et non un objectif, un effet politique qui ne peut pas se détacher de la question de l'Etat. Toutefois, à mesure qu'internet s'impose, il convient de rapprocher les études de la surveillance avec les études de l'information afin de mieux cerner la surveillance des journalistes à l'ère du numérique.

[43] Giddens Anthony, *The Nation-State, and Violence,* 1985.
[44] Aïm Olivier, *Les théories de la surveillance. Du panoptique aux Surveillance Studies*, Armand Colin, 2020.
[45] Castagnino Florent, *Critique des surveillances studies. Éléments pour une sociologie de la surveillance*, Déviance et Société, 2018.
[46] Castagnino Florent, *Critique des surveillances studies. Éléments pour une sociologie de la surveillance*, Déviance et Société, 2018.

C. La surveillance des journalistes s'inscrit dans une économie nouvelle : le capitalisme numérique, un lourd danger pour la liberté de la presse

Nous évoluons dans un âge nouveau, nous dit Shoshana Zuboff, l'âge du capitalisme de surveillance : un âge où nos démocraties sont en dangers. Le premier travail à faire, nous dit Zuboff, « doit être de nommer les choses »[47] car selon elle, l'un des plus grands freins à la prise de conscience massive des dangers que constitue cette ère numérique tient de l'édifiante asymétrie de savoir qui se traduit en asymétrie de pouvoir. En effet, elle revendique en quoi ce capitalisme nouveau constitue une menace pour nos démocraties : une société où les individus sont surveillés à chaque instant est une société qui pousse à la conformité, à l'obéissance et à la destruction progressive de l'esprit critique et de la capacité à s'indigner.

Selon Jérôme Valluy, il faut aussi comprendre le « sans précédent » du capitalisme de surveillance décrit par Shoshana Zuboff comme un objet à part entière qui vient ébranler les interprétations classiques de la surveillance[48]. Selon lui, la croissance des notions « capitalisme informationnel », « capitalisme numérique », « capitalisme cognitif », « capitalisme de plateforme », « capitalisme de surveillance », etc. est la marque même que nous évoluons au sein d'un champ théorique peu stable. Il y aurait quatre manières d'interpréter cette prolifération conceptuelle[49] : elle pourrait être liée à « l'instabilité des structures capitalistes dans une période transitionnelle » ; au caractère sans précédent du capitalisme numérique où 5 milliards d'individus sur 8 sont connectés en 2022 ; à des divergences « éthico-politiques » ; ou encore à un embarras culturel face à la défense de la vie privée, droit très récent dans l'histoire. Une chose est sûre, il est encore à ce jour impossible d'évaluer l'amplitude de l'économie de surveillance qui se développe chaque jour un peu plus dans le monde.

Au sein de cet âge nouveau et incertain, la liberté de la presse figure parmi les premières victimes de cette ère nouvelle[50]. Son ouvrage apporte plusieurs éclairages quant aux contextes de surveillance dans lesquels s'inscrit la pratique journalistique contemporaine. Tout d'abord, Shoshana Zuboff explique comment les médias, tout autant – voire plus – que les individus, sont désormais confrontés à la surveillance et à la collecte de données à grande échelle de la part d'entreprises de technologies, communément les GAFAM (Google, Facebook, Twitter…). Laurent Richard explique à ce titre :

---

[47] Zuboff Shoshana, *L'âge du capitalisme de surveillance*, éditions Zulma, 2018.
[48] Valluy Jérôme, « Sur 'L'âge du capitalisme de surveillance' de Shoshana Zuboff et sa difficile réception ».
[49] Valluy Jérôme, « Sur 'L'âge du capitalisme de surveillance' de Shoshana Zuboff et sa difficile réception ».
[50] Zuboff Shoshana, *L'âge du capitalisme de surveillance*, éditions Zulma, 2018.

« Je pense que c'est quelque chose qu'on doit vraiment prendre en considération, nous journalistes mais aussi évidemment pour tous les citoyens c'est que souvent, depuis 10 ans, 15 ans on a un peu abandonné cette idée-là en se disant, je vais sur Facebook j'accepte de donner une partie de mes datas à Facebook, à WhatsApp, je vais chez Carrefour, j'ai une carte de fidélité j'accepte de donner un peu mes datas. On a abandonné petit à petit et on s'est fait un peu à cette idée-là de 'je suis un peu surveillé et je vois pas comment lutter contre ça'. Et du coup s'il y a aussi peu de préoccupations, je pense, du législateur sur comment faire en sorte pour que nos citoyens puissent réagir, puissent être protégés contre ce type d'attaques, c'est parce qu'on a pas conscience de la déflagration que c'est que d'être une victime de cybersurveillance ».

Laurent Richard, extrait de la formation « Sécurité numérique des journalistes ».

Laurent Richard fait ici écho à Zuboff qui évoque également en quoi les médias ont eux-mêmes été impliqués dans la collecte de données à grande échelle ainsi que dans la surveillance de ses utilisateurs, en particulier dans le cadre de la publicité ciblée – élément représentatif de la naissance du capitalisme de surveillance. En effet, les entreprises de médias peuvent collecter des données sur les habitudes de consommation des utilisateurs et les vendre à des annonceurs, compromettant de fait la confidentialité des informations personnelles des utilisateurs. Le danger réside dans ce que Laurent Richard décrit par de la désinformation à grande échelle :

« On a enquêté sur une entreprise israélienne qui se faisait appeler Team Jorge qui pratique la désinformation à grande échelle, qui prétend être derrière la manipulation de 33 élections présidentielles dirigée par un homme qui se faisait appeler Jorge et qui était en fait un ancien sous-traitant de Cambridge Analytica, que vous connaissez je suis sûr, qui était donc une entreprise impliquée dans la désinformation autour du Brexit ou sur la campagne américaine de 2016. Aujourd'hui on est face à une industrie qui a un nouveau visage et qui peut comme on l'a vu dans l'enquête Story Killers proposer à un client qui est prêt à payer 6 ou 15 millions d'euros d'aller déstabiliser une campagne présidentielle pour aller discréditer une ONG en se servant d'un journaliste qui va relayer ce propos et qui est un propos mensonger. Mais tout ça fait partie d'un vaste ensemble de services où on peut harceler en ligne un journaliste qu'on veut discréditer, ou le hacker pour désinformer globalement l'opinion publique et puis pour servir les intérêts de celui qui va payer très cher ces solutions-là ».

Laurent Richard, extrait de la formation « Sécurité numérique des journalistes ».

Ici Laurent Richard permet de voir en quoi la désinformation de masse transforme l'influence des journalistes sur les réseaux et sur l'opinion publique en arme et dont l'impact est amplifié par le poids croissant des plateformes. Cette surveillance, qui favorise les logiques d'intimidation ou de hacking, constitue une lourde menace pour l'indépendance des journalistes et pour la liberté de la presse mais rappelle aussi en quoi la protection de la vie privée des journalistes est essentielle pour garantir le droit des citoyens à une information libre.

De manière parallèle, Guilhem Giraud nous explique, dans son ouvrage *Confidences d'un agent du renseignement français*, comment la surveillance des journalistes est devenue une pratique courante chez les agences de renseignements[51]. Lui-même ancien agent de renseignement, il y développe les différentes techniques utilisées pour collecter des informations, y compris la surveillance des communications électroniques et la collecte des données. Ces informations sont cruciales pour comprendre les techniques de surveillance les plus couramment employées par les gouvernements et services de renseignements pour surveiller les journalistes. Aussi, bien que le livre ne parle pas directement du logiciel espion Pegasus, Guilhem Giraud détaille le début des activités de la société israélienne NSO. Il nous apporte un témoignage en interne levant le voile sur la manière dont les sociétés de technologies comme NSO opèrent et comment elles vendent leurs technologies de surveillance numérique toujours plus sophistiquées à des gouvernements. Il mentionne notamment des pays comme la Chine, la Russie, l'Iran, l'Arabie Saoudite qui ont pour habitude de surveiller de manière agressive leurs journalistes et défenseurs des droits de l'Homme. Cependant, il souligne également que de nombreux gouvernements d'autres pays, y compris en Europe et en France, utilisent aussi des technologies de surveillance numérique sur les journalistes. Cette surveillance, de manière identique à celle décrite par Zuboff, constitue une atteinte très lourde à la liberté de la presse.

Ainsi, si les journalistes sont au centre de nouveaux enjeux à la fois économiques et politiques et se retrouvent parmi les premières cibles de la surveillance, ils ne le sont pas par hasard. Les journalistes occupent en effet un rôle qui, au centre de deux phénomènes que l'on observe en parallèle – la croissance de la surveillance et du numérique – les surexposent aux dangers qu'elles impliquent. Mais pourquoi ?

[51] Giraud Guilhem, *Confidences d'un agent du renseignement français*, éditions Robert Laffont, 2022.

II.

II. Les raisons de la surexposition des journalistes à la surveillance et aux attaques en ligne : une dépendance structurelle au numérique, virale et à position stratégique

Dans cette partie, nous verrons que les journalistes sont surexposés en raison : de leur dépendance au numérique (A) ; d'une surveillance devenue banalisée et virale (C) ; de leur rôle stratégique dans la société (C).

A. La surexposition des journalistes : la conséquence d'une dépendance au numérique

Depuis le tournant digital des années 2000, les journalistes ont développé une dépendance structurelle au numérique : en 2019, on considère que Google, Facebook et Twitter constituent à eux seuls la source de plus de 85% du trafic des principaux sites de presse aux Etats-Unis[52]. Cette dépendance les surexposent sur les plateformes médiatiques et conduit à les rendre, en tendance, plus vulnérables aux attaques en ligne.

Cette surexposition aux dangers du numérique doit se comprendre comme le revers d'une évolution structurelle de la pratique journalistique, à savoir la « plateformisation des médias »[53]. En effet, les plateformes jouent désormais un rôle crucial : elles reconfigurent la production, la distribution et la valorisation du contenu. Si leur point commun est de « traiter » le contenu sans le produire[54], les journalistes doivent nécessairement concilier avec les règles algorithmiques qui jouent un rôle que l'on pourrait qualifier de « méta-éditorial »[55] en ce qu'elles régissent l'accès et la diffusion de l'information d'actualité. Gardons-nous d'une clarification : les plateformes ne remplacent pas les journalistes mais elles travaillent en complément, chargées non pas de publier mais de publiciser les contenus. Toutefois, une chose apparaît certaine, elles ont acquis un rôle important dans l'accès à l'information et qui leur confère un poids édifiant sur l'impact escompté de l'information. Cette dépendance forte aux plateformes et où la marge de négociation est très faible, conduit à considérer que l'écosystème de l'information s'intègre, voire se dilue dans l'industrie d'internet. De cette manière, il semble que la mission des journalistes n'est plus uniquement d'écrire mais de plus en plus, comme l'exprime Johanna Siméant, « d'écrire pour être lus »[56].

[52] Sebbah Brigitte, Sire Guillaume, Smyrnaios Nikos, « Journalisme et plateformes : de la symbiose à la dépendance », *Sur le journalisme,* Vol 9, n°1, le 15 juin 2020.
[53] Tow Center for digital journalism, "Hybrid media systems and digital platforms", 2021.
[54] Sebbah Brigitte, Sire Guillaume, Smyrnaios Nikos, « Journalisme et plateformes : de la symbiose à la dépendance », *Sur le journalisme,* Vol 9, n°1, le 15 juin 2020.
[55] Ibid.
[56] Ibid.

De plus, il faut comprendre que cette dépendance provoque une présence accrue des journalistes sur les plateformes, illustrée par l'émergence et la stabilisation du format *live.* Apparu en France sur Le Monde fin 2009[57], le format du *live* s'impose comme un format incontournable de suivi de l'actualité. Il est toutefois plus complexe qu'en apparence et s'appuie sur quatre fonctionnalités de l'information numérique : l'hypertextualité, le multimédia, l'interactivité et l'immédiateté[58]. La participation du public, pilier du format, fait du *live* un moment de « partage et d'émotion »[59] avec les internautes.

Une particularité de ce format *live*, comme l'essor d'autres techniques de direct, il participe d'une personnification croissante des contenus qui provoque de nombreux dangers pour les journalistes alors surexposés en ligne. Elodie Vialle, alerte à ce sujet :

> *« Pour ce qui est de la croissance du numérique, il y a une sorte de retour de bâton de l'utilisation des réseaux sociaux par les journalistes ».*
>
> **Extrait d'entretien avec Elodie Vialle, le 9 janvier 2023.**

En effet, cette exposition des journalistes en tant qu'individus tend à associer de manière plus étroite l'information à l'image de son auteur et peut compromettre leur vie privée et leur intégrité. Selon le rapport du Comité de Protection des journalistes, un quart des journalistes assassinés dans le monde étaient déjà attaqués en ligne[60], avec dès les premières attaques de lourdes conséquences sur leur santé mentale et sur la censure de l'information. Le harcèlement en ligne est d'autant plus dangereux qu'il ne doit pas être compris comme une pure attaque envers le corps numérique. En effet, aujourd'hui nos corps virtuels se donnent de plus en plus à voir, quelle que soit leur utilisation, et notre identité digitale ne participe pas uniquement à la construction de notre identité numérique mais bien à la représentation de notre corps physique[61]. Les attaques digitales envers les journalistes, dont la présence en ligne augmente, doivent ainsi s'entendre comme des attaques physiques : sécurité numérique et sécurité physique apparaissent alors comme deux expressions dont la sémantique leur accorde plus de distance que ce qu'elles ne partagent empiriquement.

[57] Bonfils Philippe, « Environnements immersifs : spectacle, avatars et corps virtuel, entre addiction et dialectique sociales », éditions CNRS, dans « Hermès, la revue », 2012.
[58] Bonfils Philippe, « Environnements immersifs : spectacle, avatars et corps virtuel, entre addiction et dialectique sociales », éditions CNRS, dans « Hermès, la revue », 2012.
[59] Ibid.
[60] Laurent Richard, formation en « Sécurité numérique des journalistes », le 16 mars 2023.
[61] Bonfils Philippe, « Environnements immersifs : spectacle, avatars et corps virtuel, entre addiction et dialectique sociales », éditions CNRS, dans « Hermès, la revue », 2012.

Par ailleurs, pour harceler, cyber-attaquer ou surveiller un journaliste, les techniques sont nombreuses. En effet, on comprend de plus en plus que l'une des manières de détenir le pouvoir passe par le contrôle de l'information, et donc des réseaux sociaux. Et une technique de désinformation peut dès lors consister à aller harceler en ligne les sources fiables de l'information que sont les journalistes. Cela peut se traduire de manière très spontanée : on n'a pas aimé un contenu ou quelqu'un, on publie un commentaire mauvais, voire haineux. Cependant, cela peut aussi se traduire de manière très organisée : des armées de *trolls* mises en place par des gouvernements ou des groupes politiques pour harceler les journalistes de manière massive et systémique. Reporters Sans Frontières enquêtait en 2018 sur ces nouvelles techniques de harcèlement via les réseaux sociaux qui menacent les journalistes[62]. C'est le cas des « gangs de trolls » au Mexique dont les campagnes de désinformation cherchent à favoriser ou décrédibiliser des candidats politiques. C'est le cas des « Yoddhas » en Inde qui, engagés par le pouvoir, menacent et font taire toute opposition, incluant les journalistes.

> *« Il y a plusieurs types de cyberharcèlement, mais dans certains cas on est dans une technique de guerre de l'information avec la conséquence pour la liberté de la presse qui est que les journalistes se retirent des espaces numériques ».*
>
> **Extrait d'entretien avec Elodie Vialle, le 9 janvier 2023.**

Les conséquences sont d'abord d'ordre psychologique et poussent à la déconnexion temporaire, voire à l'autocensure et incitent les journalistes à éviter des sujets sensibles. Si certaines attaques sont le fruit de communautés d'individus et de groupes non-étatiques, elles peuvent ainsi également être organisées au plus haut niveau par des régimes soucieux de propager sur le Web leur modèle répressif. Au moins une trentaine de pays dans le monde auraient ainsi mis en place des armées de trolls[63], à savoir des commentateurs payés par les autorités pour faire taire la dissidence en ligne. Comme l'exprime Elodie Vialle, la conséquence est que les journalistes se « retirent des espaces numériques », voire se censurent. Selon une étude publiée par le Conseil de l'Europe en avril 2017[64], 31 % des journalistes atténuent la couverture des sujets après avoir été harcelés, 15 % les abandonnent, 23 % ne diffusent pas certaines infos, et 57 %... ne dénoncent même pas ces violences. Laurent Richard alerte à ce sujet :

[62] Reporters Sans Frontières, « Harcèlement en ligne des journalistes. Quand les trolls lancent l'assaut », 2018.
[63] Reporters Sans Frontières, « Harcèlement en ligne des journalistes. Quand les trolls lancent l'assaut », 2018.
[64] Conseil de l'Europe, rapport sur la sécurité des journalistes, avril 2017.

« Quand on est hacké c'est des personnes qui à priori vous veulent du mal, viennent de récupérer des informations et un jour vont les utiliser contre vous. Et quand vous êtes un dissident marocain, quand vous avez fui le baril, quand vous êtes la fiancée d'un journaliste saoudien qui écrit dans le Washington Post, c'est un cauchemar qui commence et qui va pas s'arrêter ».

Laurent Richard, extrait de la formation « Sécurité numérique des journalistes ».

Ainsi, il est possible de comprendre les dangers du numérique auxquels, en tendance, font face les journalistes comme le fruit d'une addiction sociologique au numérique. Entendue comme la vision d'Eric Loonis, l'addiction ici à l'œuvre se traduit, du fait du revers de la plateformisation de l'info, par une « menace existentielle »[65] pour la presse.

B. La surexposition des journalistes : la surveillance des reporters, un phénomène banal, viral et peu couteux

La surveillance des journalistes est devenue une pratique presque banale et peu couteuse. Elle existe dans de nombreux pays, y compris en Europe et en France, nous dit Guilhem Giraud[66]. Selon lui, la surveillance numérique est en effet une pratique courante dans de nombreux services de renseignement français. Si la France était à l'été 2021 sur le point de contracter elle-même avec la société NSO[67], il nous laisse à voir que Pegasus n'est qu'un outil de surveillance parmi tant d'autres. Phineas Rueckert explique de même :

« Pegasus c'est la technologie de surveillance la plus poussée, mais en fait c'est un outil qui affecte très peu de monde. Ce que je veux dire c'est qu'il y a tout un arsenal de menaces contre les journalistes ».

Extrait d'entretien avec Phineas Rueckert, le 11 janvier 2023.

En effet, Guilhem Giraud confirme en interne que pour un gouvernement, la dépendance croissante des journalistes au numérique permet d'augmenter l'arsenal des moyens de surveillance : surveillance des communications, des réseaux sociaux, utilisation de logiciels espions, espionnage électronique…La dimension digitale, s'agissant de la surveillance, vient ainsi frapper d'autant plus fort les journalistes qui reposent de plus en plus dans leur travail sur des outils numériques et sur des réseaux sociaux.

[65] Collard Victor, « L'addiction au prisme de la perspective sociologique », Introduction, EHESS, 2017.
[66] Giraud Guilhem, *Confidences d'un agent du renseignement français*, éditions Robert Laffont, 2022.
[67] France Info, « Pegasus : le gouvernement et toute la classe politique française dans le viseur du Maroc », Elodie Guéguen, le 20 juillet 2021.

Cette dimension digitale de la surveillance et attaques des journalistes doit alors se comprendre comme un phénomène amplifié par la viralité du web[68]. En effet, les conséquences du harcèlement en ligne sont d'autant plus dramatiques que les nouvelles technologies amplifient les messages de haine ; que l'intelligence artificielle peut être utilisée à des fins malveillantes ; que la censure est automatisée via des bots ; que les fausses informations diffusées par des robots peuvent être relayées par des activistes influents…La stratégie reste identique : désinformer, amplifier, intimider. En 2017, déjà 40 % de la population mondiale était présente sur les réseaux sociaux[69] et 94% des journalistes les utilisaient pour promouvoir leur contenu[70]. Les réseaux sociaux apparaissent ainsi comme un outil à la fois incontournable pour l'accès aux contenus journalistiques mais offrant en revanche une caisse de résonnance édifiante et inédite, que tout ennemi de la liberté de la presse peut exploiter.

C'est pourquoi Phineas Rueckert raconte que Pegasus nourrit des menaces déjà existantes et qu'elles vont ainsi encore plus loin :

> *« En dépit de notre enquête, de toutes les informations disponibles sur ces outils-là, on va toujours pouvoir arrêter des journalistes qui gênent ».*
>
> **Extrait d'entretien avec Phineas Rueckert, le 11 janvier 2023.**

La surveillance et les attaques en ligne constituent à tout point de vue, une pratique peu couteuse. D'un point de vue politique, les gouvernements s'octroient le droit de surveiller les journalistes dans le cadre de la protection des intérêts nationaux, explique Guilhem Giraud[71]. D'un point de vue économique, harceler en ligne coûte de moins en moins cher avec l'essor permanent de l'industrie de surveillance digitale[72] et des techniques de « e-mail bombing », d' « astroturfing », de retweets par milliers…Elodie Vialle résume ainsi :

> *« Ça coute moins cher de cyberharceler un journaliste que de le mettre en prison… ».*
>
> **Extrait d'entretien avec Elodie Vialle, le 9 janvier 2023.**

Très élégamment décrit, Elodie Vialle permet de rappeler le rouage souvent à l'œuvre : faire taire l'information, harceler pour peu cher un journaliste en ligne, discréditer publiquement son image et travailler ainsi l'acceptation politique de son départ forcé, voire de son arrestation.

---

[68] Reporters Sans Frontières, « Harcèlement en ligne des journalistes. Quand les trolls lancent l'assaut », 2018.
[69] Reporters Sans Frontières, « Harcèlement en ligne des journalistes. Quand les trolls lancent l'assaut », 2018.
[70] Cision, enquête menée sur l'usage des réseaux sociaux chez les journalistes, 2017.
[71] Giraud Guilhem, *Confidences d'un agent du renseignement français*, éditions Robert Laffont, 2022.
[72] Reporters Sans Frontières, « Harcèlement en ligne des journalistes. Quand les trolls lancent l'assaut », 2018.

Si la surveillance et la harcèlement des journalistes apparaît comme monnaie courante pour tout gouvernement souhaitant contrôler ou faire taire l'information, il convient de s'intéresser plus en détail au rôle stratégique qu'occupent les journalistes dans une société et qui les surexposent à la surveillance et aux attaques.

C. La surexposition des journalistes : les reporters, entre cibles directes, conséquences et moyens de surveillance de la population

La surveillance des journalistes est-elle un objectif en soi ? Si l'on pense la surveillance comme un phénomène global, alors la surveillance des reporters est comprise plus largement au sein d'une tendance à la sécurisation des sociétés.

Comme l'exprime Olivier Aïm, on observe une double focale sur l'identification des individus et la gestion des circulations des territoires[73]. Cette société de sécurité qui prend forme au XIXe selon Michel Foucault[74] répond à la visée d'un contrôle social croissant et qui glisse rapidement vers une « obsession sécuritaire ». Toutefois, selon l'observation qu'en fait Giorgio Agamben, les « dispositifs de sécurité » décrits par Gilles Deleuze[75], se sont vite mués en « technologies de contrôle »[76]. En ce sens, Agamben décrit deux tendances parallèles[77]. La première, l'extension du champ signalétique avec : une extension des pratiques d'identification à la totalité de la population – tout le monde devient suspect à priori ; une extension des pratiques de localisation à la totalité de l'espace public et privé – caméras de surveillance et empreintes digitales d'abord conçues pour les prisons puis étendues partout ; enfin, une extension numérique des techniques – avec un espace politique de plus en plus réduit à sa dimension policière. La deuxième, le réductionnisme biologique qui normalise la surveillance, comme illustré par l'Etat d'urgence et le plan Vigipirate en France en 2015 ou bien par les dispositifs sanitaires exceptionnels lors de la pandémie de COVID-19. Dès lors que l'exception est la norme, la surveillance des journalistes peut se définir plus largement comme la conséquence d'une surveillisation de la population.

De plus, les journalistes sont également surveillés car ils occupent une place stratégique dans la société : ils sont le premier relai des sources de l'information. En effet, que les services

[73] Aïm Olivier, *Les théories de la surveillance. Du panoptique aux Surveillance Studies*, Armand Colin, 2020.
[74] Foucault Michel, *Surveiller et punir : Naissance de la prison*, éditions Gallimard, 1975.
[75] Deleuze Gilles, *Foucault*, 1986.
[76] Agamben Giorgio, *Qu'est-ce qu'un dispositif ?*, éditions Payot & Rivages, 2014.
[77] Aïm Olivier, *Les théories de la surveillance. Du panoptique aux Surveillance Studies*, Armand Colin, 2020.

de renseignements aient pris pour habitude de surveiller les journalistes, comme décrit par Guilhem Giraud[78], n'est pas un hasard. À ce titre, Elodie Vialle exprime :

> *« Les sources c'est comme un filet de pêche que vous allez lancer. Et un journaliste c'est ça, tu relèves le filet de pêche et t'as tous les poissons qui tombent. Donc effectivement dans un système de surveillance, c'est un point qui va donner accès à tous les autres ».*
>
> **Extrait d'entretien avec Elodie Vialle, le 9 janvier 2023.**

En effet, notamment dans le cadre de la lutte contre le terrorisme, il est communément considéré que les journalistes seront potentiellement en contact avec des terroristes présumés ou des groupes extrémistes dans le cadre de leur travail d'enquête. A l'inverse, les journalistes peuvent en retour être la cible directe de terroristes en raison de leur profession ou de leur couverture médiatique de certains sujets. En surveillant les journalistes, les autorités espèrent recueillir des informations sur des activités suspectes pouvant menacer la sécurité nationale.

> *« Le journaliste il a tissé un filet et souvent, avec des activistes, avec des opposants d'un régime, donc y'a qu'à tirer le filet pour choper toutes les infos, les contacts ».*
>
> **Extrait d'entretien avec Elodie Vialle, le 9 janvier 2023.**

Au-delà d'un enjeu exclusivement sécuritaire, les journalistes occupent une position centrale en ce qu'ils peuvent être les porte-parole de minorités – politique, ethnique, religieuse, sexuelle, – réelles ou perçues. Pour tout Etat souhaitant faire taire toute dissidence, surveiller les journalistes peut conduire à connaître la position des opposants. À ce titre, Laurent Richard explique :

> « *En général, si on est surveillés, c'est d'ailleurs pas souvent directement pour nous-mêmes, mais c'est d'abord pour savoir qui nous parle, quelles sont nos sources. Ça, on a pu le vérifier plein de fois dans plein d'enquêtes, les journalistes sont surveillés parce que des services de renseignement veulent savoir qui est à l'origine de la fuite d'information. Parce qu'ils vont sans doute la plupart du temps, surtout dans les démocraties, avoir du mal à menacer un journaliste. Ils pourront le faire de manière légale, judiciaire, après la publication. Mais par contre, il est beaucoup plus simple et beaucoup plus discret finalement de menacer une*

[78] Giraud Guilhem, *Confidences d'un agent du renseignement français*, éditions Robert Laffont, 2022.

source. Donc souvent les services de renseignement nous surveillent et vont intercepter une communication pour savoir qui est en train de nous donner l'information, qui nous parle, et aussi pour en savoir plus sur l'enquête que l'on va publier ».

Laurent Richard, extrait de la formation « Sécurité numérique des journalistes ».

La surveillance des journalistes peut dès lors apparaître comme la conséquence d'une plus grande tendance, celle d'une surveillance croissante de la société. Mais avec cette position stratégique qu'ils occupent, étant le contact rapproché des sources, les journalistes mettent aussi en jeu la sécurité de ces-derniers :

« *Il faut qu'on se protège nous, mais il faut surtout qu'on protège les sources qui prennent le risque de nous contacter. Et il y a cette phase du premier contact qui est ultra dangereuse. C'est la première fois qu'une source va vous contacter pour vous livrer un document, parce qu'elle travaille dans une entreprise et qu'elle a accès à un document, et elle, sans trop vous connaître, en connaissant un peu votre réputation de journaliste, elle vous envoie un document. C'est très important d'être proactif là-dessus, et de faire savoir publiquement de quelle façon vous voulez être joint par des personnes que vous ne connaissez pas encore. Parce que si vous ne le faites pas, elles peuvent commettre des erreurs qui sont difficilement réparables. C'est-à-dire que si une source vous contacte depuis son ordinateur de travail sur votre email professionnel, il y a de fortes chances, si jamais ce qu'elle a fait relève d'un délit pénal ou criminel, qu'il y ait ensuite une investigation sur son ordinateur et que l'email soit retrouvé et que la personne soit incriminée pénalement à cause de ça. Se connecter, vous envoyer des documents sur une adresse mail qui est la vôtre, mais qui n'est pas totalement sécure, ou sur un numéro de téléphone que vous affichez, ou la personne va vous joindre par SMS ou sur un appel non chiffré…Tout ça peut être très dangereux* ».

Laurent Richard, extrait de la formation « Sécurité numérique des journalistes ».

Les journalistes se retrouvent dès lors au cœur d'une dynamique plus globale de société : les déplacements n'ont jamais été aussi libres et pourtant jamais autant contrôlés. Devant ainsi considérer la surveillance comme un système, la question de la protection des journalistes doit être pensée de manière indissociable avec la question de la sécurité des sources.

III.

III. Négocier la dépendance : les inégalités devant la surveillance et attaques en ligne des journalistes qui posent un enjeu de résignation et de régulation

Dans cette troisième partie, nous aborderons les éléments éclairant la surveillance contemporaine des journalistes : ses profils (A) ; sa résignation (B) ; son encadrement (C).

A. Redéfinir les profils de la surveillance : la surveillance et les attaques reposent et viennent renforcer des inégalités économiques, ethniques et de genre préexistantes

Les journalistes sont inégaux devant les dangers du numérique. Elodie Vialle, dont la profession même de chercheuse en sécurité numérique et liberté de la presse constitue un indicateur du danger croissant que posent la surveillance, nous alerte sur un enjeu de taille :

> *« C'est compliqué d'aborder ce sujet-là [la sécurité numérique] dans un contexte de crise économique des médias. Et je pense que c'est un élément que l'on ne doit absolument pas omettre. On est dans un contexte où les questions de sécurité sont intrinsèquement liées aux questions économiques et aux questions de précarité ».*
>
> **Extrait d'entretien avec Elodie Vialle, le 9 janvier 2023.**

Elodie Vialle dans cet extrait confirme la dimension, transversale à toute notre réflexion, de la question des inégalités devant les dangers de la surveillance. Penser le lien entre les questions de sécurité et de précarité tient de l'approche des « *People at risk* » en ce sens que les dangers du numérique relèvent, comme bien souvent, d'une question d'inégalités préexistantes. Dans un contexte donné, l'objet principal est de surveiller des minorités ethniques, religieuses, politiques, sexuelles, qui s'opposeraient de manière active ou silencieuse au régime en place…La surveillance et les attaques en ligne fonctionneraient ici comme des outils qui viendraient intensifier des discriminations préexistantes.

Appliqué au cas des journalistes, il faut ainsi faire l'exercice de penser les reporters comme une catégorie à risque. Les journalistes d'investigation, en exil et plus globalement, ceux qui sont isolés, viennent ici en premier lieu explique Laurent Richard :

> *« Dans un pays comme la Hongrie, les journalistes d'investigation c'est pas étonnant qu'ils soient ciblés. On a vu un grand nombre de journalistes qui étaient des journalistes en exil aussi, qui avaient fui un pays mais qui continuaient de travailler depuis l'étranger sur ce pays-là, comme Jamal Khashoggi. Les journalistes les plus menacés dans le monde sont*

toujours les plus isolés. Ceux qui sont au fin fond d'un État dans un pays et qui se retrouvent dans une situation qui est tellement dangereuse qu'il n'y a plus aucune rédaction qui les soutient et qui publient donc leurs informations sur leur page Facebook. Alors eux ce sont vraiment des cibles de premier choix pour des gouvernements centraux ou plus régionaux qui vont les cibler ».

Laurent Richard, extrait de la formation « Sécurité numérique des journalistes ».

À l'inverse, en France, ce risque pour les journalistes est issu d'une tendance dans le milieu journalistique à la précarisation de l'emploi, à l'augmentation des contrats courts, des statuts indépendants qui accordent de moins en moins de droits et de protections aux reporters[79]. À cette tendance vient s'ajouter la question, centrale pour tous les médias, des financements. Il en va de même dans le cas des ONGs spécialisés dans la défense des journalistes. Maxine Singeot, chargée de projet chez Reporters Sans Frontières, raconte :

« *On fait très peu de formations liées à la sécurité numérique. Avant on avait une conseillère à RSF qui s'occupait de ces questions-là et qui est partie en 2017 et depuis on est très nuls. Son poste n'existe plus et nos manuels de sécurité numérique datent d'il y a dix ans. L'assistance travaillait sur ces rapports mais ils sont pas du tout mis à jour et on est plus du tout spécialisés sur ces questions [...]. Et tous les autres groupes sont au même stade que nous en matière de sécurité digitale, c'est-à-dire pas très au courant de ce qui se passe et qui vont donc vite référer à des groupes comme Tech 4 Press. Et aussi par manque de fonds* ».

Extrait d'entretien avec Maxine Singeot, le 3 février 2023.

Fournir des services de sécurité numérique est couteux, et apparaît aussi de moins en moins comme une priorité pour les rédactions françaises qui désormais font appel de plus en plus à des journalistes en freelance qui partent en reportage à leur propre dépens, leur propre risque, afin de tenter de revendre leur article, leurs photos[80]…

En ce sens, les personnes qui font le plus face aux dangers du numérique sont les personnes les plus précaires, qui n'ont pas, ou peu, les moyens de se protéger. S'il est déjà difficile de mettre la lumière sur le besoin de formation des reporters en matière de sécurité

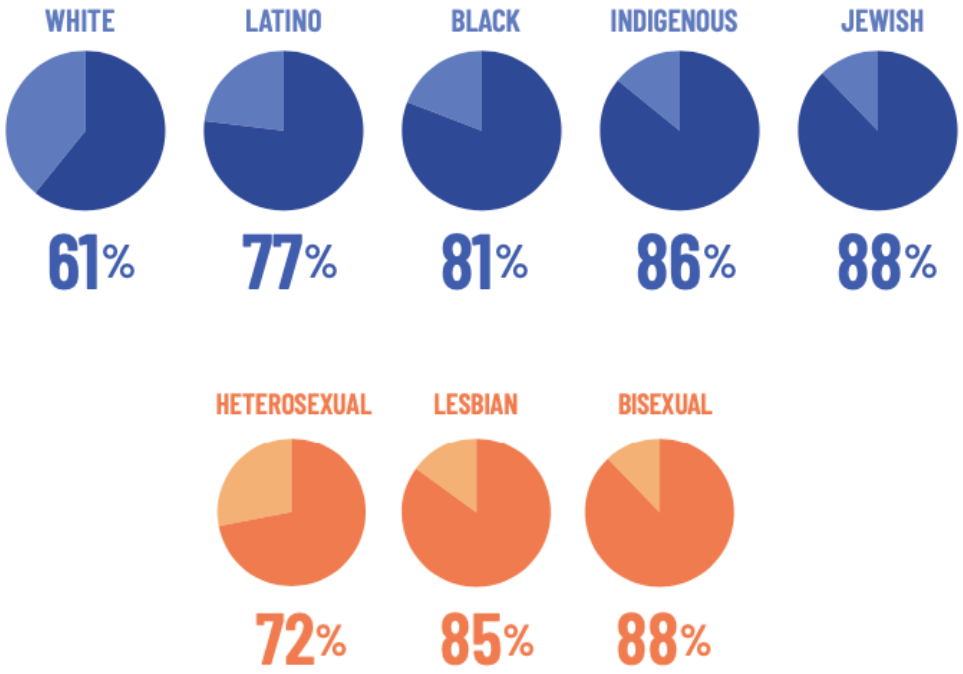
[79]Lyubareva Inna, Marty Emmanuel, « Vingt-cinq ans d'information en ligne : une exploration des transformations structurelles des médias », 2022.
[80]Lyubareva Inna, Marty Emmanuel, « Vingt-cinq ans d'information en ligne : une exploration des transformations structurelles des médias », 2022.

physique, Elodie Vialle, par son travail, rappelle la nécessité de penser l'imbrication nécessaire avec les enjeux de sécurité numérique. En effet, même à titre individuel, il y a une dimension économique importante : changer de téléphone régulièrement, avoir un téléphone spécifique pour le travail, adopter un VPN…Il existe une dimension onéreuse qui s'additionne au manque de formation et qui surexpose certains reporters, du fait de leur dépendance au numérique, aux dangers de ce-dernier.

> *« J'ai bossé avec pas mal de consœurs du continent africain et la première problématique c'est la précarité. Et c'est ce qui fait que la nana journaliste elle peut pas se protéger quand elle couvre certains sujets ou quand elle va lutter contre le harcèlement au sein d'une rédaction ».*
>
> **Extrait d'entretien avec Elodie Vialle, le 9 janvier 2023.**

Dans cette continuité, on observe également que les femmes reporters sont d'autant plus une catégorie à risque. Il existe, en effet, une variable de genre dans cette surexposition aux dangers du numérique. Selon le rapport de 2020 de IWMF[81], près de trois femmes journalistes sur quatre (73%) disent avoir déjà expérimenté de la violence en ligne, avec en première forme des menaces de violences physiques (25%) et sexuelles (18%). 41% des femmes disent être victimes de ces violences en ligne dans le cadre de campagnes orchestrées de désinformation. Encore une fois, ce rapport rappelle le manque de prise de conscience structurel des dangers du numérique : seules 25% des femmes abusées en ligne déclarent avoir reporté l'incident à leurs employeurs – soit les employeurs ne répondent pas (10%), soit ils invitent à s'endurcir (9%), soit ils demandent ce qu'elles ont fait pour provoquer cette attaque en ligne (2%). Autrement dit, ces chiffres rappellent également de manière cruciale les conséquences physiques des dangers en ligne : 20% des femmes disent avoir subi des violences physiques suite à des violences en ligne ; 26% déclarent un impact sur leur santé mentale ; 30% déclarent répondre à ces attaques par de l'autocensure. Il existe ainsi une approche intersectionnelle dans les logiques d'attaques numériques. Dans les cas des femmes reporters, elles apparaissent comme une catégorie doublement à risque.

[81] International Women's Media Foundation, survey on online harassment.



Incidence du harcèlement en ligne des femmes reporters[82].

Ce constat vient également nourrir l'hypothèse selon laquelle le harcèlement de genre se trouve à l'intersection de l'ethnie et de l'orientation sexuelle. Toute catégorie confondue, plus d'une femme reporter sur deux est victime de violences en ligne, une tendance qui reste bien plus élevée chez les femmes qui s'identifient comme latinos, noires, juives ou d'origine indigène, allant jusqu'à un écart de 27% entre les femmes blanches (61%) et les femmes juives (88%). Cet écart d'incidence se retrouve également du point de vue des orientations sexuelles : 88% des femmes reporters s'identifiant comme bisexuelles et 85% comme lesbiennes déclarent être victimes de violences en ligne, contre 72% des femmes se déclarant hétérosexuelles. C'est pourquoi il faut être capable, pour mesurer les dynamiques des dangers du numérique, de penser l'intersectionnalité des discriminations liées aux identités de genre, d'ethnie, d'orientation…De manière analogue à l'analyse de Danièle Kergoat dans *Le genre du monde*, on observe ici à la fois une forme de coextensivité entre les discriminations et les dangers de la surveillance qui s'entraînent mutuellement ainsi qu'une consubstantialité dans les rapports de dominations ici imbriqués. En ce sens, on ne peut que conclure d'une forme de reproduction sociale, et inégalitaire, des dangers du numérique chez les reporters.

[82] International Center for Journalists and UNESCO, "The Chilling: a global study of online violence against women journalists", 2020.

« Il faut donc toujours considérer le contexte dans lequel on s'inscrit, et on s'inscrit dans un contexte d'énorme pression politique, précarité économique pour les journalistes et qui va avoir des conséquences directes sur ce qu'on peut faire ou non en termes de sécurité ».

Extrait d'entretien avec Elodie Vialle, le 9 janvier 2023.

En outre, les dangers du numérique ne peuvent être pensés de manière individuelle car la précarité et la discrimination sont des faits sociaux qui s'observent collectivement dans une société. C'est ainsi qu'il faut opter pour une approche holistique des dangers du numérique chez les reporters. A l'image de sociologues comme Émile Durkheim, il faut penser l'explication sociale du risque, ou de Norbert Elias dans *La société des individus*, il faut penser l'objet « danger numérique » à travers les réseaux de dépendance et d'interdépendance dans lesquelles il s'inscrit. Les tendances individuelles des dangers subis par les reporters deviennent des variables dépendantes explicables par des variables macrosociales.

Les inégalités des reporters face aux dangers du numérique s'inscrivent donc dans un plus large contexte de discriminations politiques, de précarité économique et qui va avoir des conséquences physiques et directes en termes de sécurité. Ces éléments nous conduisent dès lors, à venir questionner le degré de résignation face à une société de surveillance autant établie : les journalistes peuvent-ils encore manœuvrer librement ?

B. Redéfinir l'acceptation de la surveillance : le double effet de la prise de conscience, une dépendance forte et souvent résignée

Dans un monde où les technologies de surveillance commerciales et politiques sont toujours plus poussées, est-il encore possible d'échapper à la surveillance ? Tout d'abord, il convient de mener une observation : la surveillance, dans tous ses aspects, est bien souvent acceptée et banalisée. Florent Castagnino analyse ainsi la surveillance contemporaine, décrivant notamment le caractère banal que prennent aujourd'hui les diverses formes de techniques d'enregistrement et de collectes des données dans la vie quotidienne[83]. Pour beaucoup, cette amélioration de l'efficacité des techniques de surveillance est considérée comme un facteur d'amélioration de la vie quotidienne. Individuellement, d'une part, le capitalisme de surveillance décrit par Shoshana Zuboff peut apporter une pratique de consommation

[83] Castagnino Florent, *Critique des surveillances studies. Éléments pour une sociologie de la surveillance*, Déviance et Société, 2018.

personnalisée[84] qui est pour beaucoup de ménages recherchée ; de l'autre, la surveillance des services de renseignements décrite par Guilhem Giraud peut apporter une sécurité supplémentaire et en partie acceptée :

> « *Aujourd'hui, le monde entier s'est habitué à deux décennies de surenchère sécuritaire, si bien que plus personne ne s'étonne quand des individus sont désignés comme terroristes*[85] »
>
> **Guilhem Giraud, dans *Confidences d'un agent du renseignement français*.**

Cependant, il convient d'entendre que ces logiques à l'œuvre peuvent être aussi être l'apparat de qui veut contrôler la population. C'est ainsi que décrit le philosophe Michaël Foessel[86] la prégnance et l'acceptation du motif même de la sécurité à travers le régime de la « vigilance » qui s'impose avec un double sens : l'État de vigilance globalisé désigne à la fois une réalité politique et une forme, sous-jacente, de subjectivation.

Malgré sa logique économique, voire politique, il existe une dimension volontaire de la surveillance qui met en péril la notion de vie privée. Dans la logique décrite par Shoshana Zuboff, la transaction est en partie consentie : l'apanage traditionnel « si c'est gratuit, c'est vous le produit » se comprend et s'accepte comme si l'exploitation des données constituait la nouvelle monnaie d'accès aux services[87]. Cette acceptation s'accompagne d'une forme d'apathie aux dangers de la surveillance. Bauman exprime ainsi son désarroi, observant la tendance à valoriser faiblement le droit à la vie privée, lui faisant conclure que nous évoluons peu à peu dans une société « exhibitionniste » [88], vers une société de transparence.

Ces dynamiques ont un lourd impact chez les journalistes eux-mêmes. Est-il réellement possible de concilier avec les règles « méta-éditoriales » imposées par les plateformes ? Est-il encore possible de se protéger des attaques numériques ? La journaliste d'investigation Paloma de Dinechin alerte :

> *« C'est un peu comme s'il y avait une résignation collective ».*
>
> **Extrait d'entretien avec Paloma de Dinechin, le 3 février 2023.**

[84] Zuboff Shoshana, *L'âge du capitalisme de surveillance*, éditions Zulma, 2018.
[85] Giraud Guilhem, *Confidences d'un agent du renseignement français*, p.60, éditions Robert Laffont, 2022.
[86] Fœssel Michaël, *Etat de vigilance. Critique de la banalité sécuritaire*, éditions Essais, 2010.
[87] Aïm Olivier, *Les théories de la surveillance. Du panoptique aux Surveillance Studies*, Armand Colin, 2020.
[88] France Culture, « Société liquide : retour sur la pensée de Zygmunt Bauman », le 13 janvier 2017.

La résignation à la surveillance est collective mais doit également se penser d'un point de vue contextuel. Dans un pays comme le Mexique, ou d'autres pays où la liberté de la presse n'est pas garantie, les journalistes et proches de journalistes sont habitués à être surveillés.

> *« Tu vois, en France, les gens qui ont appris qu'ils étaient visés par NSO, ils étaient totalement choqués, mais aussi parce que c'était un truc auquel ils étaient pas habitués. Au Mexique c'est chaque année qu'il y a une révélation sur l'espionnage ».*
>
> **Extrait d'entretien avec Paloma de Dinechin, le 3 février 2023.**

La résignation à la surveillance s'apparente ainsi à un contexte, car comme l'explique Paloma de Dinechin de ses investigations, au Mexique, même un logiciel espion aussi puissant que Pegasus, ne constitue en fin de compte, qu'un nouveau danger qui s'ajoute à une longue liste de menaces et dangers préexistants.

En France, la prise de conscience de la part des journalistes des dangers de la surveillance numérique relève elle d'une double logique. Elodie Vialle explique notamment en quoi on observe dès les formations en école un double discours :

> *« À la demande des rédactions, les journalistes sont poussés à parler sur les réseaux sociaux, donc toutes les nanas elles se font harceler et elles doivent gérer elles-mêmes cette merde. Et en même temps on leur fait des points sur la cybersécurité. Moi ce que je voudrais c'est qu'on allie ces deux conversations ensemble ».*
>
> **Extrait d'entretien avec Elodie Vialle, le 9 janvier 2023.**

C'est ainsi que la dépendance croissante du journalisme au numérique semble ne pas encore être suffisamment mise en relation avec les dangers qu'elle constitue en ce qu'elle surexpose les journalistes au harcèlement en ligne et aux dangers de la surveillance de leurs données. C'est pourquoi il faut comprendre la surveillance et le numérique de manière globale : un journaliste harcelé, c'est un journaliste surveillé, c'est un journaliste présent sur les réseaux sociaux. Les menaces vont de pair et face à des technologies toujours plus puissantes, la sensibilisation aux enjeux de sécurité des journalistes et de leurs sources doivent ainsi advenir le plus tôt possible.

C. Redéfinir l'encadrement de la surveillance : de la difficile mise en responsabilité des Etats à la négociation de la dépendance aux plateformes

Est-il possible d'encadrer la surveillance des journalistes et d'en limiter les dangers à une ère où la société, dans tous ses aspects, devient de plus en plus transparente ? Tout d'abord, il faut s'intéresser aux discours qui légitiment ces moyens de surveillance. Dans le cadre de la surveillance venant des services de renseignements, la dialectique est celle de justifier la surveillance au nom de la sécurité nationale, nous explique Guilhem Giraud[89]. En matière légale en France, il existe notamment deux lois encadrant la surveillance des journalistes. La première, du 10 juillet 1991, garantit le secret des correspondances émises par communications électroniques[90]. La seconde, du 4 janvier 2010, porte amendement à la loi du 29 juillet 1881 sur la liberté de la presse et garantit la protection de l'identité des sources des journalistes[91]. Cependant, dans la lutte contre le terrorisme, et depuis l'Etat d'urgence de 2015, la loi du 24 juillet 2015 autorise les services de renseignement de recueillir des données sur les journalistes s'ils sont suspectés de porter atteinte à la sécurité nationale[92].

Ces actions, devant être autorisées par une autorité judiciaire, et demeurant secret défense car pouvant compromettre la sécurité de l'Etat ou des personnes concernées, accordent ainsi une grande marge de manœuvre aux Etats souhaitant surveiller leurs journalistes, parfois de manière abusive. Ce fut notamment le cas en France lors de « L'affaire des fadettes du Monde » où en 2012, deux journalistes étaient mis sur écoute dans le cadre de l'enquête Bettencourt[93]. Dans le cadre du logiciel Pegasus, l'argument avancé par le groupe NSO est de permettre aux Etats de lutter plus efficacement contre la criminalité et le terrorisme[94]. S'agissant d'une entreprise privée dont l'exportation est régie par le Ministère de Défense israélien, la question de sa régulation en droit international pose de nombreuses questions, et surtout de nombreux défis diplomatiques. Amnesty International défend ainsi depuis plusieurs années un contrôle indépendant du secteur de la surveillance numérique ciblée permettant de garantir une transparence et empêcher les violations des droits humains[95].

[89] Giraud Guilhem, *Confidences d'un agent du renseignement français*, éditions Robert Laffont, 2022.
[90] Légifrance, loi du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques.
[91] Légifrance, loi du 4 janvier 2010 relative à la protection du secret des sources des journalistes.
[92] Giraud Guilhem, *Confidences d'un agent du renseignement français*, éditions Robert Laffont, 2022.
[93] Le Monde, « Les fadettes, le procureur et la liberté de la presse », le 18 janvier 2012.
[94] NSO GROUP, voire site internet.
[95] Amnesty International, « La partie immergée de l'iceberg », 2021.

Toutefois, faut-il encore pouvoir prouver la surveillance. Par exemple, dans le cas de l'enquête *Pegasus* coordonnée par Forbidden Stories, prouver l'existence du logiciel espion au sein des téléphones portables de journalistes et défenseurs des droits de l'Homme n'a pas été tâche facile. Phineas Rueckert résume :

> *« Pour faire simple, on a une liste de milliers de numéros, dont on a pas les noms. Ce qu'il faut faire c'est de trouver un moyen de matcher ces numéros à des gens ».*
>
> **Extrait d'entretien avec Phineas Rueckert, le 11 janvier 2023.**

D'une liste de 50 000 numéros de téléphones potentiellement surveillés dont ils ont eu l'accès, environ 10 000 ont pu être matchés, raconte-t-il : un journaliste par région enquête par données croisées dans des bases d'informations, dans des carnets de contacts de journalistes clefs, à identifier les clusters de personnes susceptibles d'être targetées…Ensuite, il était encore nécessaire de mener l'analyse forensique auprès du Security Lab d'Amnesty International, et là encore un obstacle : comment obtenir la confiance d'un journaliste allant jusqu'à lui demander d'accéder à son téléphone juste après lui avoir expliqué qu'il était potentiellement surveillé ?

> *« Ça a forcé des Etats non forcément concernés directement à réagir ».*
>
> **Extrait d'entretien avec Phineas Rueckert, le 11 janvier 2023.**

Pour Amnesty International, « la simple affirmation d'un intérêt potentiellement légitime n'est pas suffisante pour justifier des restrictions du droit à la vie privée » [96]. Mais en pratique, il n'existe pas de cadre global s'agissant de surveillance numérique ciblée et le large vide juridique existant permet aux Etats de faire fi des risques relatifs aux droits humains. Laurent Richard explique ici la dynamique à l'œuvre chez les législateurs :

> *« Il n'y a pas vraiment de législation pour protéger le citoyen. Et pour plusieurs raisons. La première, c'est que le législateur, je pense, n'a pas encore perçu la gravité des faits dont on parle. C'est ce que je disais tout à l'heure, être victime de cybersurveillance, c'est vraiment être victime d'une intrusion terrible. Et ce n'est pas seulement un drame personnel, c'est une vraie atteinte à la démocratie. Parce qu'en général, les personnes qui sont surveillées sont des personnes qui luttent pour défendre les systèmes démocratiques. Ensuite, il y a une hypocrisie aussi du législateur. C'est-à-dire qu'en France, nous, on a révélé le projet*

[96] Amnesty International, « La partie immergée de l'iceberg », 2021.

Pegasus, mais on s'est aussi rendu compte qu'en fait, la plupart des pays membres de l'Union européenne utilisent aussi Pegasus. Donc c'est aussi pour ça que les États membres de l'Union Européenne n'ont pas critiqué trop fort la société NSO Group ou questionné vraiment le sujet parce qu'ils étaient eux-mêmes clients »

Laurent Richard, extrait de la formation « Sécurité numérique des journalistes ».

Aussi, d'un point de vue de citoyen, le problème c'est de savoir contre qui une action peut être menée. À priori, on ne sait pas qu'on est victime. Si jamais on sait, alors on peut porter plainte, explique Laurent Richard. Porter plainte contre l'Etat ? Celui-ci va nier utiliser Pegasus, ou ce sera une information secret défense. Porter plainte contre le vendeur du téléphone soi-disant sûr ? Apple se retourne aujourd'hui de lui-même contre NSO Group. Porter plainte contre la société NSO Group ? Cela suppose de prendre un avocat et d'agir devant la justice israélienne et donc avec peu de chances de gagner.

En parallèle, Shoshana Zuboff invite à renforcer la régulation du capitalisme de surveillance qui selon elle a progressé sans barrière depuis les années 2000. Elle considère le RGPD[97] comme un bon début mais que les politiques antitrust visant à fermer les entreprises détenant le monopole de la surveillance numérique ne permettront pas de freiner d'autres entreprises du même modèle de se constituer[98]. S'agissant du numérique dans la profession journalistique, la dépendance aux plateformes est économique, éditoriale, mutuelle mais asymétrique[99]. Les éditeurs de presse semblent contraints de développer leurs activités numériques à une ère du déclin de la presse papier. En retour, l'Etat joue un rôle essentiel afin de garantir le droit voisin – rémunération de la communication des publications – et la pérennité financière des éditeurs et agences de presse[100].

[97] Règlement Général sur la Protection des Données.
[98] Zuboff Shoshana, *L'âge du capitalisme de surveillance*, éditions Zulma, le 4 octobre 2018.
[99] Ouakrat Alain, « Négocier la dépendance ? Google, la presse et le droit voisin », le 15 juin 2020.
[100] Lyubareva Inna, Marty Emmanuel, « Vingt-cinq ans d'information en ligne : une exploration des transformations structurelles des médias », 2022.

* *

*

Conclusion

Ainsi, la surveillance de journalistes s'apparente comme un enjeu complexe et difficile à encadrer car pris au milieu de logiques sociologiques, économiques et politiques plus larges. Les enjeux du logiciel espion Pegasus sont très intéressants à étudier et en disent long sur la complexité des imbrications politiques à l'œuvre. Elles ne constituent toutefois que l'œillet de la porte d'entrée à une société de surveillance dans laquelle interagissent : des Etats – autoritaires comme démocratiques ; des services de renseignements ; des entreprises privées ; des géants du net – GAFAM ; et bien d'autres…La surveillance des journalistes à l'ère du capitalisme de surveillance doit se comprendre comme à la croisée de deux évolutions parallèles : la croissance de la surveillance et la croissance du numérique.

Au sein de cette société, les journalistes jouent un rôle qui, en tendance, les surexposent à la surveillance et à ses revers – attaques en ligne, harcèlement, intimidation, *hacking*…Et ce pour plusieurs raisons, parmi lesquelles : une pratique professionnelle dépendante d'une économie de plateformes et de réseaux sociaux qui collectent de plus en plus les données de ses utilisateurs ; une industrie peu couteuse de la surveillance privée comme présente au plus haut des services de renseignements qui banalisent la surveillance des reporters ; ou encore, un travail d'investigation qui leur confère un rôle clef dans la surveillance des sources de l'information, pour beaucoup dissidentes, voire dites dangereuses pour la sécurité nationale.

Il est par ailleurs nécessaire de concevoir encore plus loin la surveillance des reporters comme relevant d'une indissociation entre leur travail et leur identité – sexuelle, politique, religieuse. Une fois ces différents constats établis, que dire de la résignation des journalistes ? Pour certains, elle est collective ; pour d'autres, elle est contextuelle. En outre, la très faible législation encadrant la surveillance, et encore moins celle des journalistes, laisse à présager que la profession court un grave danger dans son degré d'indépendance.

Gardons toutefois quelques conclusions importantes : que la barrière sémantique entre sécurité numérique et sécurité physique doit être brisée ; que penser la sécurité des journalistes est indissociable de penser la sécurité des sources ; que l'encadrement de la surveillance doit être largement renforcé et étendu ; enfin, que la surveillance des journalistes doit être étudiée à partir, et nécessairement, d'une approche socionumérique nouvelle incluant les enjeux technologiques du XXIe siècle.

Pour la sécurité des journalistes et de leurs sources.

Pour la liberté de la presse.

Bibliographie

LIVRES

Agamben Giorgio, *Qu'est-ce qu'un dispositif ?*, éditions Payot & Rivages, 2014.

Aïm Olivier, *Les théories de la surveillance. Du panoptique aux Surveillance Studies*, Armand Colin, 2020.

Castagnino Florent, *Critique des surveillances studies. Éléments pour une sociologie de la surveillance*, Déviance et Société, 2018.

Deleuze Gilles, *Foucault*, 1986.

Fœssel Michaël, *Etat de vigilance. Critique de la banalité sécuritaire*, éditions Essais, 2010.

Foucault Michel, *Surveiller et punir : Naissance de la prison*, éditions Gallimard, 1975.

Giraud Guilhem, *Confidences d'un agent du renseignement français*, éditions Robert Laffont, 2022.

Lyubareva Inna et Marty Emmanuel, *Vingt-cinq d'informations en ligne, une exploration des transformations structurelles des médias*, Revue « Les enjeux de la communication et de l'information », le 26 septembre 2022.

Lyon David, *Au nom du 11 septembre…,* in Didier Bigo et Al., éditions La Découverte dans « Cahiers libres », 2008.

Marthoz Jean-Paul, *En première ligne. Le journalisme au cœur des conflits*, éditions Mardaga, 2018.

Marthoz Jean-Paul, *Journalisme international*, éditions De Boeck Supérieur, 2018.

Neveu Erik, *Sociologie du journalisme,* éditions La Découverte, 2009.

Zuboff Shoshana, *L'âge du capitalisme de surveillance*, éditions Zulma, 2018.

ARTICLES SCIENTIFIQUES

Bonfils Philippe, « Environnements immersifs : spectacle, avatars et corps virtuel, entre addiction et dialectique sociales », éditions CNRS, dans « Hermès, la revue », 2012.

Collard Victor, « L'addiction au prisme de la perspective sociologique », Introduction, EHESS, le 27 mars 2017.

Eyenga Macaire Georges, « Les nouveaux yeux de l'État ? L'introduction de la télésurveillance dans l'espace public à Yaoundé », éditions de l'EHESS dans « Cahiers d'études africaines », 2021.

Jung Barbara, « L'image télévisuelle comme arme de guerre. Exemple de la guerre du Biafra, 1967-1970 », éditions IRICE, dans « Bulletin de l'Institut Pierre Renouvin », 2007.

Lafarge Géraud, Marchetti Dominique, « Les portes fermées du journalisme. L'espace social des étudiants des formations 'reconnues' », éditions Le Seuil, dans « Actes de la recherche en sciences sociales », 2011.

Lafarge Géraud, Marchetti Dominique, « Les hiérarchies de l'information. Les légitimités 'professionnelles' des étudiants en journalisme », presses de Sciences Po dans « Sociétés contemporaines », 2017.

Lafarge Géraud, « Les diplômés du journalisme. Sociologie générale de destins singuliers », éditions DARES, dans « Travail et emploi », 2020.

Marchetti Dominique « Les révélations du "journalisme d'investigation" » Actes de la recherche en sciences sociales, vol 131-132, dans Persée, mars 2000.

Ouakrat Alain, « Négocier la dépendance ? Google, la presse et le droit voisin », *Sur le journalisme,* Vol 9, n°1, le 15 juin 2020.

Ruellan Denis, « Profession : reporter. Genre : féminin », pour l'Association Effeuillage dans « Effeuillage », 2018.

Ruellan Denis, « La fabrique du genre dans le journalisme de la sécurité », pour l'Association Effeuillage dans « Effeuillage », 2019.

Sebbah Brigitte, Sire Guillaume, Smyrnaios Nikos, « Journalisme et plateformes : de la symbiose à la dépendance », *Sur le journalisme,* Vol 9, n°1, le 15 juin 2020.

ARTICLES DE PRESSE

Aristegui Noticias, « Pegasus Project : Más de 25 periodistas en México de TV, radio, internet y prensa fueron blanco de espionaje », Sebastian Barragán, le 18 juillet 2021.

Forbidden Stories, « Pegasus : la nouvelle arme mondiale pour faire taire les journalistes », le 18 juillet 2021.

France Info, « Cyber espionnage : comment fonctionne le logiciel Pegasus ? », le 19 juillet 2021.

France Info, « Pegasus : le gouvernement et toute la classe politique française dans le viseur du Maroc », Elodie Guéguen, le 20 juillet 2021.

Le Monde, « Projet Pegasus : dans les coulisses de la traque d'un logiciel espion sophistiqué », Floriand Reynaud, le 18 juillet 2021.

Proceso, « Peña Nieto, el desenfrenado espionaje contra periodistas », le 18 juillet 2021.

The Guardian, "What is Pegasus spyware and how does it hack phones?", David Pegg et Sam Cutler, le 18 juillet 2021.

The Guardian, "Revealed: leak uncovers global abuse of cyber-surveillance weapon", le 18 juillet 2021.

The Guardian, "Revealed: murdered journalist's number selected by Mexican NSO Client", Nina Lakhani, le 18 juillet 2021.

The New York Times, "Using texts as lures, governments spyware targets Mexican journalists and their families", Azam Ahmedet Nicole Perlroth, le 19 juin 2017.

The Washington Post, "Private Israeli Spyware used to hack cellphones of journalists, activists, worldwide", le 18 juillet 2021.

The Washington Post, "How mexico's traditionnal political espionage went high-tech", Mary Beth Sheridan, le 21 juillet 2021.

The Washington Post, "Takeaway from the Pegasus Project", le 2 août 2021.

RAPPORTS

Artículo 19, rapport sur « La sécurité des journalistes mexicains », 2018.

Amnesty International, « Les géants de la surveillance. Le modèle économique de Facebook et google menace les droits humains », 2019.

Amnesty International, "Twitter scorecard: Tracking twitter's progress in addressing violence and abuse against women online", 2020.

Amnesty International, "Out of control: Failing EU laws for digital surveillance export", 2020.

Amnesty International, « La partie immergée de l'iceberg. La responsabilité des Etats et du secteur privé dans la crise de la surveillance numérique », 2021.

Amnesty International, « Attaques de cyber mercenaires en Afrique de l'ouest », 2021.

Amnesty International Security Lab, "Forensic Methodology report. How to catch NSO Group's Pegasus", 2021.

Committee to Protect Journalists, « Guide de sécurité des journalistes. Couvrir l'actualité dans un monde dangereux et changeant », 2012.

Conseil de l'Europe, rapport sur « La sécurité des journalistes », avril 2017.

Conseil de l'Europe, « Touchez pas à la liberté de la presse ! Les attaques contre les médias en Europe ne doivent pas devenir la règle », rapport annuel des organisations partenaires de la Plateforme du Conseil de l'Europe pour renforcer la protection du journalisme et la sécurité des journalistes, 2020.

Conseil de l'Europe, « Liberté des médias en Europe : des actions concrètes s'imposent! », rapport annuel des organisations partenaires de la Plateforme du Conseil de l'Europe pour renforcer la protection du journalisme et la sécurité des journalistes, 2021.

Conseil de l'Europe, « Défendre la liberté de la presse en période de tension et de conflit », rapport annuel des organisations partenaires de la Plateforme du Conseil de l'Europe pour renforcer la protection du journalisme et la sécurité des journalistes, 2022.

Freedom House, rapport "Freedom of the Net", avec l'Université d'Oxford, 2017.

International Center for Journalists, "The Chilling: A global study of online violence against women journalists", with the UNESCO, le 2 novembre 2022.

International Women's Media Foundation, Survey on online harassment.

Michael N. Schmitt, "Tallinn manual on the international law applicable to cyber warfare", prepared by the International Group of Experts at the Invitation of The NATO Cooperative Cyber Defense Centre of Excellence, Cambridge University Press, New York, 2013.

Reporters Sans Frontières, « Censure et surveillance des journalistes : un business sans scrupules », 2017.

Reporters Sans Frontières, « Guide pratique de sécurité des journalistes. Manuel pour reporter en zones à risques », avec l'UNESCO, 2017.

Reporters Sans Frontières, « Droit des femmes : enquêtes interdites », le 1er mars 2018.

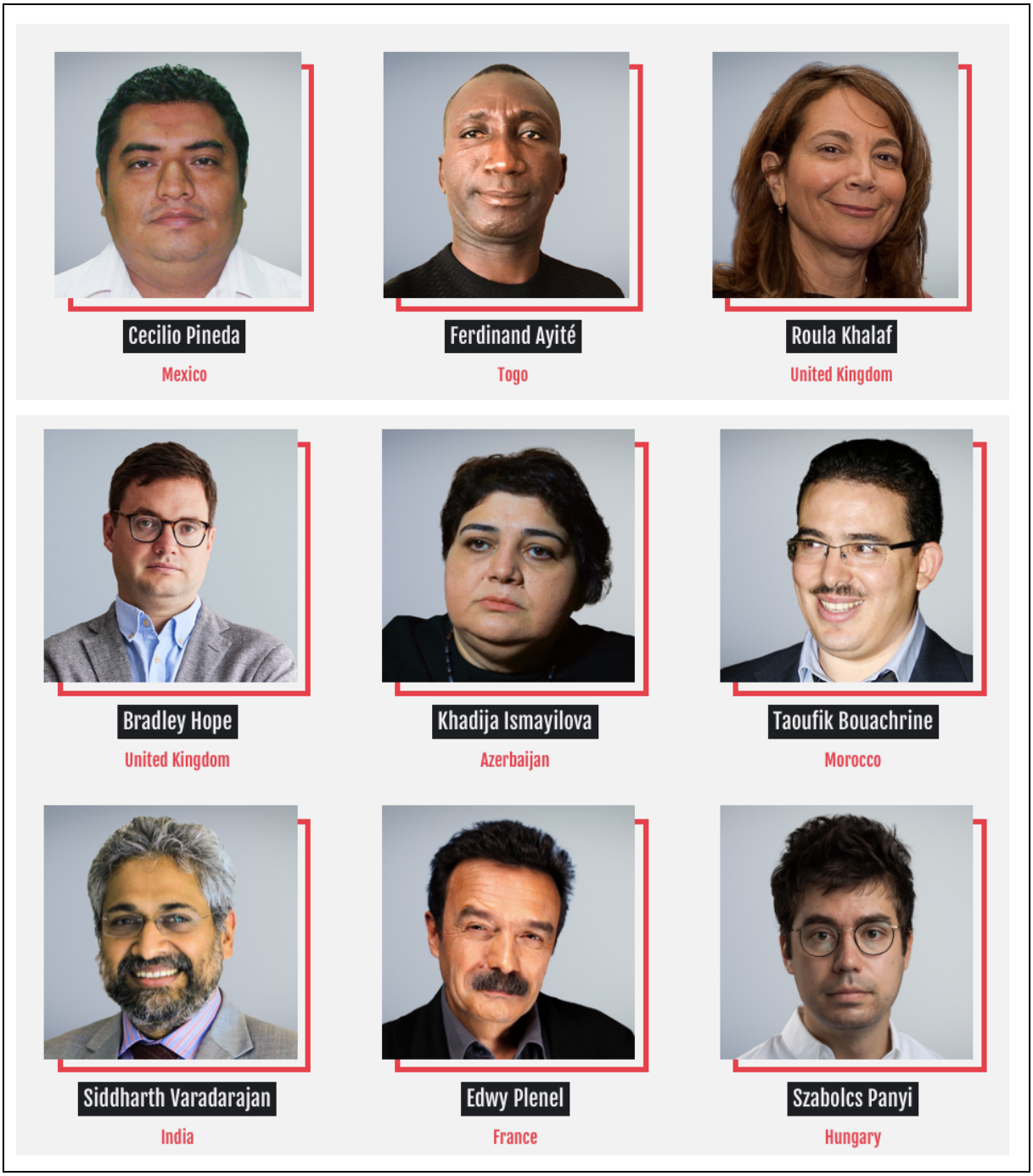
Reporters Sans Frontières, « Harcèlement en ligne des journalistes. Quand les trolls lancent l'assaut », le 25 juillet 2018.

Annexes

Annexe 1 : « La liberté de la presse dans le monde » en 2023 par Reporters Sans Frontières.

Annexe 2 : “Countries where journalists were selected as targets”, par Forbidden Stories.

Annexe 3 : « Profiles : journalists under surveillance ». *Forbidden Stories met en avant les portraits de journalistes dans le monde afin de remettre un visage sur les victimes de l'espionnage orchestré par des Etats via le NSO Group. Venant d'Inde, du Mexique, du Maroc, d'Angleterre, de France, d'Hongrie, d'Azerbaïdjan, du Togo, du Rwanda, de Turquie ou encore d'Espagne…Aucun continent ne manque à l'appel.*



Yuriria Sierra

Mexico

Eric Bagiruwubusa

Rwanda

Alejandro Patrón

Mexico

Carmen Aristegui

Mexico

Souleimane Raissouni

Morocco

Vijaita Singh

India

Paranjoy Guha Thakurta

India

Sevinc Vaqifqizi

Azerbaijan

Aboubakr Jamai

Morocco

Lenaïg Bredoux

France

Rafael Rodriguez Castañeda

Mexico

MK Venu

India

Turan Kışlakçı

Turkey

Jaspal Heran

India

Rosa Moussaoui

France

Maria Moukrim

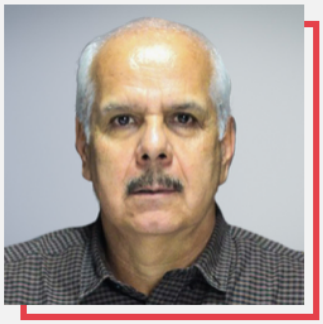
Morocco

Jorge Carrasco

Mexico

Swati Chaturvedi

India



Alejandro Sicairos

Mexico

Smita Sharma

India

Hicham Mansouri

Morocco

Alejandra Xanic Von Betrab

Mexico

Ignacio Cembrero

Spain

Sushant Singh

India

Ali Amar

Morocco

Marcela Turati

Mexico

Carlos Ketohou

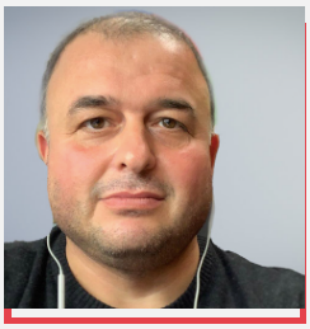
Togo

Ricardo Raphael

Mexico

Iftikhar Gilani

India



Jasur Sumerinli

Azerbaijan

Rohini Singh

India

David Dercsenyi

Hungary

Luis Hernández Navarro

Mexico

Alvaro Delgado

Mexico

Omar Brouksy

Morocco

ENTRETIENS

Elodie Vialle

Chercheuse en liberté d'expression et sécurité des journalistes.

Entretien réalisé le : 9 janvier 2023, en visioconférence.

Durée de l'entretien : 1h30.

Aujourd'hui, quelles sont vos recherches ?

« Alors moi aujourd'hui j'ai un profil comme *Press Freedom Defender,* je suis consultant en sécurité digitale et liberté d'expression pour l'organisation Pen America qui défend les écrivains, les journalistes et les artistes aux Etats-Unis. Je suis indépendante. Et aujourd'hui je suis aussi fellow à *l'Institute for rebooting social media* au Berkman Klein Center for Internet Society à Harvard. C'est une sorte de programme où je travaille sur un projet. Moi mon projet c'est de la recherche, c'est de travailler sur une ligne, un service d'urgence pour les journalistes harcelés en ligne. Aujourd'hui vous êtes harcelés en ligne, il y a pas moyen de contacter Meta, Twitter, etc., donc moi l'idée c'est de mettre en place une sorte de service client pour les journalistes et défenseurs des droits humains qui pourraient avoir des interlocuteurs au sein des réseaux sociaux. Donc je travaille là-dessus à Harvard avec le soutien de Pen America, et je travaille pour des organisations de défense des journalistes de manière générale ».

« Voilà pour mes recherches, et anciennement j'étais responsable du pôle Tech pour Reporters Sans Frontières. Depuis trois ans, je travaille uniquement sur la question du cyberharcèlement des journalistes et quand j'ai été à RSF en 2017, là j'ai travaillé sur tous les sujets tech et donc j'ai été amené à travailler sur ce sujet de la surveillance des journalistes ».

Diriez-vous qu'il y a une prise de conscience au sein du milieu journalistique auprès duquel vous intervenez sur les dangers de la surveillance ? Si oui, comment se manifeste-t-il ?

« Dans mon travail, comme je suis en lien avec beaucoup d'experts en cybersécurité et que je produis de nombreuses ressources pour les journalistes, j'ai en effet une vision globale de ces sujets au niveau français et international. »

« Oui, depuis Pegasus et le travail mené par Citizen Lab, par Amnesty, par Forbidden Stories, il y a une prise de conscience chez les journalistes. Mais alors je dirais qu'il y a le double effet qui se coule, c'est-à-dire qu'il y a d'un côté les journalistes qui se disent '*woh on est tous surveillés'* et ils flippent, et de l'autre, c'est '*bon on est tous surveillés'* et ils ne font rien. Donc c'est comme un régime, là c'est la nouvelle année et vous vous dites '*foutu pour foutu je vais manger des bonbons'*. Et en fait là c'est pareil, dans les formations de cybersécurité je constate ce double effet, celui de se dire '*de toute façon on est surveillés, de toute façon c'est mort, Pegasus on arrive même pas à évaluer si on est surveillés ou pas'*. Et ça a été un gros truc, on a pas la possibilité de traiter toutes les demandes des journalistes qui voudraient vérifier leur *device*. Donc en fait il y a un côté foutu pour foutu. Moi je pense que les gens ont tout à fait conscience mais qu'ils se disent que c'est mort ».

« Ce qui est compliqué aussi, c'est qu'on donne aux gens des règles d'hygiène digitale de base, pareil pour la cybersécurité. Mais en fait les règles d'hier ne sont plus les mêmes qu'aujourd'hui. Donc il y a une forme de confusion je dirais. »

En tant que chercheuse, que pensez-vous des recherches en sciences sociales qui sont produites en la matière ?

« Ce que je peux dire, ce que je trouve pertinent en tout cas, c'est de considérer les choses de manière holistique. Et notamment pour rejoindre votre question d'avant, nous on est les personnes en première ligne, on travaille sur la cybersécurité etc., et dans ce cas-là, je note une tendance, que j'observe aussi auprès de collègues qui travaillent sur la sécurité des journalistes et la surveillance aux Etats-Unis, on essaie de faire une approche de la cybersécurité qui est presque comme un conseiller, comme à l'école le conseiller pédagogique ou le conseiller psy. Certains travailleurs comme moi se définissent presque comme travailleurs sociaux, ils vont prendre le journaliste par la main et le guider, car en effet faire des *trainings* c'est compliqué car comme vous le dites ça évolue tout le temps. En fait les gens ont besoin d'un suivi pas à pas, en continu et que c'est quelque chose d'humain avant d'être technologique. En fait je pense qu'il y a une vraie tendance à essayer de rendre plus sexy le sujet, avec des *squads* etc., aux

Etats-Unis contrairement en France où on est en retard. Et du coup ça rejoint la question de la prise de conscience : on a d'un côté une évolution des technologies, de l'autre une problématique des prises de consciences, soit trop soit pas assez, et du coup y'a besoin de faire une sorte de soutien aux journalistes pas à pas. Et de plus en plus de travailleurs se définissent comme ça ».

Vous avez exposé dans vos recherches, vos rapports, qu'il existe plusieurs risques liés au numérique. Qu'est-ce qui explique, selon vous, la croissance du harcèlement en ligne ? Pourquoi, dans son fonctionnement, est-il si dangereux, à la fois pour la victime comme pour la profession ?

« Pour ce qui est de la croissance, il y a une sorte de retour de bâton de l'utilisation des réseaux sociaux par les journalistes et les droits humains pour faire avancer des causes. Au moment des Printemps Arabes on parlait aussi de révolution Twitter. Il y a aussi beaucoup de mouvements qui se construisent sur la base d'un hashtag et donc aujourd'hui on voit bien que si on veut avoir le pouvoir, il faut contrôler l'information et ça passe par les réseaux sociaux. Et une technique de désinformation c'est d'aller cyberharceler des sources fiables d'informations que sont les journalistes. Alors ça peut être quelque chose de très spontané, on n'a pas aimé quelque chose, on poste un mauvais commentaire. Et ça peut être des choses très organisées, donc là on a vraiment des armées de *trolls* mises en place par des gouvernements, des groupes politiques pour harceler les journalistes de manière massive, systématique, synchronisée. Il y a plusieurs types de cyberharcèlement, mais dans certains cas on est dans une technique de guerre de l'information avec la conséquence pour la liberté de la presse qui est que les journalistes se retirent des espaces numériques.

Et ce qui est terriblement injuste, au moment où on parle de diversité, c'est que les personnes les plus visées sont les femmes, sont les journalistes non blancs, c'est-à-dire les groupes qui sont déjà les plus ciblés, les plus marginalisés dans la profession. Donc c'est un vrai problème de liberté de la presse et de censure et c'est un vrai problème aussi pour toutes les questions de diversité des voix dont on parle souvent. Et puis ça coute moins cher de cyberharceler un journaliste et de le mettre en prison, d'où la montée de ce phénomène : l'imbrication avec les questions de surveillance.

Quand on dit aux journalistes de faire de l'évaluation des risques, de la menace, je parle aussi à ceux qui travaillent sur la surveillance pour que les médias en prennent conscience, que souvent un journaliste surveillé va aussi être harcelé, etc. Ce sont des menaces qui vont de pair. Là par exemple, on a travaillé sur une ressource à destination des journalistes cyberharcelés dans le monde arabe. Et pour eux, la problématique numéro un c'est celle de la surveillance. Rashovi c'est comme ça qu'il a été assassiné. Mais il y a un problème aussi de cyberharcèlement, car avant d'être démembré et assassiné : il était surveillé et cyberharcelé aussi. ».

« Les journalistes sont aussi une population marginalisée. Il y a une expression qu'on utilise beaucoup dans la recherche, c'est *People at risk*. Ça veut tout et rien dire mais on l'utilise de plus en plus. Moi le problème c'est quand j'arrive et que je dis '*les journalistes, les défenseurs des droits humains'* on me demande '*et les personnes exilées, personnes vulnérables ?*' donc c'est vrai que moi au départ j'ai un mandat, je travaille sur les journalistes. Mais cette expression dans la cybersécurité de *People at risk*, c'est en fait de dire qu'il y a des gens plus à risque, comme dans le secteur de la santé. Et en fait j'ai trouvé qu'il y avait beaucoup de parallèles avec des chercheurs qui travaillaient sur la question des migrants harcelés. Donc ce qu'on doit identifier ce sont les *Pattern* entre différents types de population et montrer les manières dont ils sont surveillés, harcelés, etc. »

Dans la suite de cette idée d'imbrication, pourquoi, selon vous, ces phénomènes touchent avec plus de force les femmes reporters ?

« Moi j'ai davantage vu des femmes journalistes ciblées par du cyberharcèlement. Par ailleurs on a aussi plus d'éléments, c'est bien plus difficile de documenter la surveillance, puisque même dans le cas de Pegasus, il est très difficile d'établir la preuve formelle de la surveillance des journalistes. Donc en fait on a beaucoup plus de documentation sur les questions de cyberharcèlement que sur les questions de surveillance par ce biais. Et le problème, c'est que le cyberharcèlement est pas vraiment perçu comme une menace. Moi une grosse partie de mon boulot c'est de faire des conférences, aller voir des rédactions pour leur dire de faire attention, de réfléchir à des campagnes. Moi j'aimerais faire un programme *No diversity without safety* : toutes les rédacs qui parlent de mettre de la diversité c'est du bulshit car elles mettent pas en place les actions pour protéger leurs équipes et leurs journalistes. »

« On a les chiffres du cyberharcèlement. Etude de l'UNESCO, 73% des femmes journalistes cyberharcelées dans le monde. L'IWMF dit qu'un tiers des femmes journalistes envisage de quitter la profession du fait du cyberharcèlement. Et je trouve qu'on s'occupe pas assez de cette problématique en France et on a des journalistes qui sont complètement cramés, pas bien. C'est une profession où les gens vont pas forcément super bien. Et donc ces problématiques de cyberharcèlement, dans un métier qui est pas évident, avec toujours une certaine tension, y contribuent. C'est très difficile d'avoir les éléments. Il y a des études sur la surveillance des femmes, mais plutôt dans le cadre de la violence domestique ».

Lorsque l'on observe l'état des technologies de surveillance, avec à son apogée, Pegasus, peut-on dire qu'il est encore possible de se protéger, de protéger ses données, et donc, de protéger ses sources ?

« Il est possible de rendre la tâche de votre agresseur en ligne plus compliquée. Déjà nous ce qu'on fait c'est beaucoup de sensibilisation-risque. Il faut que tous nos journalistes soient informés des risques et connaissent les outils pour s'en protéger. Si on peut déjà assurer ça, comme la plupart du temps c'est pas le cas, ce serait déjà bien. Donc les rédactions, les écoles de journalismes doivent assurer un degré de sensibilisation des journalistes. Et on peut rendre oui la tâche de l'agresseur plus compliqué : *password* unique pour chaque plateforme, mise à jour des logiciels, information sur l'évolution des risques, utiliser Signal ».

(…)

« Nous ce qu'on dit aux journalistes, c'est que se protéger, c'est pas seulement pour vous, c'est pour vous sources, pour vos proches. C'est ça aussi dans l'évolution de la prise en compte des risques, on introduit de plus en plus de penser aux familles. C'est-à-dire que vous vous allez peut-être faire gaffe si vous bossez sur Pegasus mais eux ? Eux ils y connaissent rien. Donc on a aussi créé des ressources sur comment parler de ces sujets-là à vos proches. Donc on est vraiment aujourd'hui dans un truc de leur dire de faire attention à ce qu'ils partagent sur les réseaux, de pas divulguer où ils habitent ou bien où vous vous habitez. Il y a donc plus de sensibilisation pour les proches. Aux Etats-Unis par exemple, il y a des solutions pour les *data brokers* car il y a des sites qui aspirent les données mais on a des problématiques similaires en France. Et donc les rédactions américains souscrivent à des services qui permettent d'aller chercher vos informations en ligne et de les effacer. On a demandé à ce que ces ressources, comme *delete me*, soient accessibles pas juste pour les journalistes mais que la rédaction paie pour les proches du journaliste ».

« C'est aussi pour ça que c'est compliqué d'aborder ce sujet-là dans un contexte de crise économique des médias. Et je pense que c'est un élément que l'on ne doit absolument pas omettre : on est dans un contexte où les questions de sécurité sont intrinsèquement liées aux questions économiques, aux questions de précarité. Là j'ai bossé avec pas mal de consœurs du continent africain et la première problématique c'est la précarité, c'est ce qui fait que la nana journaliste elle peut pas se protéger quand elle couvre certains sujets. C'est ce qui fait que face à d'autres questions, comme celle du harcèlement au sein d'une rédaction, elle va moins pouvoir se protéger car elle est dans une situation de précarité. Donc à Pen America on essaie vraiment d'avoir cette approche holistique. Et dernièrement j'étais à une réunion du sommet international pour la sécurité des journalistes à New York organisé par Cos et y'avait l'OCCRP qui fait aussi pas mal d'enquêtes, eux ils ont quasiment monté une assurance pour les journalistes. Donc là on parle de risques légaux mais aussi de sécurité. Parce que la plupart des journalistes, direct ils se prennent des procès et donc ils ont besoin d'assurance et tous les assureurs refusent car c'est trop dangereux mais aussi pour la sécurité physique. Et donc c'est les journalistes eux-mêmes qui sont en train de se réunir et de créer une mutuelle de journalistes pour s'assurer. Il faut donc toujours considérer le contexte dans lequel on s'inscrit, et on s'inscrit dans un contexte d'énorme pression politique et précarité économique pour les journalistes et qui va avoir des conséquences directes sur ce qu'on peut faire ou non en termes de sécurité. »

Qu'est-ce qui explique selon vous la dépendance croissante au numérique dans la profession journalistique ? Diriez-vous qu'elle est la raison de leur surexposition à la surveillance ? Le journaliste est-il au final la cible ou la conséquence de la surveillance de la population ?

« Avant d'être spécialisée sur la liberté de la presse, je donnais pas mal depuis une douzaine d'années, des formations au numérique, et à ce moment-là on voyait moins les dangers, c'était plus '*aller tous sur Twitter c'est cool'* et en fait je me souviens quand je parlais des réseaux, j'avais l'image du filet de pêche. Je disais aux jeunes des écoles de journalisme qu'ils devaient faire leur réseau de contact, et que les sources c'est comme un filet de pêche que vous allez lancer. Sur Twitter vous suivez de gens, etc vous faites rien, mais le jour où il y a une info qui tombe, vous relevez le filet de pêche comme un pêcheur, parce que c'est pas le jour où l'info tombe qu'il faut aller chercher la source, c'est avant. Et en fait, un journaliste c'est ça, tu relèves le filet de pêche et t'as tous les poissons qui tombent. Donc effectivement dans un système de surveillance, c'est un point qui va donner accès à tous les autres. Et c'est bien comme ça que

ça doit être pensé. Et c'est pour ça qu'un bon élément pour sensibiliser les journalistes c'est de dire qu'on est en train de parler de protection des sources là et moins d'eux. Parce que les journalistes aiment pas parler d'eux, ils ont du mal à dire qu'ils sont cyberharcelés, ils ont du mal à dire qu'ils souffrent. C'est vraiment une profession où on veut pas parler de nous-mêmes, à part pour montrer nos prix, Awards tout ça. Mais il y a un malaise à parler de la souffrance des journalistes eux-mêmes, comme s'ils voulaient uniquement mettre la lumière sur les autres et les gens dont on parle dans nos articles. Et je pense que pour ça il est pas mal le narratif, de dire que c'est de la protection des sources dont on parle. Et voilà comme vous le dites, le journaliste il a tissé un filet et souvent, avec des activistes, avec des opposants d'un régime, donc y'a qu'à tirer le filet pour choper toutes les infos, les contacts. D'ailleurs dans beaucoup de pays, quand un journaliste est arrêté, on va voir ses réseaux sociaux, ses sources. C'est pour ça que je dis de bien cacher la liste d'amis sur Facebook par exemple parce que là vous avez toutes vos sources, vos amis, vos familles qui se mêlent. Et puis en fait on va surveiller le journaliste pour l'intimider. Un journaliste d'investigation que je connais, la veille de la publication d'une enquête, il me disait qu'il reçoit des menaces. Je suis pas sûr qu'il ait été surveillé mais on savait qu'il bossait là-dessus.

En France, vous qui êtes beaucoup intervenue en écoles, pensez-vous que les formations journalistiques sont adaptées aux risques du métier, en ce sens, pensez-vous que nos futurs journalistes sont équipés pour y faire face ?

« Beaucoup de gens qui s'expriment sur les écoles de journalisme le font sur la base de ce qu'ils ont connu, mais qui y ont pas mis les pieds depuis vingt ans. Moi je suis intervenu de manière soutenue dans les écoles de journalisme de 2011 à 2017, et depuis j'ai fait des interventions plus ponctuelles (…). Une étudiante que j'ai rencontrée racontait que dans son école, les protocoles cyber et sécurité numérique n'existent pas et qu'il y avait une sorte de clash entre elle et le responsable pédagogique de son école. »

« Moi j'ai l'impression que ces risques sont un peu plus pris en compte, mais ce que vous devez pointer c'est qu'il y a une tension entre des discours contradictoires qui sont donnés aux journalistes, entre d'un côté la nécessité de *engage* avec l'audience, donc il faut faire du *reach*, du *live*, du commentaire. Et arrêtons de nous mentir, il y a plein de rédacs où on va être recrutés en fonction du nombre de followers qu'on a sur Twitter. Là je suis méchante mais c'est en partie vrai. Là j'avais une formation dans une grande télévision française il y a quelques jours, où les

journalistes nous disaient '*non seulement on nous demande de présenter, on bosse comme des tarés, mais en plus on a tout le SAV de nos émissions à faire sur les réseaux sociaux'*. Donc à la demande des rédactions, ils sont poussés à parler sur les réseaux sociaux, donc toutes les nanas elles se font harceler et elles doivent gérer elles-mêmes cette merde. Et donc on pousse les journalistes à ça, et en même temps on leur fait des petits points sur la sécurité. Moi ce que je voudrais c'est qu'on allie ces deux conversations ensemble et qu'on arrête de faire des cours séparés sur d'un côté la cybersécurité où on dit des trucs, de l'autre les réseaux sociaux où on dit qu'il faut aller chercher de l'audience et qu'on ait une vision plus globale. Moi je voudrais qu'on dise : on va pas moins publier, on va pas pas publier mais à chaque article, à chaque production journalistique, quel est le risque de cyberharcèlement ? C'est trop facile de dire qu'on va pas l'évaluer car on risquerait de se censurer : au contraire, on va mieux protéger nos journalistes. Parce qu'aujourd'hui on en a rien à foutre, et quand ça arrive à un journaliste on lui dit pas démerde toi parce qu'on peut plus trop dire ça mais on va lui dire que c'est pas grave. Parce que c'est facile, ça touche pas pareil la meuf de vingt ans, la petite journaliste que le rédac chef de cinquante balais qui est blanc et complètement en-dehors de ce type de menace. ».

« Je pense que quand même oui les journalistes sont un peu mieux protégés en écoles de journalisme, mais il y a selon moi de conversations qui ne sont pas encore là et qu'il faut amener. »

Sur la technophobie des sciences sociales

« Il y a en effet une technophobie, et elle est due à une méconnaissance. Même quand on parle de l'ingérence russe dans les élections américains de 2016, quand on creuse un peu, les mecs ils ont juste utilisé les outils de *Facebook for business.* En fait il y a aussi une méconnaissance de tout ce qu'on met derrière surveillance, et il faut bien la définir, des fois c'est juste le système de publicité ciblée comme le dit Zuboff. C'est comme la désinformation, à RSF j'avais fait une note en interne pour dire qu'on est dans de la micro-désinformation, et c'est pour ça que c'est passé sous le radar des journalistes et des chercheurs. Pourquoi aujourd'hui il y a tout un pan de choses qui passent sous notre radar en tant que journalistes, chercheurs, et comment est-ce qu'on peut l'intégrer à notre recherche sur la surveillance ».

Phineas Rueckert

Journaliste d'investigation à Forbidden Stories.

Entretien réalisé le : 11 janvier 2023, dans un café à Paris.
Durée de l'entretien : 1h30.

Conséquences pour les journalistes de Pegasus

« Pegasus c'est la technologie de surveillance la plus poussée, mais en fait c'est un outil qui affecte très peu de monde. C'est des journalistes plutôt d'enquête, plutôt dans des pays compliqués comme la Hongrie. Ce que je veux dire c'est qu'il y a tout un arsenal de menaces contre les journalistes. Donc la surveillance et Pegasus, ça nourrit des menaces qui existent déjà et ça va plus loin. Donc c'est une toute petite part des journalistes. Même dans les pays clients de NSO, c'est pas tous les gens qui sont espionnés.

Par exemple en Inde, il y a je sais pas combien de journalistes en inde, mais en total on a réussi à en identifier quarante. La plupart à Delhi, quelques-uns dans des régions un peu plus éloignées de la capitale. Je pense notamment à un journaliste dans une région centre d'Inde où il y a un mouvement Mawiste et des groupes qui luttent contre l'Etat. Lui il est pas membre de ces groupes là mais il enquête sur ça. Son cas il est intéressant parce qu'exactement un an après la publication de Pegasus, il a été arrêté et il est toujours en prison actuellement. Donc voilà, en dépit de notre enquête, de toutes les informations disponibles sur ces outils-là, on va toujours pouvoir arrêter des journalistes qui gênent. Ça c'est plutôt un cas négatif. Il y a d'autres cas où cette surveillance a fait en sorte que les journalistes puissent lutter, puissent faire des cas judiciaires ensemble, ça a eu un effet de rassembler des journalistes autour d'un sujet et ils ont par exemple fait appel à des cours européennes pour avoir plus d'informations sur cet espionnage-là.

Il y a d'autres journalistes qui ont été espionnés, comme *Chabox* en Hongrie, espionné, qui après le projet, lui-même membre du consortium d'enquête, il a été mis en cause par son propre gouvernement pour avoir accéder à des informations qu'il n'était pas censé obtenir. Ça montre encore une fois que les journalistes qui ont été espionnés, c'était des targets très importantes pour un gouvernement donc ils allaient pas juste laisser tomber les autres moyens de faire pression après le projet ».

D'où est partie l'implication de Forbidden Stories dans cette enquête ? Reporters qui vous ont contacté, reporters menacés, censurés ? Volonté issue de vos équipes ? Parce que les révélations de 2017 du Citizen Lab pointaient déjà du doigt les dérives de Pegasus ?

« Je pourrai pas vraiment rentrer dans le détail, mais avec Amnesty on a eu accès à un *leak.* Et pourquoi nous ? C'est parce qu'on avait déjà fait des enquêtes sur ce sujet-là, en fait la première fois qu'on a traité les questions de Pegasus c'était en 2020 pendant le projet Cartel, pour poursuivre le travail de journalistes mexicains menacés qui enquêtent sur la corruption de l'Etat, des choses comme ça. Et il y a un cas d'un journaliste à Proceso, média indépendant mexicain, on avait révélé avec Amnesty que le réd chef de ce média avait été targeté plusieurs fois par Pegasus. Donc nous on a réussi à enquêter sur ce sujet-là, on avait montré notre légitimité sur ce sujet. Et je pense que la mission ça jouait aussi parce que notre but c'était pas forcément de se concentrer sur les histoires d'hommes politiques, des grands noms, c'était de vraiment de lancer ça à partir des histoires de journalistes, des activistes et défenseurs des droits de l'Homme, des gens qui ont pas beaucoup de voix, et pour qui l'impact allait être plus important. Donc nous on a commencé comme ça, mais on pourra jamais dire que le projet Pegasus c'est nous, c'était déjà le Citizen Lab et d'autres, et même avant 2017 des organisations étaient dessus depuis quelques temps mais pas au même niveau. Je pense que notre focus c'était de partir des histoires des victimes et de mettre en visage un thème très tech. Souvent quand on parle de la surveillance, on pense les caméras cachées, partout, à la surveillance de masse, c'est pas une surveillance de masse Pegasus, c'est de la surveillance très visée. Donc ouais nous le but principal c'était de mettre un visage à ça, de parler des gens qu'on dirait pas être la cible d'une surveillance sophistiquée à ce niveau-là ».

Réaction sur le focus sur la classe politique et comment cela empêche de voir que la surveillance impacte très différemment selon les contextes politiques, sociaux, économiques…

« Je voulais souligner ce point-là. Le cas du journaliste indien dont je te parlais c'est un cas type, c'est un journaliste indépendant, éloigné de tout, qui est vraiment la seule personne qui enquête sur ce sujet dans une certaine région. Si lui est espionné et arrêté, ça crée une zone de silence dans cette région de l'Inde. Et des acteurs en ont intérêt ».

Quelles ont été les étapes de vos recherches ?

« Pour faire simple, on a une liste de milliers de numéros, dont on a pas les noms. Ce qu'il faut faire c'est de trouver un moyen de matcher ces numéros à des gens. Il y avait des moyens techniques, avec une base de données de *True Color* et *Collapse*. On a pu ainsi matcher des bases de données de numéros et de noms. On a aussi pris des carnets d'adresses des journalistes partenaires dans les pays clients et eux vont avoir les contacts des journalistes de leur pays, un carnet d'adresse assez costaud. On peut prendre tous les numéros, les dématérialiser, on les matche contre la base de données, peut-être qu'on va avoir vingt réponses et là on va demander aux journalistes partenaires s'ils connaissent la personne. Ça ça nous a donné peut-être un pourcentage important de numéros. Sur les 50 000, peut-être 10 000 ont pu être matchés. Evidemment c'est pas forcément cent pour cent fiable non plus. Par exemple, *True Color* c'est une application utilisée pour obtenir des carnets de contacts, mais parfois l'information est partielle, on va avoir l'info – *ami de* – donc ça donne pas tout. Ça nous a aidé à avoir une vision pkus globale de qui étaient les gens, après il y avait aussi une structure de l'opération qui faisait en sorte qu'il y avait des clusters de groupe avec un tel un tel un tel et t'imagines que un tel s'y retrouvera ».

Quelles étaient les méthodes de coordination au sein du consortium ? Qui faisait quoi ?

« Au départ on a commencé en interne. On était pas très nombreux, on était cinq ou six. D'abord on a réparti les régions : moi j'avais l'Inde et la Hongrie, ma collègue Paloma a fait le Mexique, une autre collègue Audrey a choisi les pays du Moyen-Orient, Cécile se concentrait sur le Maroc…On a choisi par hasard mais surtout par compétences linguistiques, Paloma parle espagnole, l'Inde beaucoup sont anglophones, le Maroc c'est francophone…Tout le monde coordonnait que cette partie de l'enquête. Et pour tout ce qui est interview avec le NSO, droit de réponse, c'était Laurent et Sandrine, le directeur et la réd cheffe. Et pour coordonner on a fait comme les autres projets mais avec un niveau de sécurité beaucoup plus élevé. Moi par exemple j'avais un groupe de journalistes qui bossaient que sur l'Inde, venant du Wire, du Guardian, du Monde. Donc d'abord on a matché les numéros, après on a commencé à contacter des gens fiables, des targets fiables, où on pouvait faire un lien de confiance pour leur demander de faire un forensique de leur portable. Ça c'était vraiment important pour nous, de pouvoir prouver techniquement que les chiffres alignaient avec l'infection de portables. Donc on a commencé avec les journalistes parce que c'était avec eux qu'on pouvait le plus faire un lien

de confiance. On les contactait à niveau individuel, on leur disait qu'on travaillait sur l'espionnage, on leur expliquait qu'ils avaient été espionnés, mais on parlait de l'ampleur du truc au début. Après on a fait ptet dix ou douze forensiques où dans la plupart on a vu des infections. En gros la procédure c'est : la personne doit télécharger une copie de son portable sur un site très sécurisé, et après le Digital Tech Lab d'Amnesty ils font une vérification. La plupart disait oui à vérifier leur téléphone, certains étaient pas confortables avec ça ce qui est normal, c'est comme donner l'intégralité de ton portable à quelqu'un que tu connais pas. Et en plus c'était pendant le Covid donc il fallait souvent convaincre des gens depuis des appels vidéo. Donc il y a pas le même niveau de confiance. »

« Pour le consortium, nous on a contacté des partenaires avec qui on avait une grande confiance, on les a fait venir à Paris, sans leur dire tout à fait pourquoi. Une fois ici, on leur a présenté le projet, les pistes et ce qu'il fallait prouver. Et après avec ce petit groupe, comme on a fait des forensiques qui étaient prometteurs, après on a contacté d'autres partenaires et là on a lancé le projet global plus grand. On continuait de faire des forensiques et on utilisait les réseaux de ces journalistes là pour continuer de matcher avec des numéros. Et puis à la toute fin on a commencé à contacter tout le monde, à chaque fois qu'on matchait un numéro on donnait la possibilité de faire un forensique et s'ils le faisaient pas on pouvait pas dire qu'ils avaient été infectés, mais on disait '*sélectionnés pour surveillance'* ».

Quelles sont les principales difficultés que vous avez rencontré dans votre enquête ?

« Je pense que c'est vraiment la question de la confiance, comment est-ce que tu convaincs quelqu'un de donner l'intégralité des infos de son portable. Déjà c'est des gens à qui tu viens de dire, '*je pense que vous êtes espionnés'*, et on peut pas vraiment trop détailler pourquoi on sait ça. Donc voilà il y avait la question de la confiance avec les victimes. Il y avait aussi la question de la sécurité digitale entre les partenaires. Quand on travaille sur la surveillance on peut pas juste appeler par téléphone ni-même parler par message WhatsApp. Donc nous on communiquait via un système très difficile à hacker. On communiquait pas du tout par SMS ou WhatsApp, Signal c'est *safe* mais on a préféré éviter quand même. C'était très difficile parce que c'était un système un peu compliqué à mettre en place et il fallait faire ça avec des journalistes aux Etats-Unis par exemple. Il fallait leur expliquer comment mettre ça en place sans être là et c'était pas toujours évident. Et puis à la fin y'avait un moment très tendu comme à chaque enquête où il faut la présenter au groupe sur lequel tu enquêtes et ils vont te dire soit c'est de la mauvaise information, soit que vous avez mal compris l'information, soit de diviser

les journalistes individuellement donc il faut que tout le monde soit d'accord sur comment on décrit notre information, avec quel langage ».

Est-ce que certains journalistes ont subi des attaques pendant l'enquête ?

« On a principalement, et tous, reçu des menaces légales. Mais en termes de menaces digitales, vu notre système on s'inquiétait pas trop pour ça. Mais on se disait que oui à tout moment on pouvait se faire hacker donc on a fait en sorte que pour tous les journalistes, tous les portables privés soient complètement déconnectés de l'enquête. Mais la menace la plus évidente était légale. Je pense que des journalistes aient subi des menaces physiques ou des tentatives de *hacking*. En même temps, si tu es NSO ou un client de NSO, et que tu sais qu'on enquête sur toi, venir hacker les journalistes serait pas forcément une bonne idée non plus ».

Quelle a été la démarche du consortium pour conclure de la responsabilité des Etats dans cette surveillance et des conséquences impliquées ?

« J'aurai pas vraiment de réponse. La responsabilité renvoie à l'Etat client, à la boite qui a vendu cet outil très puissant à des Etats avec des respects des droits de l'Homme très pénibles, et c'est aussi une question de régulation donc ça renvoie à l'Etat d'Israël et son département de défense qui valide l'exportation de Pegasus qui est une arme. Eux aussi ont une part de responsabilité. Donc pour moi il y a vraiment ces trois acteurs principaux. Ce qui est bien c'est que ce projet a montré ça et ça a forcé des Etats non forcément concernés directement à réagir, ça a été le cas pas mal de l'Union européenne, des Nations Unies, des institutions globales. Et ça faisait très longtemps que les activistes et défenseurs de droits de l'Homme voulaient que les gens se rendent compte de la responsabilité des Etats. »

Quelle est la limite que vous vous êtes posés dans cette enquête-là ?

« On essaie de pas faire de liens directs entre l'espionnage et les conséquences sur des victimes d'assassinés. On a dit qu'un journaliste mexicain avant son assassinat était en effet targeté, mais on ne peut pas faire le lien direct entre les deux car ce serait pas légitime. La seule personne qui sait comment l'information a été fuitée, c'est la victime, et ça fonctionne que si on a le mec au Mexique, et il est décédé. On voulait répondre à cette question bien sûr, mais c'était pas possible. Donc on a voulu dire que l'espionnage des journalistes dans le monde ça sert à ça, ça et ça. Ça peut être utilisé pour du chantage, mais dans des cas particuliers comme celui-là on sait pas exactement comment ça a été utilisé ni même si ça a vraiment été utilisé. Donc on a

voulu se concentrer sur les histoires de journalistes, et d'autres du consortium sur les histoires de politiques, et ça aurait pas eu le même impact si on avait juste fait un gros travail uniquement sur les journalistes. Ça a été notre objectif à Forbidden, mais on l'a pas imposé aux autres du consortium. Et pour terminer avec le Mexique, il y a des limites d'informations, et le gouvernement actuel a tout intérêt à enquêter sur les actions de leurs prédécesseurs. Donc au final on a souvent le comment mais rarement le pourquoi de l'espionnage et c'est ça l'une des plus grandes difficultés de cette enquête. »

(…)

Quelle est l'étendue selon toi de la prise de conscience des dangers présentés dans votre enquête ?

« Je pense que les journalistes du consortium en ont désormais tous très conscience, de même pour les journalistes victimes. Mais le problème et le grand danger avec Pegasus c'est son invisibilité, son côté zéro-click, on le voit pas et il y a pas une manière parfaite de se protéger. Et il y a d'autres moyens de surveillances, le *phishing*, le *hacking* qui sont moins sophistiquées et qui sont plus souvent utilisés contre les journalistes. Et pour le *phishing*, il existe des milliers de boites d'intelligence privée qui proposent ce service. Et ces méthodes nécessitent une interaction à un moment donnée, donc pour ces méthodes là les journalistes peuvent être attentifs. Mais il faut faire beaucoup de formations et sensibilisation dans tous les cas. Les journalistes sont des cibles faciles, ils reçoivent toujours de l'information, pas toujours vérifiée. Je pense que la prochaine étape c'est de montrer que la surveillance des journalistes c'est pas que Pegasus, c'est principalement des méthodes moins sophistiquées, c'est la surveillance des réseaux sociaux, c'est le *fiching*, le *hacking*, une attaque digitale pour faire tomber un site. Il existe donc plein de moyens, Pegasus ça reste un outil très cher, qui n'est vendu qu'à des Etats. La surveillance c'est un marché. Il y a un monde entier de la surveillance. Et le fait qu'on en sache plus sur Pegasus ça le protège un peu parce que maintenant la boite comme le logiciel ou les clients ne peuvent que s'adapter pour contourner la dénonciation, changer de nom, change de stratégie, etc ».

Paloma De Dinechin

Journaliste d'investigation freelance.

Entretien réalisé le : 3 février 2023 par appel sur Signal.

Durée de l'entretien : 1h.

A (Alexandre) : Oui, allô ?

P (Paloma) : Allô Alexandre ?

A : Oui, comment ça va ?

P : Ça va et toi ? J'essaye juste de mettre des écouteurs.

A : Bien sûr, bien sûr.

P : Une petite seconde. Ça sera plus simple. Attends une seconde, je regarde si ça marche. Et là tu m'entends ?

A : Oui, là je t'entends bien, oui.

P : Ok, ok, donc tu veux dire...Non mais j'ai...En fait, j'ai acheté des écouteurs...

A : Ouais ?

P : J'ai acheté des écouteurs dans un marché...Enfin, dans un marché. Genre dans la rue.

A : Ouais ?

P : Et ils marchent pas.

A : Ouais, ouais, ça m'étonne pas haha.

P : Ça ira comme ça !

A : Oui, oui, c'est très bien. Encore une fois, merci encore d'avoir répondu à ma demande pour pouvoir échanger un petit peu. Encore une fois, je vais essayer de pas prendre trop de ton temps.

P : Non, t'inquiète, ça va.

A : J'ai bien conscience, comme tu me disais la semaine dernière, que c'est un peu compliqué à gérer avec le décalage horaire depuis le Mexique. Pour faire le tour et te remettre un peu en contexte, là aujourd'hui, je réalise un travail de recherche sur la sécurité numérique des reporters et, on va dire, essentiellement aussi, je pense, les reporters d'investigation. Et je vais travailler sur cette question à partir de, on va dire, comme porte d'entrée l'affaire Pegasus pour montrer que, bon, Pegasus a été déjà des révélations très, très conséquentes, mais que, quelque part, c'est un peu que le sommet de l'iceberg d'une série de dangers du numérique très pressants pour le métier et qui sont peut-être encore assez peu identifiés. Donc, la question à laquelle j'essaie de répondre, c'est pourquoi est-ce que, alors qu'il commence à y avoir depuis déjà une bonne dizaine d'années une documentation croissante sur les dangers du numérique, du harcèlement en ligne, du vol d'informations, enfin, un peu toutes ces choses regroupées, pourquoi est-ce que, on va dire, collectivement, même en tant que journaliste, on a encore du mal à appréhender cette question-là ? Et moi, je travaille à la fois sur la France et sur le Mexique, d'abord d'un point de vue pratique, parce que je suis moi-même Mexicain, du coup, j'avais une meilleure connaissance, on va dire, du terrain, et puis aussi par intérêt et curiosité personnelle. Donc voilà , si je voulais pouvoir échanger un peu avec toi, c'est Phineas qui m'avait parlé de toi quand j'ai eu l'occasion de discuter avec lui, et qui m'a dit que tu avais spécifiquement travaillé sur le cas du Mexique pendant votre investigation, il y a déjà deux ans. Donc je voulais revenir un peu avec toi sur certains éléments de ça.

P : Ça marche !

A : Est-ce que tu acceptes que j'enregistre notre conversation ?

P : Oui, oui, il n'y a aucun problème.

A : Parfait ! Tout d'abord, est-ce que, dans le cadre spécifique de cette enquête-là à laquelle tu as participé, est-ce que tu dirais que les journalistes mexicains que tu as réussi à identifier, à Forbidden Stories, quand tu y étais, j'ai compris que tu n'y étais plus aujourd'hui...

P : Là, je travaille encore avec Forbidden, mais en freelance.

A : Est-ce que tu dirais que les journalistes que vous avez réussi à identifier, toi individuellement et avec qui tu as pu rentrer en contact, avaient conscience du danger que Pegasus pouvait représenter ? Est-ce que c'était quelque chose, quand tu es rentrée en contact avec eux, dont ils avaient déjà connaissance ou est-ce que c'était un peu très nouveau ?

P : Alors, en fait, je pense qu'ils ont conscience, en général, du danger d'être espionnés. Mais, en fait, ce qui est assez particulier au Mexique, c'est un peu comme s'il y avait une résignation collective. Tu vois ? Comme si , en fait, on ne pouvait rien faire contre ça. Donc, tu vois, je ne sais pas, ce n'est pas un pays où la personne est consternée, tu vois, quand elle apprend qu'elle a été espionnée, parce qu'il y a eu plein d'affaires. Et du coup, c'est un peu, ils partent du principe qu'en tant que journaliste, c'est quelque chose qui peut arriver. Ils ne prennent même pas beaucoup de mesures, tu vois ? Enfin, par exemple, particulièrement dans les zones je ne sais pas moi, dans le Guerrero tu vois, dans des États qui sont particulièrement dangereux, en fait, des États où, en gros, être journaliste, enfin, où les journalistes tombent comme les mouches. Enfin, c'est une fâcheuse expression, mais c'est le cas. En fait, ils vont, par exemple, t'écrire sur WhatsApp, tu vois, au lieu d'utiliser Signal. Enfin, tu vois, des petits tricks qu'on a, même si Signal, ce n'est pas de toute sécurité, enfin, comment dire, ce n'est pas complètement hors de danger, mais dans tous les cas, tu vois, ils ne vont pas prendre vraiment de fortes précautions sur ça, tu vois ? Ouais, ou par exemple, téléphoniquement, c'est moi qui dois leur dire, tu vois. Si on va s'appeler, c'est un sujet délicat et tout, ils pourraient me parler de choses sur WhatsApp dont ils ne devraient pas me parler ? Donc, en fait, il y a vraiment ce truc-là où ils ont conscience que c'est un danger. Quand ils apprennent qu'ils ont été espionnés, ils ne sont pas concernés parce qu'ils savent que c'est quelque chose qui peut leur arriver en tant que journaliste. Et oui, après, peut-être individuellement, je ne sais pas, c'est sûr que... Enfin, tu vois, par exemple, dans le cas de Carmen Aristegui, quand sa sœur, elle l'a appris, Theresa Aristegui, c'est sûr que, tu vois, elle...Sa vie, tu vois, c'est une femme retraitée qui s'occupe des affaires de sa maison. Enfin, elle savait que c'était parce que sa sœur est journaliste, tu vois ? Et elle était, bien sûr,

choquée. Mais en même temps, tu vois, c'est pas non plus quelque chose qui l'a énormément étonnée, tu vois ?

A : Oui.

P : Parce qu'en plus, il y a eu des campagnes massives, tu vois, le truc des textos, ce que c'était par textos et liant. Après, maintenant, ils ont des méthodes beaucoup plus sophistiquées. Mais à l'époque, c'était par textos. Et donc, en fait, ils ont tous reçu, à des moments, des textos bizarres. Et donc, en fait, ils vont relier tout de suite ça à cette expérience-là, tu vois ? Donc, en fait... Enfin, c'était un Pegasus visible, en plus, au Mexique, tu vois ?

A : Oui, oui.

P : Genre, par exemple, le fils Emilio Aristegui, tu vois, il recevait aussi des SMS. Et El Chapo vient d'être arrêté, tu vois ? Et du coup, il y avait un lien. Et en fait, tu vois, t'es tenté d'appuyer dessus. En fait, il disait que El Chapo a été arrêté dans un restaurant. Et le restaurant, c'est le restaurant d'à côté de chez lui, tu vois ?

A : Oui.

P : Donc, forcément, si t'es un peu curieux, tu reçois ça, t'as envie de cliquer sur le lien. Donc, lui, par exemple, je me souviens de ce type de texto qu'il a reçu. Donc, en fait, plusieurs qui ont pu se rendre compte qu'ils étaient espionnés et tout, en fait, c'est eux-mêmes, tu vois, qui sont allés voir Citizen Lab ? Enfin, ceux qui savent détecter les attaques Pegasus.

A : Ouais, parce qu'ils avaient déjà des doutes.

P : Donc, en fait, ouais au Mexique, c'était pas une énorme surprise. Après, c'est la quantité, tu vois, qui choque.

A : Oui, 15 000 personnes…Mais, justement, pour remettre un peu en contexte, parmi les 15 000 numéros de téléphone qu'il fallait un peu cross-check, pour réussir à retrouver la source, on va dire, il y a combien de journalistes, spécifiquement, que vous avez réussi ou que tu as réussi à identifier ?

P : Ça fait longtemps, donc je peux pas te dire le chiffre exact. Mais il y a un truc que tu peux trouver, en fait. Enfin, tu peux trouver certains qui sont totalement identifiés, en gros. Ah, je sais pas si on l'a fait pour tous. On a fait des espèces de fiches.

A : Ouais, ouais, j'ai vu sur le site de Forbidden. C'est les fiches journalistes. Mais je me demandais justement si c'était vraiment toutes les informations, tu vois, qui avaient été trouvées.

P : Non, je sais pas. Je pense pas que ce soit tous. Mais dans les articles, il y a écrit le nombre de journalistes, je crois. Mais si tu veux, je vérifie. Je me le note !

A : Oui, oui, je veux bien ! Parce que je voulais quand même doublement vérifier, tu vois, s'il n'y avait pas un écart entre, mettons...Parce que j'imagine qu'il y avait aussi des vérifications partielles. Je veux dire, on pouvait remonter peut-être à...jusqu'à la ville ou la région dans laquelle le numéro de téléphone, on va dire, circulait, fonctionnait, mais pas forcément jusqu'à la personne.

P : Après, le truc, honnêtement, pour les journalistes, c'est que, tu vois, on a eu accès à des carnets d'adresses de journalistes. Donc, en fait, ils ont tous les...Enfin, tu vois ?

A : Ouais.

P : Genre, ça a été un truc assez facile à identifier, dans le sens où, tu vois, si tu cross-matches...Par exemple, si tu cross-matches les numéros avec, je sais pas moi, l'adresse de contact de quelqu'un, qui est d'un journaliste mexicain, et après d'un journaliste de différentes localités, et tout ça, tu vois, ils sont en contact avec les autres journalistes. Donc, en fait, je pense qu'on a réussi à arriver au nombre exact entre guillemets.

A : Et est-ce que de tes souvenirs, quand tu es rentré en contact avec les journalistes que tu avais réussi à identifier, est-ce que, au-delà de leur surprise d'avoir été potentiellement infecté, est-ce que tu sais si ces mêmes journalistes étaient déjà victimes d'attaques du même style ? D'intimidation ? Est-ce que c'était quelque chose qui était déjà présent dans leur métier ?

P : Oui, oui. Par exemple, Carmen Aristegui, elle a aussi eu des campagnes, tu vois, de différents types, mais en ligne, par exemple, à un moment donné, ils voulaient dire qu'elle était

lesbienne. Mais du coup, tu vois, ils faisaient une campagne sur ça, ils ont fait une campagne pour...enfin, c'est pas public. Enfin, moi, je sais, tu vois, mais c'est pas public, sur le père de son fils. Et du coup, ils inventaient un père qui n'était pas le vrai. Ouais, quand t'es target d'espionnage, c'est sûr qu'on a déjà essayé plusieurs outils contre toi quoi.
A : Et est-ce qu'à ta connaissance ces journalistes, après la prise de contact de Forbidden, et après, pour certains, être allés jusqu'à la vérification très tech auprès du Citizen Lab ou celui de Lab d'Amnesty International est-ce que leur manière de se protéger a évolué ?

P : Alors, peut, mais en fait, c'est vraiment lié au Mexique. C'est ce truc-là que je te dis, c'est tout à fait lié au Mexique. Tu vois, en France, les gens qui ont appris qu'ils étaient visés par NSO, d'abord, ils étaient totalement choqués, mais deuxièmement, parce que c'était un truc auquel ils n'étaient pas habitués. Enfin, tu vois, les scandales d'espionnage au Mexique, il y a eu Gobierno Espía en 2017 par exemple. Au Mexique tu vois c'est chaque année qu'il y a une révélation sur l'espionnage. Donc, en fait c'est un peu différent, mais du coup, disons qu'en fait, pour eux, c'est comme un truc qui s'ajoute à une longue liste de menaces, tu vois ? Et en fait, de là à dire qu'ils ont changé leur méthode, je pense, forcément, tu vois, quand tu sais que t'as été espionné, ils font un peu plus attention à tout, mais c'est pas qu'ils ont changé radicalement leur méthode, tu vois ? Tu vois, plusieurs continuent d'utiliser leur téléphone sans prendre tellement de précautions, quoi.

A : C'était quoi, un peu, le profil des journalistes qui ont été targetés ? Est-ce que c'étaient principalement des hommes, des femmes ? Est-ce que c'était des journalistes plutôt en freelance ou plutôt, genre, attachés à des grands médias mexicains ? La dernière, est-ce que c'étaient des journalistes plutôt, de ce que tu pouvais savoir, mais plutôt aisés financièrement ou déjà dans des situations assez précaires ?

P : Je pense qu'il n'y a pas de profil type, mais souvent, quand on regardait dans le travail que le journaliste avait effectué à ce moment-là, il y avait une certaine logique, tu vois ?

A : Oui.

P : « Parce qu'ils étaient en train de mener, à ce moment-là, une enquête importante. Il y avait toujours des éléments de leur vie professionnelle qui l'expliquaient, tu vois ? Donc, il y a ça. Et après, il y a des journalistes, mais tu vois, c'est pas un frein qu'ils soient dans un grand média ?

Il y a des médias, particulièrement, par exemple Proceso, c'est un média qui est connu pour être critique du pouvoir, etc., qui a été particulièrement visé. Genre, il y avait...Enfin, je ne sais plus combien, mais tu vois, il y avait au moins 5 ou 6 journalistes de Proceso visés. Et parmi eux, des Hauts Postes, etc. Donc, quoi, il y a des médias qui menacent le pouvoir en place, des journalistes qui menacent le pouvoir en place, qui font des enquêtes qui dérangent, tu vois ? Enfin, sur tout ça. Mais il n'y a pas un profil, tu vois, particulier mais bien sûr avec beaucoup de journalistes d'investigation ».

A : « J'aime bien travailler sur le Mexique parce que globalement, tout change, en fait, en tendance au vu du contexte. Mais c'est vrai que des recherches que j'ai pu effectuer dans d'autres pays, du poids que peut avoir l'espionnage numérique sur les journalistes d'investigation, c'était quelque chose qui j'avais remarqué, frappait davantage en tendance les femmes reporters. Tu vois, les reporters qui travaillaient de manière indépendante et qui étaient, pour la plupart, déjà dans des situations, financièrement assez précaires ou, en tout cas, suffisamment pour que les dynamiques de surveillance ou d'attaque en ligne, en fait, soient très difficilement dures à s'occuper ».

P : « C'est vrai…Alors, dans le cadre du Mexique, vraiment, je pense qu'il y a un espèce de « on fait ce qu'on veut », genre, vraiment, on a pu voir aussi des sources de gens qui s'occupaient de ces programmes-là, tu vois, et, enfin, c'était vraiment, ils pouvaient même le faire par amusement, entre guillemets, enfin, tu vois il n'y a pas de limite, pas de chiffre, tu fais ce que tu veux. Donc, non, ils n'ont même pas eu un frein, tu vois, Carmen Aristegui, quand même, au moment où ils l'espionnent, c'est la journaliste la plus médiatique de tout le Mexique, tu vois. Et il n'y a pas de profil type, c'est j'espionne tout le monde, quoi. Enfin, c'est vraiment tout le monde, tous ceux qui peuvent être en danger à un moment donné, au Mexique, dans, ouais, dans ce qu'on a pu voir. Mais, ouais ».

A : « Et, j'avais une dernière question, mais celle-là, elle relève plus de la direction que vous avez prise dans votre enquête concernant la mise en responsabilité qu'on pouvait donner des États dans ces logiques de surveillance des reporters et, là, pour le coup, celle de services de l'État mexicain. J'ai pu lire dans votre enquête à Forbidden, et qui étaient des informations aussi qu'on retrouvait dans d'autres médias, qu'on, qu'on était capable de dire que le numéro de téléphone d'un journaliste mexicain venait d'être ajouté deux semaines avant son assassinat…Et ma question c'était de savoir dans votre investigation, quelles étaient les limites que vous vous

étiez fixées sur la mise en responsabilité des Etats qui dans cette dans cette industrie qu'est Pegasus sont devenues un acteur-clé ? »

P : « Tu entends quoi par la limite qu'on s'était fixé ? »

A : « Par exemple, est-ce que vous vous étiez dit que c'était de votre rôle de pouvoir dire que l'État, mettons, l'État mexicain aurait commandé indirectement, l'assassinat de tel ou tel reporter ? La question de prouver la potentielle causalité me semble ici essentielle ».

P : « Non pas vraiment. Nous on dit ce qu'on sait et puis, ce qu'on ne sait pas, on assume. Ce qu'on sait, on le sait et, tu vois, on n'a pas pu arriver à savoir quelle est la personne qui a demandé que le nom de Cecilio Pineda, par exemple, enfin, d'espionner le téléphone de Cecilio Pineda, ça oui on le sait pas. Donc, en fait, ce qu'on a fait, c'est d'être assez transparent sur ce qu'on sait, ce qu'on ne sait pas et, voilà, c'est aucune limite qu'on s'est fixé parce que pour des questions, je sais pas, sécuritaires ou... Non, c'est vraiment juste les trucs qu'on réussit à élucider et celles qu'on n'arrive pas à élucider. Après, heureusement, on espère que c'est un point de départ, tu vois, et après qu'il y a quelqu'un d'autre qui va s'intéresser à un cas particulier et peut-être aller plus loin, tu vois, c'est aussi l'objectif de ce type d'enquête et je pense que Pegasus, un peu, dix ans après l'affaire Snowden, ça a permis de remettre un peu au centre du débat public cette question de l'espionnage, de comment s'en préserver, du fait qu'il faut créer des régulations là-dessus, tu vois, et réguler ce marché ».

A : « Oui, oui, bien sûr. Ben écoute, merci beaucoup, c'était les grandes questions que j'avais à te poser. Je trouve ça vraiment très intéressant de pouvoir échanger avec toi parce qu'il y a très peu de gens qui ont très spécifiquement travaillé là-dessus. Peut-être juste en conclusion, est-ce que... maintenant qu'on en a un peu rediscuté, est-ce qu'il y a des choses qui, pendant l'enquête, du point de vue de numérique, on va dire, t'ont... je sais pas, t'ont paru un peu étranges ? »

P : « Non, mais il y a plusieurs questions, par exemple, est-ce qu'ils continuent de l'utiliser ? Ouais. Au Mexique, avec Asus, par exemple. Après forcément, tu vois, si on n'a pas publié quelque chose, c'est que c'est pas abouti, donc je peux pas m'étendre. Mais disons qu'il va y avoir encore beaucoup d'histoires là-dessus parce que, ben ouais, c'est un marché qui est pas régulé. À la base, Pegasus, ils disent qu'ils vendent à des Etats et, en fait, les Etats après, se

disent pas responsables de l'espionnage, donc ça veut dire, c'est qui qui espionne, quoi, tu vois. Et, enfin, ouais, c'est très peu régulé sous l'excuse de la sécurité nationale parce qu'à la base Pegasus, quand tu vois des vidéos de promotion, ils disent, enfin, une belle idée, hein, qui est, quand il y a une séquestration, on peut savoir à quel endroit, où la personne est, et donc, ça nous permettrait de retrouver des victimes, criminels…Enfin, tu vois, en soi c'est nécessaire que l'Etat ait ce type d'armes, mais la question, c'est comment on le régule et comment on met des limites, quoi. Oui, oui, ben, c'est clair. Et qu'est-ce qui... Et surtout, est-ce qu'il y a une impunité totale à partir du moment où quelqu'un a utilisé cette arme pour espionner des gens de la société civile, des journalistes ? Est-ce qu'ils sont punis ? Est-ce qu'il se passe quelque chose ou pas du tout ? Enfin, ça, c'est ce qu'on va suivre ».

A : « Oui. Ben, écoute, merci beaucoup encore d'avoir pris un peu de temps pour répondre à mes questions. C'était vraiment hyper intéressant d'avoir ton avis un peu sur tout ça. Et oui, en fait, c'est... Bon, de manière anecdotique, mais ça m'étonne pas tant que ça, en fait, pour les reporters au Mexique, il y a un côté un peu foutu pour foutu, qui n'est pas propre qu'au Mexique, mais qui, je sens, en fait, se généralise de plus en plus ».

P : « Ouais, tu vois, il y a aussi AMLO qui a participé à ça, tu vois, parce que quand on sort le scandale à un moment donné, c'est vrai qu'il dit, bon, on va faire la lumière et tout, mais sinon, en fait, il dit, « ah, je le savais, enfin ». En fait, il dégonfle tout. On vient d'apprendre quand même que son médecin personnel était espionné pendant qu'il était en campagne, enfin, c'est quand même hyper fort, tu vois, genre, son médecin, quoi, et le gars, il agit un peu en mode, « ah, ouais on le savait ». Enfin, on sent qu'il y a un malaise vis-à-vis de ce truc-là, en fait, il dit qu'il peut faire la lumière, après, en fait, il ne l'a fait jamais.

Je crois que R3D a pu même démontrer que, tu sais il y avait des documents, ils ont dit que c'était des documents classifiés et en fait, non, enfin, toute une histoire avec les documents, genre, des documents, des contrats sur Pegasus et tout, où, en fait, il a dit qu'il mettrait la lumière. En gros, R3D a demandé des contrats et après, R3D s'est rendu compte qu'il y en a un qu'ils n'avaient pas donné et ils les ont retrouvés, et du coup, ça prouvait qu'en fait, ils avaient vraiment menti tranquillement et donc, ouais, il y a vraiment ce truc où il a un peu dégonflé aussi l'histoire. Parce qu'après il a cherché à enquêter. Mais on sait tout ce qui se passe au Mexique avec les pactes politiques, tout ce qui se passe un peu dans l'obscurité des accords entre parties sur ne pas enquêter sur tel truc ou tel truc…Bref, ce qui est sûr, c'est que ça aide

pas non plus un président qui prend pas du tout ça au sérieux. Et c'est un peu tous les États qui étaient gênés comme ça, tu vois, en fait, c'est qu'eux aussi utilisent des armes d'espionnage, etc.

Même en France, pour l'instant sur les trucs de l'espionnage et tout, ça s'est un peu géré en interne. Quand tu vois, genre, et parce que, aussi, je pense, parce qu'il y a un malaise généralisé, parce que si tu enquêtes trop sur ce que les autres font, on va aussi regarder ce que tu fais et t'es pas irréprochable non plus en tant qu'État, quoi. T'as peur qu'un jour ce soit ta liste qui soit mise.

Maxine Singeot

Chargée de projet au pôle Assistance de Reporters Sans Frontières.

Entretien réalisé le : 3 février 2023 par appel sur Signal.
Durée de l'entretien : 45 minutes.

Peux-tu présenter tes missions chez Reporters Sans Frontières ?

« Alors oui, moi je suis chargée de projets au bureau assistance RSF à Paris. On a plusieurs bureaux et sections à l'étranger mais à chaque fois qu'un journaliste doit être soutenu, le soutien passe par le siège à Paris. Et donc à l'assistance on est trois chargés de projets et Caroline est la directrice du bureau assistance. Et le rôle de chargé de projet ça va être de recevoir les demandes d'assistance des journalistes et de les traiter. Quand je dis traiter c'est qu'on va échanger par mail avec les journalistes, poser des questions pour comprendre son parcours journalistique et ses besoins. On va même lui envoyer un questionnaire ultra détaillé, dont savoir si leurs comptes, leurs réseaux sociaux ont été hackés. Une fois qu'on a toutes les infos, ça passe par des échanges de mails peut d'ailleurs durer quelques jours, voire quelques mois, et après on va envoyer un résumé au correspondant. On a un correspondant à peu près par pays et c'est le correspondant qui va nous faire un retour, confirmer les activités journalistiques de la personne et les menaces. Et une fois ce retour-là, on va prendre une décision en équipe sur comment aider la personne ».

« Nous notre mandat à l'assistance ça va être : soutenir des journalistes en danger en raison de leur travail actuel, donc il faut que la personne soit journaliste, qu'elle le soit toujours et qu'elle soit menacée en raison de son travail. Si elle est menacée pour son activisme, mais qu'elle est aussi journaliste, ça rentrera pas dans ce cadre-là car il faut vraiment que ça remplisse ces deux critères. Quand je dis journaliste, ce sont les professionnels des médias, donc ça peut être un preneur de fonds, un caméraman, ça peut aussi être un bloggeur s'ils font aussi du travail d'information. Donc c'est assez large ».

« Et on a du coup deux types de soutien individuels. Le premier type de soutien ça va être un soutien financier, donc on peut faire des bourses aux journalistes. Le premier type de soutien qu'on fait ça va être d'aider les journalistes à se réinstaller, soit en interne quand la personne

par exemple est menacée à l'Ouest de la RDC et qu'elle considère que ça suffit pour elle de changer de régions et d'aller à l'Est. Quand elle considère que ça suffit pas, on peut l'aider à quitter son pays et à se réinstaller ailleurs. Donc on va prendre en charge les frais de billets d'avion, leur loyer pour deux trois mois, la nourriture etc. car en général quand un journaliste se réinstalle il arrête de travailler. Donc ce soutien on le fait énormément en ce moment pour des journalistes d'Afghanistan qui se réinstallent au Pakistan, et pour ceux qui se sentent encore en insécurité, on peut soutenir leur demande d'arriver en Europe. Et on le fait aussi énormément pour les journalistes russes qui veulent un soutien financier pour s'installer dans les pays limitrophes, comme la Géorgie ou la Turquie, etc. Soit pour se réinstaller aussi en Europe, notamment en Allemagne et en France. Un autre type de soutien financier qu'on peut faire c'est un soutien aux frais d'avocats. On peut faire du soutien médical si des journalistes ont été blessés dans l'exercice de leur fonction. Ça a été beaucoup le cas en 2020-2021 au Bélarus quand beaucoup de journalistes se sont retrouvés frappés par les forces de police. Un autre soutien financier qu'on peut faire c'est le soutien prison : on peut arriver de l'argent aux familles des journalistes en prison pour permettre de payer les frais en prison, parce que parfois l'aspect de soin d'hygiène ou pour le transport ».

Toutes ces protections sont-elles accordées différemment selon leur statut (indépendant, rattaché à un média…) ?

« Non du tout on va apporter notre soutien à tout le monde, même quand ils sont en freelance. Par contre quand les journalistes vont se réinstaller, et qu'on sait que c'est des grosses rédactions qu'ont les moyens, on fera peut-être une bourse un peu plus faible que pour un journaliste freelance ».

« Un autre soutien financier qu'on fait c'est un soutien psychologique qui est assez nouveau depuis la guerre Russie-Ukraine, on va payer des séances de psy aux journalistes où ils peuvent avoir accès à des consultations. Et aussi il y a le soutien matériel, qui va permettre de s'acheter du matériel, soit parce qu'il a été saisi par des autorités, soit parce qu'il a été cassé en manifestation. Aussi, lorsque le matériel a été saisi, je pense notamment au gouvernement russe, les journalistes même si ils récupèrent leur matériel on leur conseille de pas les réutiliser au cas il y aurait eu des puces, micros de placés dans leur ordi, caméra ou téléphone portable ».

« Et ensuite le deuxième type de soutien qu'on va apporter c'est un soutien administratif donc concrètement ça va être soutenir des demandes de VISA pour qu'ils puissent quitter leur pays quand ils sont en danger. Une fois avoir quitté leur pays, on va les aider à régulariser leur statut, à obtenir l'asile, des permis de résidence. Pour faire ça, on va rédiger une lettre de soutien qu'on va adresser aux ambassades où on va reprendre le parcours du journaliste, les menaces et expliquer pourquoi il doit obtenir un VISA et obtenir l'asile ».

« Après dans le pôle assistance y'a aussi le soutien média pour soutenir des médias en exil, des soutiens ponctuels pour palier des difficultés financières de court terme, payer les journalistes, les locaux, mais ça peut aussi être un soutien permettant aux rédactions de payer des formations en sécurité numérique. C'est le cas notamment d'un média russe en ce moment. Et on prête aussi des gilets pare-balles et des casques et on fournit aussi une assurance aux journalistes sur le terrain ».

Quelles actions vous menez sur le terrain ?

« On a un pôle qui s'appelle la DRIP qui s'occupe du réseau international de RSF et qui va donner des formations sur le terrain aux journalistes sur en Amérique latine et en Asie. Ça peut être des formations sur les bases du journalisme, sur le travail de terrain, à des journalistes comme à des ONGs. Par contre on fait très peu de formations liées à la sécurité numérique. Avant on avait une conseillère à RSF qui s'occupait de toutes ces questions-là et qui est partie en 2017 et depuis on est très nuls. Son poste n'existe plus et nos manuels de sécurité numérique à RSF datent d'il y a dix ans maintenant. L'assistance travaillait sur ces rapports mais ils sont pas du tout mis à jour et on est plus du tout spécialisés sur ces questions ».

« Le but du *Digital Security Lab* basé, rattaché à la section allemande de RSF à Berlin qui vient de rouvrir c'est de leur fournir des noms de journalistes qui pensent avoir été hackés et ainsi obtenir un compte-rendu. Jusque-là tous les journalistes qui pensaient avoir été compromis sur leurs réseaux on les renvoyait vers l'ONG *Tech 4 Press* parce qu'on avait pas la capacité de le faire ».

Quelles sont les relations que vous entretenez avec d'autres organismes spécialisés en liberté de la presse ?

« Nous au pôle assistance on est rattachés au réseau *JIG List Journalism in Distress* et c'est un réseau d'ONGs qui soutient des journalistes en danger. Il y a le CPJ à New York, FPU à Amsterdam. Et nous on se coordonne avec eux. Dès qu'on reçoit un cas d'assistance on va vérifier que d'autres ONGs l'ont pas déjà soutenu pour éviter les doublons. Et dès que nous on est pas forcément compétents ou qu'on a pas de fonds suffisants, on renvoie vers d'autres acteurs. Mais en fait RSF, au même titre que le CPJ, on est une ONG qui fait tout en termes de soutien alors que d'autres ONGs ont un mandat plus resserré. Donc quand on réfère à une autre ONG c'est soit parce qu'on a pas les fonds suffisants, soit parce qu'on a déjà soutenu la personne une première fois, mais je travaille avec tous les autres acteurs bien sûrs. Et tous ces autres groupes sont au même stade que nous en matière de sécurité digitale, c'est-à-dire pas très au courant de ce qui se passe et qui vont donc vite référer à des groupes comme *Tech 4 Press*.

Qu'est-ce qui explique selon toi que RSF a perdu la main sur les dangers liés au numérique ?

« Je pense que ce qui s'est passé c'est que le poste d'Elodie Vialle n'a pas été reconduit. Et c'est aussi beaucoup une question de priorités et là justement depuis plusieurs mois c'est nécessaire, d'où le projet du *Digital Security Lab* aujourd'hui. Et aussi par manque de fonds, aujourd'hui on a notamment beaucoup développé le pôle assistance qui a été créé début des années 2010 alors qu'aujourd'hui on est sept ou huit à bosser à l'assistance. Entre l'Ukraine, l'Afghanistan, l'Iran…on a beaucoup de travail. Aussi concernant l'Iran, on va notamment soutenir des journalistes iraniens en leur fournissant des VPN. Et pour les médias russes aussi on a le projet *Collateral Freedom* de RSF qui permet à des médias bloqués dans leur pays d'avoir un site miroir par des informaticiens de RSF qui permet de redonner accès à leur site ».

Alicia Arquetoux

Étudiante en journalisme.

Entretien réalisé le : 17 février 2023 par appel sur Signal.
Durée de l'entretien : 1h.

Est-ce que tu peux, pour commencer, me rappeler dans quelle école ou formation tu étudies ?

« Alors moi j'étudie à l'IUT de Lannion en Bretagne. Donc, à l'époque, quand j'ai commencé ma formation, c'était en DUT. Ma première année scolaire, c'est 2020-2021. Et là, actuellement, je suis en licence professionnelle spécialité web. Voilà. Mais toujours à l'IUT de Lannion ».

Et est-ce que, dans tes études, t'as déjà suivi une formation sur tout ce qui est enjeux de sécurité numérique, dans son sens très large, dans la profession ?

« Alors, nous, vu que c'est en DUT, c'était la moitié où c'est des cours, la moitié où c'est plus des ateliers pratiques. Donc, on a plus eu des cours en atelier pratique qu'en pure théorie sur les questions de sécurité informatique. Donc, en première année, on a eu l'intervention d'un informaticien qui est très proche des milieux militants, qui traîne beaucoup à la ZAD de Notre-Dame-des-Landes. Il nous a un petit peu expliqué tout ce qui est messages d'actualité, Proton Mail, et qui nous a initié à l'utilisation de Tails, du coup. Ouais. Donc, ça, c'était intéressant. Et du coup, en fait, lui, il avait plein de clés Tails à vendre, et du coup, on pouvait acheter une clé Tails avec lui. Ça, c'était sous un module de... un truc comme 4 heures. Tu vois, on a eu pendant 4 heures de cours avec lui où il nous expliquait plus ou moins l'intérêt de fonctionner par Tails et utiliser des messages d'actualité. Après, voilà. Je réfléchis en même temps que tu te parles. Pour les discours des intervenants, notamment sur les intervenants qui taffent sur l'enquête et l'investigation, il y a eu beaucoup, en effet, de rappels, du coup, d'utiliser Proton Mail, d'utiliser Signal, Telegram, de parfois donner rendez-vous directement aux personnes pour se parler plutôt que passer par les téléphones ou par les mails. Ça, c'est le cas ».

« Pas mal aussi, nous, on a un principe, ce qu'on appelle les PPP, qui sont les projets professionnels particuliers, un truc comme ça, où en fait, en première année, tu vas travailler sur un dossier, sur une thématique, et en deuxième année, tu vas inviter tes journalistes sur cette

thématique. Donc après les cours, t'as des conférences comme ça, et dans les conférences, t'as beaucoup de journalistes d'enquête et d'investigation qui t'invitaient et justement, on revenait sur les principes de protection des sources et du coup, de protection numérique sur la protection des sources ».

« Après, il faut que je réfléchisse, ça, c'est en deuxième année. En deuxième année, on a plus de travail sur la protection des données sur le web et du coup, d'utiliser différents outils, par exemple, juste en prenant mon ordinateur, genre par exemple, moi, je suis sur Google, mais c'est Google Chromium. Au lieu que ce soit rouge, c'est bleu. Parce qu'en fait, en termes d'accès, tu donnes moins d'informations. Pareil, j'ai installé un petit logiciel pour pouvoir bloquer les cookies automatiquement, dès qu'il y en a. Et ça, c'est dans le cadre d'un cours qui a dû durer, pareil, je pense 4 heures, un truc comme ça, c'est un module de 2 heures, fois deux. Qu'est-ce qu'il nous a montré d'autre ? Il nous a montré...On a parlé moteur de recherche, on a bien entendu, encore une fois, évoquer Tails, comment communiquer, encore une fois, de manière un peu cryptée. Et il me semble que c'est tout ».

« Après, moi, en plus, en deuxième année, j'ai fait une formation avec France 24 sur être journaliste de guerre ou être journaliste en zone de tension. Du coup, qui était en partenariat avec l'école et la formation France 24. Et là, pour le coup, on n'était que 5 à être sélectionnés, donc c'est pas beaucoup, c'est pas toute la classe qui a pu en bénéficier. Mais en gros, on a eu tout un module informatique où... Je regarde, comme ça, je te donne en direct le moment où ça s'applique. Genre... Typiquement, on nous a donné des logiciels pour apprendre à bien effacer les fichiers qu'il y a sur ton ordinateur. Genre Eraser, je sais pas si tu connais ».

Ouais, je connais !

« On nous a donné aussi...En fait, ce cours-là, c'était surtout pour apprendre à cacher des informations sur ton ordinateur et que si tu fais fouiller ton ordinateur, les gens n'aient pas accès ou les autorités n'aient pas accès à tes documents. Donc des tips en mode tu modifies l'extension de ton document pour qu'il soit pas lisible. Tu utilises des coffres en ligne pour stocker tes informations, qui sont accessibles que par des codes. Sinon, qu'est-ce que j'ai d'autre ? Aussi un espèce de logiciel, en gros, qui garde tous tes mots de passe. Comme ça, t'as pas besoin de les noter quelque part. Et en fait, c'est un logiciel qui est totalement inviolable. Toi qui connais un code, quand t'as accès à ce code, t'as accès à tous les codes possibles sur toutes les informations que t'as ».

Oui, je vois le fonctionnement, mais peut-être pas forcément ce logiciel-là.

« Pareil, comment utiliser Tor. Ouais. Enfin, ce genre d'outils. Ça a été beaucoup d'apprentissage d'outils, de prise en main d'outils, et surtout de plus, en général, réfléchir à nos pratiques et les adapter en fonction de ce que t'as besoin. Genre, si t'es journaliste en PQR et que tu travailles sur des sujets, je sais pas, culture, par exemple, t'as pas forcément besoin d'avoir des gros outils de sécurisation. Du coup, je dirais que c'était plus de l'apprentissage et de la réflexion à voir sur quels outils à mettre en place en fonction de quelles pratiques journalistiques t'as et de réfléchir à ça plus génériquement**.** Et aussi, chacun de nos intervenants a bien répété l'importance de séparer, on va dire, les utilisations. C'est-à-dire que sur ton ordinateur, t'as un ordinateur, tu fais une liste de choses précises sur ton ordinateur que tu fais pas avec ton téléphone, c'est pas les mêmes accès, c'est pas les mêmes cadres de travail pour éviter de multiplier les risques de fuites. Voilà ».

Super tout ce que tu as pu suivre en la matière. Mais toi, est-ce que de tous tes amis et un peu les autres étudiants que tu peux connaître, qui sont aussi peut-être dans d'autres formations, d'autres écoles, est-ce que t'as senti que c'était quelque chose qui était assez spécifique à l'IUT de Lannion ? Parce que tu disais que c'était quelque chose d'assez privilégié dans le sens où on ferait pas ça dans toutes les écoles de journalisme ?

« Ça, j'aurais du mal à l'évaluer. Mais je dirais que déjà, à Caen, ils travaillent moins sur ces questions. Et par exemple, notre intervenant, il est quand même venu deux fois, une fois en première année, une fois en deuxième année. Le mec qui est proche un peu de la ZAD et du coup, il a une culture hyper militante. Il est hyper branché, quadrature du net, etc. Du coup, en vrai même, je connais pas d'autres écoles où on leur a distribué des critères pour pouvoir surfer sur le net. Et puis même, Lannion est plus inscrite dans une culture militante de gauche. Donc, lui, il était hyper... Enfin, moi, ça nous faisait un peu... Des fois, il était un peu parano, un peu anti-technologie, mais anti-GAFAM. Du coup, on nous disait ‘n'utilisez jamais Google Documents quand vous travaillez sur un article, quel que soit l'article’. Le fait, on va dire que toute sa culture un peu de sécurité sur le numérique est quand même très... Vient quand même beaucoup du fait que c'est un militant qui est proche de milieux qui sont très surveillés. Donc, je pense que peut-être à Lannion, c'est ce qui fait un peu la différence sur la formation de la sécurité numérique. Parce que c'est ce mec-là qui l'a fait ».

Alors, sur un autre sujet, peut-être un peu délicat, est-ce que ça t'était déjà arrivé de subir des formes d'attaques ou pressions en ligne ? Je dis attaques, en fait, dans son sens général, parce que je considère qu'un message malicieux, du harcèlement en ligne, un piratage, du vol d'informations, des formes d'intimidation, genre toutes, doivent être à un moment donné, d'un point de vue sémantique, être considérées comme des attaques. C'est pour ça, je me demande aussi si c'est quelque chose que, déjà, en tant qu'étudiante, apprentie journaliste, c'est quelque chose que t'as déjà pu expérimenter ?

« Honnêtement, non. Mais c'est parce qu'aussi, je pense que ça vient beaucoup du fait qu'à Lannion, on a un territoire local. Du coup, tous les gens qu'on va voir, qu'on interview pour les cours, tous les articles qu'on fait, on les fait dans un cadre qui est très fermé. En général, quand il y a des frictions avec des sources, ça se fait de visu ou directement par téléphone. Il n'y a pas vraiment de harcèlement en ligne, ni rien, parce que la distance entre les acteurs est plus courte aussi, je pense. Mais moi, j'ai rien vu ».

Mais autre question, cette fois, un peu plus de mise en situation, on va dire. Si un jour, tu te faisais pirater ton ordinateur, ton téléphone, à quoi ou quel élément tu penserais en premier ?

« Mon premier réflexe en cas de piratage, c'est déjà d'évaluer à quel point les informations qui m'ont été envoyées sont confidentielles, à quel point ça peut mettre les personnes autour de moi en difficulté et du coup les prévenir automatiquement. Si ça me concerne, justement, ça va. Si ça concerne des sources ou des gens avec qui je travaille, tout de suite les prévenir pour qu'ils puissent s'organiser de leur côté. Après, ça dépend dans quel cadre c'est, si c'est dans le cadre où je suis journaliste dans une rédaction, tout de suite prévenir la rédaction, voir avec le service de protection numérique pour tout de suite sécuriser mon ordinateur. Si c'est plus en temps de pigiste et du coup c'est plus, on va dire, une attaque envers moi, dans ce cas-là, je me rapproche directement d'un informaticien. Après avoir sécurisé les personnes qui pourraient être mis en danger. Attends, je bouge parce que j'ai plus de batterie ».

Sinon, la question que je me posais c'est en fonction des expériences que tu as pu avoir mais dans les différentes rédactions dans lesquelles tu as été amenée à travailler et dans lesquelles tu travailles aujourd'hui aussi, à quel point est-ce que t'évalues, admettons que le numérique et la dimension numérique a aujourd'hui un impact dans la manière de faire

du journalisme ? C'est un peu large, je sais, mais qu'est-ce que ça t'évoque ? Comment est-ce que tu appréhendes ça ?

« C'est quelque chose qui est déjà un peu acté, le fait que maintenant il y a le numérique dans nos vies. Moi, je trouve ça intéressant, mais c'est une situation qui s'est aussi développée avec Internet. Je ne suis pas censée faire du terrain, mais j'ai juste l'affection à l'Internet. Il y a des choses aussi intéressantes qui se font, c'est-à-dire que... Je t'entends un peu mal, je ne sais pas si c'est le micro. Tu vois ça sur le data-journalisme. Oui. Et j'ai fait aussi l'année dernière une conférence avec Arthur Carpentier, qui est journaliste en Syrie. Je ne sais pas où il est. Par exemple, ils avaient essayé de trouver un CRS qui était à l'origine de l'éborgnement d'un chirurgien qui avait été dans les manifestations. Du coup, ils ont coupé toutes les photos et vidéos sur le web et ils ont essayé par triangulation de deviner le niveau du CRS. La personne n'était pas sur place. Je trouve ça très intéressant, notamment pour réduire les coûts. Après, c'est un travail qui est gigantesque en termes de recherche parce que tu passes des heures et des heures sur ton ordinateur et pour le coup, je pense que t'as aussi un peu le piège du digital labo de dire que tu travailles sur le web et du coup, entre guillemets, tu fais pas vraiment de travail journalistique, mais que pour autant, t'as une espèce de dérégulation des heures de travail parce que tu travailles bien plus que si tu faisais ton travail en action et que tu portais sur le terrain une journée ».

« Parce que là, à chaque fois, pour leurs articles, ce qui fait qu'ils ont aussi un temps de publication qui est plus long, c'est des mois où ils collectent des données et ils essaient de les analyser et d'établir une localisation aux différents angles de vue pour essayer de comprendre les situations. C'est vraiment un travail qui est gigantesque et pas intéressant, mais c'est juste que c'est très... Il faut être très appliqué. Et après, en général, le travail numérique... Je trouve qu'on observe surtout dans la presse quotidienne en général le fait que c'est déjà des journalistes qui ont écrit sur la clé. En fait, on leur demande en plus de produire sur le web, en plus de faire des photos, en plus de faire des podcasts, en plus de faire de la vidéo. Et du coup, le web, il alourdit aussi la part de travail des journalistes. Et on leur demande aussi de faire des publications sur les réseaux sociaux avec normalement du pouvoir métier. Et je pense que... Toutes ces tâches, elles produisent sur le travail des journalistes. Du coup, t'as des choses intéressantes qui peuvent se faire notamment dans l'installation, pour trouver aussi des sujets, parce qu'il y a beaucoup de choses qui émergent dans la société. Pour faire du fact-checking, c'est ce qui est intéressant. Mais après, sur des pratiques plus de presque au début, ça peut avoir des dérives sur juste le plan du travail et du temps de travail ».

Un dernier commentaire général ?

« Je dirais qu'en école, j'ai été surtout formée à protéger mes échanges avec les sources. Réfléchir à quels outils de travail t'as besoin. Parce que des fois, t'as juste ça dans le papier d'accueil. T'as pas forcément besoin d'en faire un autre. C'est comme ça. Et... Du coup, pareil, installer des moteurs de recherche où t'acceptes pas de continuité. Et... Troisième point... Les sources. Et oui, essayer d'apprendre à cacher des documents. Je trouve que c'est vraiment le troisième point sur lesquels on travaille. Pour la protection du public ».

C'est vraiment génial qu'il y ait tout ça à l'IUT de Lannion parce que j'ai le sentiment que c'est quelque chose qui est vraiment pas très généralisé dans la plupart des formations journalistiques.

« En fait, c'est vraiment hyper niche. T'as aussi très peu d'intervenants à faire venir. Il y a toujours aussi un peu un tabou à parler de harcèlement en ligne. Ce qui fait que j'ai l'impression qu'il y a un peu dans certaines écoles, un peu un discours contradictoire. D'un côté, mettons, tu vas avoir à la limite un ou deux ateliers sur tes 4-5 ans d'études quand même sur l'importance de protéger tes données, tes informations, tes sources, etc. Te protéger de faire des fausses gaffes sur Internet et sur le numérique. Et de l'autre côté, tu vas avoir des ateliers genre réseaux sociaux et comment le journalisme doit passer aussi par faire la promotion et l'accès à de l'information. Sauf que du coup, comme les deux sont entièrement séparés, il y a un peu un truc de... On te dit un truc et son contraire, mais qu'en fait, on se rend pas compte que les deux devraient être mélangés et qu'il devrait y avoir aussi une formation quand on utilise les réseaux sociaux, c'est là qu'on s'expose à ce danger-là et qu'on peut pas juste être dans une logique et une démarche de il faut absolument que l'information aille au plus grand nombre et le plus vite possible, au risque de... Au risque de se surexposer, d'exposer une partie de sa vie privée, au risque de plein de choses ». Moi, je sais que j'ai pas eu de formation par exemple sur le harcèlement, mais c'est vraiment protection numérique qu'on travaille vraiment sur le harcèlement, comment gérer les commentaires, etc. ».

FORMATION PROFESSIONNELLE

Laurent Richard

Documentariste, producteur et fondateur du média Forbidden Stories.

Titre de la formation : « Sécurité numérique des journalistes ».

Formation réalisée le : 16 mars 2023.

Durée de la formation : 3h30.

Nombre de participants : 15.

Moyenne d'âge : 45 ans, tranche d'âge de 28-60 ans.

Profil des participants : 10 femmes, 5 hommes, tous journalistes.