



MASTER 1 SCIENCE POLITIQUE - COMMUNICATION ET POUVOIR

SAVOIR, PREVOIR ET INFLUENCER

Le cercle vicieux du microciblage politique et du capitalisme de surveillance

Sous la direction de Monsieur le Professeur Jérôme Valluy

Chloé COUPAT
Année universitaire 2023-2024
UFR 11 – Science Politique

UNIVERSITÉ PARIS 1 – PANTHÉON SORBONNE
MASTER 1 SCIENCE POLITIQUE – COMMUNICATION ET POUVOIR

SAVOIR PREVOIR ET INFLUENCER
LE CERCLE VICIEUX DU MICROCIBLAGE POLITIQUE ET DU
CAPITALISME DE SURVEILLANCE

Sous la direction de Monsieur le Professeur Jérôme Valluy

Chloé COUPAT
Année universitaire 2023/2024
UFR 11 – Science Politique

*« Those who would give up essential Liberty,
to purchase a little temporary Safety, deserve
neither Liberty nor Safety »¹.*

Benjamin Franklin, père fondateur des Etats-Unis

¹ Citation extraite d'une lettre que Benjamin Franklin aurait contribué à écrire en 1755 au nom de l'Assemblée de Pennsylvanie, à l'attention du gouverneur de cette colonie américaine. Source : https://fr.wikipedia.org/wiki/Un_peuple_pr%C3%AAt_%C3%A0_sacrifier_un_peu_de_libert%C3%A9_pour_un_peu_de_s%C3%A9curit%C3%A9_ne_m%C3%A9rite_ni_l%27une_ni_l%27autre,_et_finit_par_perdre_les_deux

REMERCIEMENTS

En 2016, en seconde, j'écrivais dans le cadre des « travaux pratiques encadrés » une recherche nommée « prévoir les attentats », en réaction aux événements de 2015. Bien que très succinct, ce premier travail m'a amené à m'interroger sur l'efficacité de la surveillance de masse, et les risques pour nos vies privées de la collecte des données. Je découvrais ainsi avec incompréhension qu'un programme respectueux des libertés et capable de prévoir un passage à l'acte terroriste (Thinthread) avait été abandonné par la NSA au profit d'un projet plus intrusif, plus coûteux et moins efficace. Je n'arrivais pas à donner du sens à ces informations.

En 2023, j'assistais dans un amphithéâtre de la Sorbonne au cours dispensé par le Professeur Jérôme Valluy sur la dimension politique du numérique. Ce cours a réellement bouleversé ma manière de comprendre les évolutions actuelles et m'a permis de donner du sens aux événements. J'ai ressenti le même soulagement, et la même passion que lorsque que je découvrais en seconde la sociologie, me permettant alors de comprendre le monde social. Je comprenais enfin l'origine et les explications aux choses que je pouvais observer et que je ne comprenais pas (les inégalités scolaires, la différence de traitement entre les filles et les garçons, etc). De la même manière, j'ai

enfin pu commencer à comprendre pourquoi l'on acceptait que les GAFAM collectent nos données, violant nos vies privées grâce au concept du capitalisme de surveillance.

Je souhaite à mon tour contribuer à une meilleure compréhension de ce capitalisme, et de la manière insidieuse dont il s'institutionnalise dans nos démocraties.

Je tiens à exprimer ma profonde gratitude au Professeur Jérôme Valluy pour le soutien inestimable qu'il m'a apporté tout au long de cette année. Son expertise, le temps consacré à m'accompagner et ses encouragements ont été des piliers essentiels dans la réalisation de ce mémoire.

Je remercie sincèrement, également, Monsieur Kevin Geay pour m'avoir guidé dans cet exercice nouveau et hautement stimulant qu'est le mémoire. Ces conseils m'ont été précieux. J'ai apprécié venir chaque semaine au TD de pratique de la recherche, sa passion pour la recherche et l'enseignement étant évidents.

Je remercie mes parents, Béatrice et Christophe, ma famille et mes amis proches, notamment Julien, Alicia, Pauline et Melvin, qui m'ont aidé à croire en moi et mes capacités, qui ont supporté avec bienveillance et patience mes explications décousues alors que j'avançais dans ma recherche tout au long de cette année. Merci d'avoir été présents pour moi.

Je remercie enfin ma grande sœur, Marion, pour ses relectures, malgré la longueur de plus en plus importante de mes travaux.

Je vous remercie tous et toutes, très chaleureusement, pour avoir cru en moi et en mon travail. Cette année de recherche restera gravée dans mes souvenirs, tout comme votre soutien.

SOMMAIRE

INTRODUCTION	9
I. LES DONNEES AUX FONDEMENTS DU MICROCIBLAGE ET DES MANIPULATIONS ELECTORALES ...	21
A. L’AFFAIRE CAMBRIDGE ANALYTICA REVELATRICE DES PRATIQUES DE COLLECTE DES DONNEES NUMERIQUES	23
B. LES MECANISMES AU SERVICE DES MANIPULATIONS ELECTORALES NUMERIQUES.....	33
II. L’EFFICACITE DES MANIPULATIONS ELECTORALES NUMERIQUES QUESTIONNEE	45
A. LE DEBAT REITERATIF DE L’EFFICACITE DE LA PROPAGANDE ELECTORALE.....	47
B. LE MICROCIBLAGE POLITIQUE COMME FACTEUR D’EFFICACITE DES MANIPULATIONS NUMERIQUES	55
III. LES GRANDS GAGNANTS DU MICROCIBLAGE COMME CHEVAL DE TROIE : LES GAFAM ET LE CAPITALISME DE SURVEILLANCE ET D’INFLUENCE	65
A. LE MICROCIBLAGE POLITIQUE OU LE CHEVAL DE TROIE DU CAPITALISME DE SURVEILLANCE ET D’INFLUENCE	67
B. LES GAFAM : DES ACTEURS INCONTOURNABLES DEVENUS INDISPENSABLES	77
CONCLUSION.....	91
ANNEXE :.....	95
BIBLIOGRAPHIE	111

Introduction

« *Nous savions pour qui [...] les gens allaient voter avant même qu'ils l'aient décidé* ». ²

Voici l'affirmation faite par Ken Strasma, expert en analyse prédictive et conseiller de Barack Obama pendant sa campagne électorale de 2008.

Cette citation résume bien l'enjeu des « *data analytics* » - ou science des données. A partir de la collecte et du traitement de données des modèles prédictifs du comportement des consommateurs ou des électeurs sont conçus. L'élection de Barack Obama marquerait ainsi, selon Anaïs Theviot³, le « *point de départ des data analytics* » dans le domaine politique.

La campagne innovante du candidat démocrate a été une source d'inspiration pour de nombreux candidats à travers le monde, exportant les techniques de l'analyse de données. Se sont alors développées sur le marché électoral des cabinets de conseil assimilables à des « *data brokers* » - courtiers en données. Les data brokers sont spécialisés dans la collecte et la vente de données. Les cabinets de conseil politique se spécialisent dans l'utilisation de données pour remporter une victoire électorale. Ils peuvent collecter eux-mêmes les données d'où leur assimilation aux data brokers, mais ils peuvent aussi acheter les bases de données directement à ces derniers ou aux

² ISSENBERG Sasha, *The victory lab: the secret science of winning campaigns*, 1. ed., Crown Publ, New York, 2012.

³ Anaïs Theviot, *Big Data électoral. Dis-moi qui tu es, je te dirai pour qui voter*. Lormont, Éd. Le Bord de l'eau, coll. Territoires du politique, 2019, 200 pages.

plateformes. Les données récoltées concernent l'identité, la localisation, tout « élément spécifique à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale » de l'utilisateur⁴.

Le terme de « plateformes » est employé dans ce mémoire pour désigner à la fois la plateforme comme dispositif numérique (dimension matérielle) et comme acteur. Il n'existe pas encore de consensus concernant ce terme en sciences humaines, comme l'explique très justement Vincent Bullich dans son article « *Plateforme, platformiser, platformisation : le péril des mots qui occultent ce qu'ils nomment* »⁵. Ce terme est une reprise de l'autodésignation des plateformes par la littérature scientifique. Le terme est très englobant d'où la critique de Bullich, néanmoins nous choisirons de l'employer pour cette raison. Cela permet à la fois de parler des GAFAM (Google, Amazon, Facebook, Apple, Microsoft) mais aussi de plus petites entités qui ont les mêmes pratiques que ces géants d'internet. Ce qui compte dans la désignation de ces firmes, dans le cadre de ce mémoire, n'est pas tant la force économique de ces acteurs (bien qu'elle témoigne de leur importance et de leur pouvoir sur les Etats), ou des enjeux de classifications logistiques (portails, sites, applications, réseaux sociaux, etc) mais ce sont surtout les pratiques similaires de ces entreprises quant aux données (collecte, traitement, vente). Nous aurions aussi pu choisir de les désigner sous le terme de « data brokers » puisque les plateformes comme les cabinets de conseil politique spécialisés en science des données ont les mêmes pratiques concernant les données : collecte, traitement et vente (sous forme transformée ou brutes). Finalement ce sont tous des « data brokers ». Mais les désigner ainsi masquerait la pluralité des acteurs qui utilisent les données des utilisateurs sous un terme très générique. Les cabinets de conseils fournissent aussi un service d'accompagnement stratégique en communication, les plateformes, quant à elles, ont aussi une dimension sociale qui ne peut être oubliée (les plateformes sont le prolongement de la vie sociale des individus), enfin les data brokers *stricto-sensu* -courtiers en données- ne font que de la collecte et de la vente de données.

⁴ RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) : <https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679>

⁵ BULLICH Vincent, « Plateforme, platformiser, platformisation : le péril des mots qui occultent ce qu'ils nomment », *Questions de communication*, n° 2, vol. 40, 2021, p. 47-70, [<https://doi.org/10.4000/questionsdecommunication.27413>].

La définition donnée par Ivan Manokha est pertinente, pour définir les plateformes dans le cadre de ce mémoire. Ainsi, les plateformes « *peuvent se définir comme des infrastructures numériques qui mettent en relation les producteurs, les consommateurs, les prestataires de service, les publicitaires et autres groupes dans un écosystème interactif en permettant l'échange de produits, services ou informations* »⁶. Nous emploierons tout de même, parfois, le terme de GAFAM pour insister sur la dimension économique et monopolistique de ces acteurs. Le terme de réseau social sera aussi employé pour désigner certaines plateformes comme Facebook ou Twitter dans leur dimension sociale. Il s'agit alors d'utiliser le terme dans son sens commun. Parmi les plateformes, il y a aussi les services de livraison de nourriture, les GPS, les services de streaming de musique ou de vidéos, les services de location de logement de vacances, services de vente entre particuliers, les moteurs de recherche, les services de transport, les applications de paiement mobiles et la liste est encore longue. On voit bien que la diversité des acteurs, de leurs objectifs, de leurs logiciels obligerait à employer un trop grand nombre de désignations. Il est donc nécessaire de les rassembler sous le terme - critiquable- de plateformes pour moins insister sur leurs différences que leurs points communs notamment au regard des données.

Nous parlerons essentiellement de trois grands types d'acteurs dans ce mémoire : les cabinets de conseil politique, les data brokers *stricto sensu*, et les plateformes (que nous préciserons par moment : GAFAM, réseau social, ...).

Le point commun de ces plateformes est qu'elles accumulent les données de leurs utilisateurs, les traitent à l'aide de délégations logicielles⁷, et les vendent dans un but publicitaire. La délégation logicielle est une notion développée par Bullich. Il utilise ces termes pour désigner les intelligences artificielles, mais en mettant l'accent non pas sur ce qui serait « l'intelligence » d'une machine, mais sur le transfert de compétences vers un logiciel. Le traitement des données par la délégation logicielle permet de les transformer en un produit monétisable : des prédictions. Des listes de cibles sont vendues selon leur probabilité d'agir selon le comportement attendu (acheter le produit de la publicité). Les plateformes sont financées par le marché publicitaire qui repose sur

⁶ MANOKHA Ivan, « Le scandale Cambridge Analytica contextualisé: le capital de plateforme, la surveillance et les données comme nouvelle « marchandise fictive » », *Cultures & Conflits*, n° 109, 2018, p. 39-59, [<https://doi.org/10.4000/conflits.19779>].

⁷ BULLICH Vincent, « La délégation logicielle et la reconfiguration des pratiques rédactionnelles : le cas meltygroup », *Communication & management*, n° 2, vol. 17, 2020, p. 51-65, [<https://doi.org/10.3917/comma.172.0051>].

la capacité des publicitaires à vendre le produit ou le service de leurs clients. Les plateformes doivent donc accumuler le plus de données possibles afin d’avoir des modèles prédictifs toujours plus exactes et performants. Ces modèles prédictifs sont assimilables à la définition de « profilage » par le RGPD à son article 4 :

« Toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique ».

Le terme de microciblage englobe ces notions de profilage, de modèle prédictif et de publicité personnalisée. En d’autres termes, le microciblage est la pratique qui consiste à collecter les données personnelles des utilisateurs et à les traiter (profilage) pour prévoir leur comportement (modèle prédictif) et ainsi les soumettre à des publicités personnalisées. Les plateformes se rémunèrent à partir de leur capacité à faire du microciblage.

Certains chercheurs choisissent alors de désigner ce nouveau modèle économique sous le terme de capitalisme de plateforme, nous préférons parler de capitalisme de surveillance selon le concept de la sociologue Shoshana Zuboff⁸.

« Le capitalisme de surveillance revendique unilatéralement l’expérience humaine comme matière première gratuite destinée à être traduite en données comportementales. Bien que certaines de ces données soient utilisées pour améliorer des produits ou des services, le reste est déclaré comme surplus comportemental propriétaire, qui vient alimenter des chaînes de production avancées, connues sous le nom d’« intelligence artificielle », pour être transformées en produits de prédiction qui anticipent ce que vous allez faire, maintenant, bientôt, plus tard. Enfin, ces

⁸ ZUBOFF Shoshana, *L’âge du capitalisme de surveillance: le combat pour un avenir humain face aux nouvelles frontières du pouvoir*, trad. Bee Formentelli et trad. Anne-Sylvie Homassel, Éditions Zulma, Paris, coll. « Z a », 2022.

*produits de prédiction sont négociés sur un nouveau marché, celui des prédictions comportementales, que j'appelle les marchés des comportements futurs »*⁹.

Ce mémoire de recherche s'inscrit dans la continuité des travaux de Shoshana Zuboff. Shoshana Zuboff à partir d'une analyse durkheimienne et marxiste démontre que le capitalisme a évolué sous une nouvelle forme. Dans sa théorie, ce n'est pas le travail qui est au centre du capitalisme, mais les comportements humains. Les plateformes collectent des informations personnelles sur les utilisateurs. Ces données brutes sont la matière première gratuite qui est ensuite transformée en données comportementales qu'elles vendent. Shoshana Zuboff parle de « surplus comportemental » (ce que Marx appelait la « plus-value ») pour décrire ces données qui sont collectées et exploitées alors même qu'elles ne sont pas l'objectif déclaré de ces firmes. Elles tirent l'essentiel de leur pouvoir économique et politique de ces données et non pas de leur « objet social ». Par exemple, Google est un moteur de recherche mais ses revenus et son pouvoir viennent de sa capacité à exploiter le « surplus comportemental » de millions de personnes.

Shoshana Zuboff résume ainsi : « *L'informatique et l'exploitation des données sur la vie de tout un chacun ne sont pas intrinsèquement couplées (...). Leur catéchisme [aux GAFAM] a beau être d'« organiser les informations à l'échelle mondiale dans le but de les rendre accessibles et utiles à tous », comme l'avait encore asséné le cofondateur de Google, Larry Page (...). Le but véritable est de cibler au plus près le consommateur en lui dérobant des données précises sur ses faits et gestes, afin d'accroître le surplus comportemental et rendre plus efficace la publicité de leurs clients »*.¹⁰

Comme l'explique Shoshana Zuboff « *ce même savoir prédictif provenant du surplus comportemental et qui avait fait la fortune des capitalistes de surveillance pouvait également aider les candidats à gagner les élections »*. Même si elle commence à dessiner les contours et les risques du microciblage politique, elle écrit son ouvrage avant les révélations sur Cambridge Analytica (CA) en 2018. Elle traite seulement de cette question au sein d'un passage expliquant comment Google a réussi à normaliser et institutionnaliser ses pratiques, mais son analyse s'arrête à la

⁹ Ibid.

¹⁰ ZUBOFF Shoshana, « Un capitalisme de surveillance », *Études*, trad. Sean Rose, n° 2, Février, 2021, p. 57-66, [<https://doi.org/10.3917/etu.4279.0057>].

campagne d'Obama. Ce mémoire s'inscrit dans la continuité de sa réflexion en incluant l'analyse du scandale de CA et les élections postérieures.

Le surplus comportemental défini par Zuboff, par la délégation logicielle, est transformé en prédictions permettant d'anticiper les prochains gestes de l'utilisateur, mais aussi d'influencer ses prochaines actions. C'est pourquoi Jérôme Valluy parle de capitalisme de surveillance et d'influence¹¹. Il place au centre de sa réflexion l'enjeu de la protection de la vie privée face à la captation des données personnelles des plateformes. En m'inspirant de cette démarche, nous interrogerons aussi l'impact des plateformes sur la vie privée des utilisateurs. De plus, nous définirons « l'ère numérique » à l'aide des travaux de cet auteur. Ainsi, elle débute dans les années 1970, bien que le numérique commence dès la création des cartes perforées d'Hollerith en 1880. Nous avons choisi de faire débiter l'ère numérique dans les années 1970 car c'est à la fois la période où on constate un engouement commercial avec le développement des premiers géants du numérique comme Microsoft, et un engouement social avec une croissance importante de l'équipement individuel. La notion d'« expansion sociétale » peut être mobilisée pour décrire ce phénomène : « *ensemble des processus sociaux de diffusion dans une société d'une technologie ou d'objets l'incluant (...) ainsi que les transformations induites par cette diffusion dans les comportements humains, leurs façons de communiquer, mais aussi de travailler, de se distraire, de se regrouper, d'apprendre, de penser, etc* »¹². C'est véritablement à partir des années 1990 et l'expansion sociétale d'Internet que l'on rentre dans l'ère du numérique. En effet, pour paraphraser J. Valluy, les transformations induites par l'Internet bouleversent les comportements humains. En 1996, à Davos à lieu la « Déclaration d'indépendance du cyberspace ». Ses auteurs revendiquent un Internet libre de réglementation et anti-étatique, des valeurs qui caractérisent encore les acteurs d'Internet même si leurs discours sont plus édulcorés.

Les attentats du 11 septembre 2001 marquent un tournant, avec un basculement vers la surveillance sécuritaire au détriment des libertés individuelles. Le capitalisme de surveillance s'installe à cette période. Ce n'est pas tant le traumatisme vécu par les Etats-Unis qui expliquent la politique de surveillance des Etats-Unis, que le rôle joué par certains acteurs qui ont vu

¹¹ VALLUY Jérôme, *Sur L'âge du capitalisme de surveillance (2019) de Shoshana Zuboff et sa difficile réception* | Cahiers Costech, [<https://www.costech.utc.fr/CahiersCostech/spip.php?article153>], consulté le 23 novembre 2023.

¹² VALLUY Jérôme, « HUMANITÉ ET NUMÉRIQUE(S) », , 2023.

l'opportunité dans ces événements de légitimer la collecte de données en utilisant l'argument sécuritaire. Avant les attentats du 11 septembre 2001, les Etats-Unis commençaient déjà à pratiquer la surveillance de masse avec le logiciel « Trailblazer »¹³. Après les attentats, la lutte contre le terrorisme est devenue la justification pour collecter des données. Finalement après ce traumatisme, personne n'était en mesure de s'y opposer, ce qui a servi les intérêts de certains acteurs (les GAFAM les premiers) au détriment du droit à la vie privée. En 2013, Edward Snowden a ainsi exposé le travail collaboratif entre la NSA et les GAFAM. Ces révélations ont mis en lumière l'ampleur de la surveillance de masse et la collecte abusive des données personnelles. La NSA accédait librement aux bases de données des GAFAM, qui étaient alors encouragés à collecter toujours plus de données sur leurs utilisateurs du monde entier. La problématique de la collecte de données devient un problème public.

Cinq années plus tard, le scandale de Cambridge Analytica (CA) éclate. Une entreprise de conseil politique spécialisée en science des données a utilisé les données de plus de 50 000 millions d'utilisateurs Facebook en violation des lois de protection des utilisateurs et des conditions générales d'utilisation de Facebook, pour aider Trump à remporter l'élection de 2016. Ces révélations sont notamment le résultat du travail d'enquête de la journaliste Carole Cadwalladr et de l'ancien employé de CA, Christopher Wylie¹⁴. Même si des révélations avaient été préalablement faites en 2015 par The Guardian¹⁵. Au-delà de servir pour améliorer les stratégies de campagne comme Obama a pu le faire en 2008, la science des données sert à manipuler les électeurs. A partir des données récoltées, des prédictions ont pu être élaborées sur les profils psychologiques des citoyens et une stratégie de propagande électorale mise en place en faveur de leurs clients (notamment Trump ou le camp du Leave du Brexit).

La propagande est « *une forme intentionnelle et systématique de persuasion, ayant le but d'influencer les émotions, les attitudes, les opinions et les actions des groupes cibles pour atteindre*

¹³ Jane Mayer, The New Yorker, "The secret sharer", 23 mai 2011 : <https://www.newyorker.com/magazine/2011/05/23/the-secret-sharer>

¹⁴ WYLIE Christopher, *Mindfuck: le complot Cambridge analytica pour s'emparer de nos cerveaux*, trad. Aurélien Blanchard, Bernard Grasset, Paris, 2020.

¹⁵ Harry Davies, « Ted Cruz campaign using firm that harvested data on millions of unwitting Facebook users », The Guardian, 11 décembre 2015 : <https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data>

*des objectifs idéologiques, politiques ou commerciaux, à travers la transmission contrôlée des messages d'information partielle (qui peut être ou ne pas être factuelle) via les canaux directs de masse et des médias. »*¹⁶. La propagande est donc une forme de communication qui cherche à influencer l'opinion. Les manipulations sont le fait de chercher à influencer mais de manière occulte, cachée. Ainsi même si la propagande peut prendre la forme de manipulations, ce n'est pas systématique. La propagande peut être transparente et réglementée comme avec la « propagande électorale » (affiches, professions de foi, etc). On a alors une opposition entre une communication publique et une qui reposerait sur le microciblage. L'avantage de la communication publique c'est que tout le monde y a accès. Le candidat doit alors faire le choix entre communiquer de manière générale pour répondre à la diversité des électeurs, ou s'adresser à un groupe particulier ce qui peut déplaire à certains. Le contenu ciblé ne fonctionne pas de cette manière. Le contenu est personnalisé et individualisé, c'est-à-dire que l'individu ne se rend pas compte que le reste des utilisateurs ne visionnent pas la même chose que lui. Un candidat peut donc faire du clientélisme numérique. La démocratie repose sur le postulat que l'électeur peut faire un choix libre et éclairé. Or les électeurs sont manipulés par ce que Claire Wardle nomme les « troubles informationnels »¹⁷, c'est-à-dire les différents types de contenu mensonger. Les troubles informationnels sont des techniques qui peuvent être employées dans le cadre de manipulation électorale afin de favoriser un candidat, ou de nuire à la réputation de son adversaire.

A l'ère du numérique, la manipulation électorale prend de nouvelles formes. Les manipulations peuvent venir d'acteurs étatiques ou d'entreprises privées. Nous traiterons dans ce mémoire des manipulations électorales mises en place par des entreprises privées, notamment par CA. Le scandale de CA repose sur le vol de données d'utilisateurs Facebook par la firme, or il est nécessaire de dépasser ce cas pour s'intéresser aux facteurs structurels du capitalisme de surveillance qui permettent et encouragent cette collecte de données qui est à la base du microciblage et des manipulations. En effet, le capitalisme de surveillance est basé sur la collecte de données et sa revente sous forme prédictive qui permet le microciblage.

¹⁶ Richard Alan Nelson, *A Chronology and Glossary of Propaganda in the United States*, Greenwood Press, 1996.

¹⁷ Information Disorder Toward an interdisciplinary framework for research and policymaking, Claire Wardle, Hossein Derakhshan, with research support from Anne Burns and Nic Dias, September 2017

Ce mémoire cherche à montrer les liens entre collecte de données, microciblage politique et manipulations et les plateformes. **Comment et dans quelle mesure se met en place un cercle vicieux dans lequel l'utilisation du microciblage politique conduit au renforcement du capitalisme de surveillance ?**

Cette recherche académique a pour objectif de mieux comprendre les enjeux auxquels sont confrontées nos démocraties à l'ère du numérique et du capitalisme de surveillance¹⁸. Cette problématique nous conduira à répondre à plusieurs sous-questions. De quelle manière les données sont-elles collectées ? Et par quels acteurs ? Comment ces données sont-elles utilisées pour influencer les comportements des électeurs ? Ces manipulations sont-elles efficaces ? Et quels acteurs ont un intérêt à ce que les candidats utilisent le microciblage ?

Notre hypothèse principale est basée sur la notion de cheval de Troie mobilisée par Zuboff pour expliquer comment le capitalisme de surveillance peut s'institutionnaliser au sein de la société. Un cheval de Troie désigne une manœuvre d'infiltration. Dans le cadre de ce mémoire, nous postulons que le microciblage politique est le cheval de Troie du capitalisme de surveillance. Le microciblage politique permet de cibler les électeurs susceptibles d'être influencés par des publicités personnalisées. Ces dernières ont pour objectif de faire voter en faveur du candidat, ou d'inciter à ne pas voter pour son adverse. Les bénéficiaires de ces manipulations sont donc les candidats politiques s'ils gagnent l'élection et CA par la même occasion qui peut capitaliser cette victoire dans son argumentaire de vente (notamment pour intégrer le marché privé plus lucratif). Mais ce sont surtout les plateformes qui bénéficient de l'usage du microciblage politique. Elles deviennent indispensables aux campagnes électorales et aux candidats et peuvent continuer de collecter des données qui sont l'élément fondateur de leur modèle économique puisque les candidats en dépendent pour leur campagne. Comment des candidats politiques qui ont utilisés le microciblage pour cibler des électeurs peuvent-ils ensuite en limiter l'utilisation et avoir un regard critique dessus alors même qu'ils n'auraient peut-être pas gagné sans ?

¹⁸ Shoshana Zuboff, *"L'âge du capitalisme de surveillance"* (2018)

Pour prouver cette hypothèse, notre démarche de recherche est basée sur la construction d'un corpus de texte composé de trois sources principales : le livre de B. Kaiser¹⁹, qui travaillait pour CA lors de l'élection de Trump et du brexit-, les *leaks* (fuite d'informations) sur CA, les articles des journalistes sur le sujet mais plus majoritairement sur ceux de Carole Cadwalladr qui a révélé le scandale Facebook/ CA. En complément, nous nous intéresserons aussi à la réponse ou au silence du droit et aux enquêtes en sciences sociales sur l'efficacité des manipulations et de la propagande. Nous avons fait le choix stratégique de ne pas faire d'entretiens dans le cadre de cette recherche. Cette recherche a pour objectif de parvenir à une vision englobante du capitalisme de surveillance et de l'utilisation du microciblage. L'entretien pourrait être pertinent pour aller plus loin, d'un point de vue plus micro-sociétale, en s'intéressant par exemple aux pratiques de travail des cabinets de conseil et aux équipes de campagne mais il n'est pas apparu comme nécessaire dans l'angle de recherche choisi dans ce mémoire.

Ainsi, j'ai choisi pour obtenir des données empiriques de me baser essentiellement sur le témoignage de Brittany Kaiser, et ce pour plusieurs raisons. D'abord, elle a été bénévole durant la campagne de Obama, elle compare donc les outils de data-analyse employés par les équipes d'Obama et ceux de CA. Elle a travaillé pour CA pendant la campagne de Trump et le Brexit, à la différence de Christopher Wylie qui avait déjà quitté la firme. Enfin, elle met en avant les relations et les imbrications entre les acteurs économiques, politiques, médiatiques et les plateformes ce qui est essentiel pour comprendre comment le microciblage est au cœur du capitalisme de surveillance. D'ailleurs, le titre anglais de son témoignage est « targeted » qui signifie « ciblé ». Néanmoins, son témoignage ressemble par moment à une justification pour excuser sa participation à ces événements. Elle est considérée comme une « lanceuse d'alerte » en France, par une mauvaise traduction du concept américain de « whistleblower ». Elle n'a pas lancé l'alerte sur les pratiques de CA, elle n'a dénoncé ces agissements qu'une fois licenciée, tout comme Wylie. Nous préférons donc les appeler des « informateurs ». Même si elle n'a pas alerté sur les pratiques de CA, ses dénonciations permettent d'accéder à de nombreuses informations sur CA. Elle est ainsi à l'origine d'une fuite de données sur CA.

¹⁹ WYLIE Christopher, *Mindfuck*, op. cit., 2020 ; KAISER Brittany, *L'affaire Cambridge Analytica, Les dessous d'un scandale planétaire*, Harpercollins., 2020.

Le compte anonyme à l'origine de la fuite de données sur Twitter est « Hindsight is 2020 ». Le choix du pseudo n'est pas anodin, puisque cette expression signifie « revenir sur un événement passé avec un regard plus éclairé sur la situation ». Il est maintenant de notoriété publique que ce compte est tenu par B. Kaiser comme le révèle rapidement The Guardian²⁰. Au total, cela fait plus d'un millier de page de documents à étudier, nous avons alors choisi de nous concentrer dans le cadre de ce mémoire sur les leaks concernant les Etats-Unis et plus précisément la communication de CA pour vendre ses services.

L'étude des articles des journalistes, et notamment sur ceux de Carole Cadwalladr qui a révélé le scandale Facebook/ CA ont été nécessaire à l'écriture de ce mémoire. Journaliste d'investigation, elle écrit pour The Guardian et The Observer. Elle a enquêté pendant plus d'un an sur CA avant d'en faire les révélations en 2018 avec l'aide de C. Wylie.

Pour répondre à notre problématique, nous diviserons notre objet d'étude en trois parties : les révélations sur CA, l'efficacité des manipulations et du microciblage, et le renforcement du capitalisme de surveillance.

L'affaire Cambridge Analytica a mis en lumière les pratiques de collecte de données numériques. Issue de l'influence conjuguée de Google et du manque de solution proposée à droite du champ politique, Cambridge Analytica a été exposée par un scandale révélateur de ses méthodes. Cependant, ces pratiques ne se limitent pas à une seule entreprise ; elles sont le modèle même des plateformes et sont répandues à travers l'utilisation généralisée des cookies sur le web. Au-delà de la question de la collecte des données, le témoignage de B. Kaiser nous permet d'analyser les manipulations électorales numériques mises en place par la firme. Nous proposerons une typologie de troubles informationnels, alimentés par des mécanismes de propagation sophistiqués tels que les usines à trolls, les bots et les algorithmes créant des chambres d'écho et des bulles de filtre (I).

Malgré ces révélations, l'efficacité des manipulations électorales numériques est sujette à un débat récurrent au sein des sciences sociales. Ce débat oppose les tenants du poids des structures sociales sur le vote à ceux qui insistent sur l'impact de la campagne politique. Certes, les structures déterminent encore majoritairement le vote des électeurs, mais le nombre d'électeurs augmentent, or ils sont les plus sensibles aux campagnes politiques et à leurs influences. Les partis misent alors

²⁰ <https://www.theguardian.com/uk-news/2020/jan/04/cambridge-analytica-data-leak-global-election-manipulation>

sur ces électeurs pour remporter les élections en déployant des méthodes issues du marketing. Le microciblage politique émerge alors comme un outil majeur de l'efficacité des manipulations numériques, exploitant le consentement non-éclairé des utilisateurs à la collecte de leurs données et à la publicité ciblée. Bien que contesté, le microciblage présente des preuves indirectes de son efficacité (II).

Les grands bénéficiaires de l'utilisation du microciblage politiques sont les plateformes du numérique, les GAFAM notamment. Leur système économique repose sur le surplus comportemental qui alimente des modèles prédictifs à l'origine du microciblage publicitaire. C'est par le microciblage politique que les entreprises accèdent au marché commercial privé bien plus lucratif. En participant à la victoire d'un candidat, ces firmes peuvent prouver leurs résultats et l'efficacité de leur influence, dès lors elles peuvent promouvoir leurs services dans le champ privé lucratif. Les GAFAM sont devenus des acteurs incontournables dans cette équation. Ils sont indispensables aux cabinets de conseils et aux candidats politiques qui dépendent de leurs données. Les relations entre GAFAM et l'Etat sont très poreuses, ce qui permet une influence des GAFAM sur la construction du droit. L'Etat et les politiques facilitent l'institutionnalisation du capitalisme de surveillance à travers une politique du laisser-faire provoquée par leur dépendance au microciblage et aux données (III).

I. Les données aux fondements du microciblage et des manipulations électorales

Dans la première partie de ce mémoire, nous étudierons la collecte des données qui sont au fondement du microciblage et des manipulations électorales numériques.

Au début de ce questionnement se trouve l'affaire Cambridge Analytica. Scandale révélé en 2018, il a mis au centre de l'actualité la question de la collecte des données numériques des utilisateurs et les risques de violation de leur droit à la vie privée.

Nous débiterons par retracer l'ascension de Cambridge Analytica depuis sa genèse, en insistant sur l'influence de Google et des Républicains dans son développement. Par la suite, nous examinerons les révélations des pratiques de Cambridge Analytica qui ont mis en lumière les pratiques obscures de collecte de données. Il est cependant nécessaire d'aller au-delà de Cambridge Analytica. Des plateformes ont des pratiques similaires en matière de collecte des données, sans que cela ne fasse scandale. L'utilisation généralisée des cookies à travers le web souligne ainsi l'ampleur du problème (A).

Cambridge Analytica, au-delà de la collecte frauduleuse des données des utilisateurs Facebook, est aussi critiquée pour son influence dans les élections américaines de 2016 et le Brexit. Les leaks des informateurs permettent de comprendre les mécanismes complexes des troubles informationnels mis en place par la firme. Après avoir proposé une définition précise de ces

troubles, nous en proposerons une typologie basée sur le travail de Claire Wardle. Les manipulations et leur influence est amplifiée par différents mécanismes comme les usines à trolls, les bots et les algorithmes, qui créent des chambres d'écho et des bulles de filtre sur les réseaux sociaux (B).

A. L'affaire Cambridge Analytica révélatrice des pratiques de collecte des données numériques

Cambridge Analytica (CA) est un cabinet de conseil spécialisé dans la collecte de données et la prédiction de comportement à des fins politiques et commerciales. En 2018 éclate le scandale Cambridge Analytica qui révèle son existence et ses pratiques (1). Alors que les médias, les électeurs, et les gouvernements se sont focalisés sur cette affaire, il est nécessaire de rappeler que ces pratiques ne se limitent pas à cette firme (2).

1. De la genèse de Cambridge Analytica au scandale

Cette partie de mon mémoire a été rédigée à partir des informations récoltées par le témoignage de Brittany Kaiser dans la version originale de son livre « Targeted »²¹, et vérifiées ensuite par différentes sources (articles journalistiques et articles d'universitaires). Bien que l'ouvrage de Kaiser ressemble souvent à une tentative de justification de sa part pour excuser publiquement sa participation à la société, les événements, les dates, et les liens entre les différents acteurs politiques et économiques sont bien retranscrits dans son témoignage, et ont été confirmés par les journalistes d'investigation comme Carole Cadwalladr. Elle explique ainsi que CA a été inspirée par Google, et les raisons pour lesquelles CA a travaillé pour le camp républicain (a). Elle revient également sur les premières révélations sur CA lors de la campagne de Ted Cruz (b).

a) La genèse de Cambridge Analytica : l'influence de Google et des Républicains

CA est une société britannique fondée à l'initiative de Alexander Nix. C'est une filiale du groupe SCL (acronyme de Strategic Communication Laboratories).

²¹ KAISER Brittany, *L'affaire Cambridge Analytica*, op. cit., 2020.

Alexander Nix a l'idée de créer cette filiale en 2013 alors que Sophie Schmidt, la fille du PDG de Google -Eric Schmidt- était en stage à SCL. La jeune femme lui aurait alors présenté et expliqué les différents outils mis en place par Google et notamment Google Analytics. Ce service de la firme collecte et analyse les données des utilisateurs de Google, à l'aide de cookies. Ainsi, ils disposent d'un nombre très important de données sur les personnes partout dans le monde, et peuvent fournir des visualisations et des mesures en temps réel aux site-webs clients. Les clients peuvent alors avoir accès au nombre de clics sur un lien, le temps passé à lire un article, etc., leur permettant d'ajuster leurs stratégies en fonction du taux d'engagement d'un contenu.

Nix, en utilisant les informations fournies par Sophie Schmidt eut l'idée de créer une société capable d'utiliser de tels outils d'analyse de données. Cela s'alignait avec la stratégie du groupe SCL issu du BDI (Behavioural Dynamics Institute) créé en 1989 par Nigel Oakes – un Britannique ayant fait sa richesse dans le domaine de la publicité. Ce consortium de soixante institutions et de plus d'une centaine d'experts en psychologie travaillait sur les manières d'influencer les comportements à l'aide de la communication en se basant sur la psychologie (ex : réduire la violence). Le BDI avait notamment travaillé avec des services de la défense, et avait aidé à stopper la violence en Afrique du Sud en 1994 permettant l'accession au pouvoir de Nelson Mandela. SCL a, après les attentats du 11 septembre 2001, été recruté par des gouvernements (américain, britannique...) et l'ONU pour lutter contre le terrorisme. A ce moment, les données dont disposait le groupe étaient encore peu abondantes et pas spécialement de bonne qualité, elles étaient issues de sondages téléphoniques ou de porte à porte.

Alexander en créant Cambridge Analytica avait pour ambition d'utiliser les données issues du numérique comme le faisait Google, mais avec leurs connaissances en psychologie afin de prévoir les comportements électoraux et les influencer.

Il s'est orienté vers le camp républicain aux Etats Unis pour deux raisons stratégiques – et non-idéologiques. D'abord, il a fait le choix d'agir aux Etats-Unis où les lois sur la collecte et l'utilisation des données étaient inexistantes (ou presque). Les données personnelles n'étaient pas protégées comme faisant partie de la vie privée des utilisateurs et le consentement des utilisateurs n'était pas toujours requis. Ensuite, il a choisi de vendre ses services au camp républicain, car le camp démocrate avait déjà des solutions numériques depuis la campagne de Barack Obama de 2008 et de 2012. Kaiser cite cinq grandes firmes au service des démocrates : Blue State Digital,

BlueLabs, NGP VAN, Civis Analytics (fondé par Éric Schmidt), and HaystaqDNA. Le marché électoral était donc saturé à gauche, ce qui a laissé la voie ouverte à droite pour CA. Il est nécessaire de noter tout de même qu'au-delà de ses justifications commerciales, CA est financé par des acteurs idéologiquement situés à droite (voir l'extrême droite) aux Etats-Unis comme Robert Mercer ou Steve Bannon qui ont favorisé une clientèle républicaine.

CA a ainsi participé à la Campagne de Ted Cruz en 2016 pour les mid-terms. Puis pour la campagne du sénateur pour les primaires républicaines. Celui-ci était alors peu connu, voir peu apprécié. Un autre sénateur nommé Lindsey Graham aurait ainsi affirmé que « si quelqu'un tire sur Ted Cruz, personne au Sénat ne condamnerait son meurtrier ». ²² Néanmoins, il crée la surprise en remportant l'Iowa et le Texas lors de la primaire. Kaiser écrit à son sujet ²³ :

« Petit à petit, les efforts de Cambridge ont porté leurs fruits. Lors des premiers tests, Alexander s'est vanté d'une augmentation de plus de 30 % des performances des messages de la campagne de Cruz. Davantage de personnes ont commencé à connaître et à reconnaître le candidat, et finalement beaucoup de ces personnes ont commencé à changer d'avis. Ils cliquaient, rejoignaient la campagne et faisaient des dons en masse. La viabilité de Cruz en tant que candidat républicain a commencé à devenir une réalité, et les politiciens ont commencé à remarquer Cambridge Analytica. » ²⁴

Ainsi, bien que le candidat n'ait pas pu remporter la primaire, CA a réussi à en faire un acteur important et à lui créer une base de sympathisants évangélistes grâce au microciblage et à la publicité personnalisée.

²² <https://edition.cnn.com/2016/02/26/politics/lindsey-graham-ted-cruz-dinner/index.html>

²³ KAISER Brittany, *L'affaire Cambridge Analytica*, op. cit., 2020.

²⁴ Traduit avec DeepL.com (version gratuite) à partir de la citation d'origine « *Little by little, Cambridge's efforts succeeded. In early testing, Alexander boasted of a higher-than-30-percent uplift in performance for Cruz's campaign messaging. More people started to know and recognize the candidate, and eventually many of those people began to change their tune. They were clicking through, joining the campaign, and donating en masse. Cruz's viability as the Republican nominee began to become a reality, and people in politics started to notice Cambridge Analytica.* »

Dès 2015, et la participation de CA à la campagne de Ted Cruz, les médias commencent à s'intéresser aux pratiques de la firme et les dénoncer (2).

b) Les révélations des pratiques de Cambridge Analytica

Cette partie est basée à la fois sur l'ouvrage de B. Kaiser qui relate les premières révélations dans son témoignage, et sur les différents articles de journalistes ayant révélé le scandale CA et mis en lumière des « lanceurs d'alerte ».

En juillet 2015, le journal Politico est le premier journal à écrire au sujet de CA dans son article titré « Ted Cruz s'associe à la société "psychographique" d'un donateur »²⁵ de Kenneth P. Vogel et Tarini Parti. Cet article revient sur les modalités de financement de la campagne de Ted Cruz et de financement de la firme CA, mais rien n'est écrit au sujet des données et du microciblage.

C'est le journal The Guardian qui est le premier à révéler la manière dont CA a acquis ces données. L'article écrit par Harry Davies est publié en décembre 2015 : « Exclusif : Des documents révèlent qu'une entreprise américaine financée par des donateurs et intégrée à la campagne républicaine a payé des universitaires britanniques pour collecter des profils psychologiques sur des électeurs potentiels ».²⁶

L'auteur aurait eu accès à des documents montrant que CA aurait acquis ces données sur Facebook de manière illégitime en violation des termes d'utilisation de la plateforme. En réalité, Facebook permettait jusqu'en avril 2015 d'accéder à un outil tiers nommé « Friends API ». Cet outil permettait à une application tierce comme Candy Crush de récolter les données de celui qui y joue via Facebook avec son consentement, mais aussi -et sans leur consentement- celles de ses amis. En effet, l'utilisateur accepte les termes des services pour accéder au jeu, permettant à l'application de récolter ses données, ce n'est cependant pas le cas des amis de l'utilisateur. Dans le cas de CA, le Dr Aleksandr Kogan, universitaire à l'Université de Cambridge, a fait passer un

²⁵ Kenneth Vogel, « Cruz partners with donor's 'psychographic' firm », Politico, 7 juillet 2015 : <https://www.politico.com/story/2015/07/ted-cruz-donor-for-data-119813>

²⁶ Harry Davies, « Ted Cruz campaign using firm that harvested data on millions of unwitting Facebook users », The Guardian, 11 décembre 2015 : <https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data> dont la citation est extraite et traduite à l'aide du logiciel DeepL “*“Exclusive: Documents reveal donor-funded US startup embedded in Republican's campaign paid UK university academics to collect psychological profiles on potential voters”*”.

test de psychologie à des utilisateurs Facebook en échange d'une rémunération d'1\$. Ces données devaient être récoltées à des fins de recherches académiques mais il les a revendus à CA. Pourtant les utilisateurs n'ont pas consenti à fournir leurs données dans un objectif commercial. Cet article met en avant la responsabilité de CA mais pas de Facebook qui permettait jusqu'en 2015 de récolter les données de ses utilisateurs sans leur consentement.

L'article lors de sa publication a fait réagir aux Etats-Unis. Mais il n'a pas provoqué de scandale, et n'a pas traversé l'Atlantique. C'est seulement en 2018 que le scandale éclate véritablement, soit après le Brexit et l'accession de Donald Trump à la présidence des Etats-Unis.

En 2017, Carole Cadwalladr ainsi que Jamie Doward publient leur premier article sur CA intitulé « L'organisme de surveillance lance une enquête sur l'utilisation abusive des données en politique ».²⁷ Carole Cadwalladr continue d'enquêter sur la firme durant l'année 2017 et prend contact avec Chris Wylie. En 2018, elle publie une enquête commune avec the New York Times sur CA et Facebook, avec l'aide du « lanceur d'alerte » : « Révélation : 50 millions de profils Facebook récoltés pour Cambridge Analytica dans le cadre d'une importante violation de données »²⁸. L'article revient en détail sur la manière dont CA a récolté les données, notamment en volant les données de 50 millions d'utilisateurs Facebook avec l'aide de l'application Friends API, mais aussi sur les liens entre CA et le Brexit, et leur rôle dans l'élection de Trump.

A partir de cette date le scandale prend réellement de l'ampleur. Alexander Nix, Brittany Kaiser, Mark Zuckerberg ont été reçus par le Parlement britannique pour revenir sur le rôle de CA et de Facebook dans le referendum du Brexit, et sur la collecte de leurs données. Par la suite de, Brittany Kaiser devient à son tour « lanceuse d'alerte ». Elle fera fuiter des « leaks » de CA permettant aux journalistes de mieux comprendre les manipulations mises en place par CA. Elle avancera que 68 élections auraient été manipulées par CA²⁹. Nous n'avons néanmoins pas réussi à trouver une liste complète de ces pays ni dans les articles de journalistes, ni dans les leaks (Cf. Annexe n°7).

²⁷ Jamie Doward, Carole Cadwalladr, *Watchdog to launch inquiry into misuse of data in politics*, The Guardian, 4 mars 2017 : <https://www.theguardian.com/technology/2017/mar/04/cambridge-analytics-data-brexit-trump>

²⁸ Carole Cadwalladr, Emma Graham Harrison, *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*, The Guardian, 17 mars 2018 : <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>

²⁹ <https://www.la-croix.com/Monde/Scandale-Cambridge-Analytica-68-pays-victimes-propagande-electorale-2020-01-08-1201070529>

CA ainsi que sa société mère SCL sont mises en faillite en mai 2018, ce qui empêche le travail d'enquête et les poursuites à l'encontre des deux firmes. Par ailleurs, bien que CA ait assuré en 2015 avoir supprimé les données conflictuelles, il est probable, comme Facebook ne s'en est pas assuré, que les données aient été transmises à Emerdata. Société fondée en 2017 par SCL, Emerdata héberge à sa direction les fondateurs et cadres de CA et SCL. Il est alors possible de faire l'hypothèse que la création de cette société prévoyait de regrouper les sociétés CA et SCL après les premières publications journalistiques en 2015, afin d'échapper à de probables poursuites judiciaires³⁰.

De son côté Facebook est condamné à une amende de 500 000£ (565 000€) – plafond prévu par la loi- par l'Information Commissioner's Office. Par la suite, l'agence américaine de protection des consommateurs leur infligera une amende de 5 milliards de dollars en 2019. Enfin, en 2021, Facebook devient Meta. En 2022 la plateforme paie 725 millions de dollars pour clore l'action collective engagé en 2018 à son encontre, sans reconnaître pour autant avoir commis une infraction.

Alors que les médias et la justice se sont concentrés sur l'affaire CA, d'autres auteurs comme Ivan Manokha mettent en avant que les pratiques des plateformes sont tout aussi contestables (2).

Brittany Kaiser et Chris Wylie sont-ils des « lanceurs d'alerte » :

Dans le « dictionnaire de la Participation », Francis Chateauraynaud – sociologue- définit le lanceur d'alerte et le whistleblower.

*« 1. Toute personne, groupe ou institution qui, percevant les signes précurseurs d'un danger ou d'un risque, interpelle une ou plusieurs puissances d'action, dans le but d'éviter un enchaînement catastrophique, avant qu'il ne soit trop tard.
2. Toute personne ou groupe qui rompt le silence pour signaler, dévoiler ou dénoncer des faits, passés, actuels ou à venir, de nature à violer un cadre légal ou réglementaire ou entrant en conflit avec le bien commun ou l'intérêt général. Ce second sens est plus proche du mot anglais*

³⁰ Pascale Boyen, Courrier International, 3 mai 2018 : <https://www.courrierinternational.com/article/cambridge-analytica-une-vraie-fausse-faillite>

*whistleblower – dont l’expression de lanceur d’alerte n’est cependant pas la traduction directe. »*³¹

Selon la première définition -conception française du lanceur d’alerte- Kaiser et Wylie ne le sont pas. En effet, Wylie dénonce les actions de CA une fois le Brexit et l’élection de Trump, et surtout après que des articles aient déjà été publiés en 2015 sur le sujet. De la même manière, Kaiser ne devient lanceuse d’alerte qu’après avoir été limogée de CA, et que Wylie ait commencé à prendre la parole publiquement. Ces deux acteurs connaissaient les dangers et les limites de CA, pourtant ils n’ont pris la parole qu’une fois les révélations commencées.

Mais selon la seconde définition, ils pourraient être qualifiés de whistleblower. Ils ont en effet dénoncé des faits passés qui violaient la loi et entraient en conflit avec l’intérêt général.

Il serait alors préférable de parler de « dénonciateurs » ou d’informateur plutôt que de lanceurs d’alerte dès lors qu’ils n’ont pas « sonné l’alarme ».

2. Au-delà de Cambridge Analytica

Il est nécessaire de dépasser le cadre de Cambridge Analytica qui a focalisé les discours, pour mettre en lumière les pratiques tout aussi contestables des plateformes en matière de collecte des données (a), et plus généralement sur le web dans sa globalité avec l’usage généralisé des cookies (b).

a) Les pratiques similaires des plateformes

Ivan Manokha écrit « *nous pouvons constater que la différence entre les méthodes des plateformes numériques et celles auxquelles a eu recours Cambridge Analytica n’est pas très significative* »³². Selon l’auteur, seuls les procédés employés par CA sont considérés comme

³¹ Francis Chateauraynaud, « Lanceur d’alerte », *CASILLO I. et alii (dir.), Dictionnaire critique et interdisciplinaire de la participation, Paris, GIS Démocratie et Participation, 2013*

³² MANOKHA Ivan, « Le scandale Cambridge Analytica contextualisé », *op. cit.*, 2018, p. 39-59.

illégaux, ce qui expliquerait la différence de traitement. Néanmoins il est possible de faire l'hypothèse que ce n'est pas seulement en lien avec l'illégalité des pratiques de CA. CA a été accusé dès 2015 d'avoir volé des données, mais le scandale n'intervient qu'en 2018, après l'élection de Trump et le Brexit. Ces deux scrutins ont surpris dans la mesure où le camp adverse était annoncé gagnant par les sondages. Il a alors fallu chercher des justifications *ad hoc* à ces victoires, et certains y ont vu l'opportunité de contester les résultats. Ces deux élections ont été un séisme dans le monde provoquant une forme de traumatisme pour de nombreux citoyens. Il est donc probable que le scandale résulte plus de la participation de CA à ces élections corrélé au vol de données, que la violation même de la vie privée des utilisateurs.

Comme l'explique Manokha, les données collectées par CA ne sont « *qu'une goutte d'eau en comparaison du volume d'informations que le capital de plateforme recueille sans cesse* »³³. La faillite de CA ne conduit donc à aucune amélioration pour l'utilisateur dont les données demeurent pillées en permanence par les plateformes afin de les vendre à des tiers. La collecte des données et leur monétisation n'est pas remise en cause par le scandale, le débat est déplacé sur la légitimité du scrutin et du candidat. Le SCA n'a pas permis d'ouvrir le débat sur le capitalisme de surveillance. Pourtant la collecte de données affaiblit le droit à la vie privée, que ce soit par les institutions – notamment les autorités chargées de la sécurité et de la surveillance- ou les entreprises privées. La vie privée est pourtant un droit fondamental, il est inhérent à la personne et inaliénable. Lui porter atteinte, c'est porter atteinte à la dignité humaine qui est le principe fondateur des droits humains. Ainsi, réduire le droit à la vie privée compromet aussi d'autres droits et libertés comme celle d'expression, d'information, ou de pensées mais aussi le droit de se rassembler. La Chine en est un exemple flagrant, le système de crédit social collecte de nombreuses données sur les individus permettant au gouvernement et aux entreprises de limiter l'accès à certains droits et services. Un crédit côté « D » signifie que le citoyen ne peut plus acheter de billets d'avion et de train, ni acheter de biens immobiliers, ou se rendre dans certains restaurants et hôtels. La vie privée est ainsi un droit fondamental à protéger pour demeurer dans un régime démocratique. Manokha conclut « *en somme, tant que les plateformes perdureront, les invasions régulières de la sphère privée, indispensables au fonctionnement du capital de plateforme subsisteront, et l'idée selon laquelle les données sont une marchandise dont la possession peut générer des revenus deviendra de plus en*

³³ *Ibid.*

plus objectivée et normalisée »³⁴. Le modèle économique des plateformes ne peut subsister sans violer le droit à la vie privée des utilisateurs car la collecte de données en est le fondement même.

Les plateformes ne sont cependant pas les seules à collecter les données personnelles des individus. Les données étant partout dans le monde numérique, la question est bien plus globale (b).

b) L'usage des cookies à travers le web

CA n'a pas seulement collecté ses données à l'aide de l'application Friends API sur Facebook. La majorité des datas sont collectées via l'usage des cookies lors de la navigation web de l'utilisateur. Avant le RGPD, les cookies étaient d'office considérés comme acceptés par l'utilisateur. Dorénavant dans l'Union européenne, les utilisateurs doivent décider s'ils acceptent ou non l'utilisation de cookies sur le site web qu'ils consultent. Les cookies sont une forme de logiciel espion dans la mesure où ils permettent de suivre tout ce que l'utilisateur fait sur le site internet. L'utilisateur accepte les cookies pour accéder à un service sans se rendre compte que ses données sont collectées, mais surtout partagées à des tiers.

La CNIL a développé une application nommée CookieViz qui permet de voir qui accède aux cookies de navigation d'un site web et propose une représentation graphique de ces acteurs. En utilisant cette application, j'ai cherché le journal français « Le Point » et j'ai ouvert l'un des premiers articles d'actualité. L'application me révèle alors que mes cookies sont partagés à 46 tiers dont plus de la moitié ne serait pas déclaré dans les fichiers ads.txt du site Le Point. Ces fichiers permettent pourtant de déclarer avec quels prestataires publicitaires travaille l'éditeur. Mes données ont été partagées à 46 groupes tiers et cela en seulement une minute de navigation internet. Ainsi, des heures et des heures par jour de navigation fournissent une quantité inestimable de données.

³⁴ *Ibid.*

Votre navigation

Vous avez visité 2 sites.

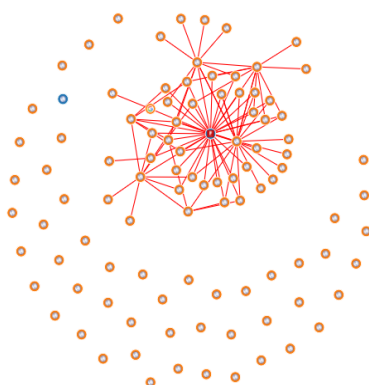
50% d'entre eux ont déposé au moins un cookie.

Ces cookies **échantent** potentiellement des informations avec 46 domaines tiers.

Usage des cookies

La **zone orange** indique la couverture de tiers déclarés comme publicitaires dans les fichiers ads.txt des sites visités.

La **zone violette** indique la couverture des tiers non déclarés dans les fichiers ads.txt des sites visités.



Présence des tiers

Usage des cookies

Qu'importe le support utilisé, que cela soit en lisant un livre sur une tablette, en navigant sur internet, en achetant un jeu sur le store d'une console, en commandant à manger via une plateforme de livraison, ou encore un aspirateur ou frigo connecté -etc- des données sont collectées. Absolument chaque trace numérique fournit un nombre de données incalculables : préférence alimentaires/sexuelles/politiques/littéraires/etc., temps de lecture d'un livre/à quel endroit le lecteur s'est arrêté/etc., tous les achats en ligne, les données socio-démographiques, localisation, etc... Cela permet *in fine* aux entreprises de tout connaître des utilisateurs grâce à ces données comportementales. Kaiser explique ainsi dans son ouvrage que le problème n'est pas que CA : « *Le problème était plus grand que CA, le problème était les Big Data* »³⁵.

³⁵ Extrait de "KAISER Brittany, *L'affaire Cambridge Analytica*, op. cit., 2020" et traduit par DeepL à partir de la citation suivante "The problem was bigger than Cambridge; the problem was Big Data".

En résumé, les révélations sur CA à la fois des journalistes et des dénonciateurs mettent en avant les violations du droit à la vie privée des utilisateurs face aux pratiques de collecte des données de CA. Mais les experts du numérique préviennent que les données des utilisateurs sont collectées et vendues à partir de n'importe quelle plateforme. Cela permet de dépasser le cadre du vol de données de CA sur Facebook. La collecte de données sur le web est généralisée, mettant en danger le droit à la vie privée des utilisateurs.

Les révélations sur CA ne concernent pas uniquement la collecte frauduleuse de données mais aussi les pratiques manipulatoires mises en place par la firme, notamment dans le cadre de la campagne de Trump en 2016 et du Brexit (B).

B. Les mécanismes au service des manipulations électorales numériques

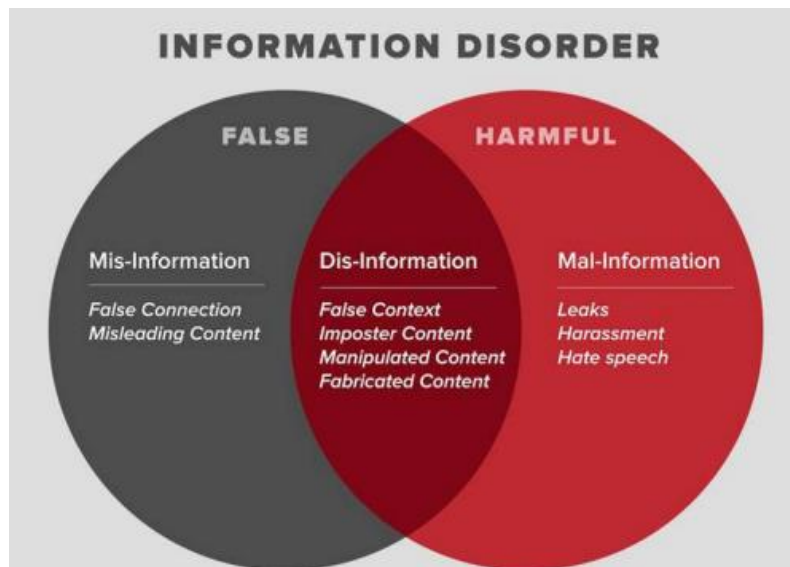
Les manipulations numériques sont les différentes méthodes employées pour influencer de manière malhonnête une élection. En effet, il est normal dans le cadre de la compétition politique de chercher à influencer le comportement des électeurs, cela se fait traditionnellement en cherchant à convaincre l'électeur que le programme de tel ou tel candidat est le meilleur pour lui, et qu'il est donc nécessaire de voter en sa faveur le jour du scrutin. Ainsi, la propagande électorale est légale, des affiches, des tracts, les discours, etc. permettent aux candidats de porter publiquement leurs programmes. Néanmoins, la manipulation intervient à partir du moment où la tentative d'influence est cachée. Celui à l'origine de la manipulation cherche à privilégier un candidat sans le dire clairement, ses intentions sont obscures. Les manipulations électorales relèvent de stratagèmes, c'est-à-dire de ruse pour tromper la personne qui en est la cible, dans le cadre d'une élection. Dès lors, les manipulations peuvent être protéiformes, d'où la nécessité de les définir en se basant sur la notion développée par Claire Wardle sur les troubles informationnels et d'en proposer une typologie (1). Ces manipulations ont une ampleur importante en raison de stratégies et de mécanismes spécifiques, mettant en avant le rôle des algorithmes des réseaux sociaux et l'influence des bots (2).

1. Typologie des troubles informationnels

Après avoir proposé une définition des troubles informationnels en s'appuyant sur les travaux de Claire Wardle (a), nous proposerons une typologie sous forme de tableau (b).

a) Définition

Les troubles informationnels sont selon Claire Wardle - auteure du rapport du Conseil de l'Europe sur les désordres informationnels³⁶ - différents types de contenu mensonger.



Dans ce rapport, les auteurs décident d'écarter le terme de « fake news » trop galvaudé. À la place, ils distinguent trois types d'« information disorder » (troubles informationnels) : la « mis-information », la « dis-information » et la « mal-information ».

La « mis-information » est une information trompeuse, tout comme la « dis-information » mais à la différence qu'elle ne vise pas à faire du mal, c'est une information erronée mais sans intention malhonnête (une erreur de date, une satire prise sérieusement, une erreur dans les statistiques, une mauvaise traduction, etc).

³⁶ [*Information disorder: Toward an interdisciplinary framework for research and policy making*](#) (le schéma "Information Disorder" à la page suivante est issu de ce rapport)

Les auteurs distinguent dans les pratiques de « dis- et mis- information » sept niveaux de trouble informationnel³⁷.



³⁷ <https://fr.ejo.ch/deontologie-qualite/cinquante-nuances-desinformation-fakenews-trouble-information-claire-wardle-manipulation>

contexte ». Le contenu est véridique mais le cadrage est trompeur. Par exemple la photo d'un éboueur se reposant a circulé sur les réseaux sociaux avec la phrase « Voilà à quoi servent les impôts locaux des Parisiens à payer les agents de propreté à roupiller, on comprend pourquoi Paris est si dégueulasse »³⁸. Le salarié a été licencié à la suite de la polémique. Pourtant le salarié était en réalité en pause et a terminé sa tournée à l'heure. Le cinquième niveau est celui du « contenu imposteur », qui fait partie de la dis-information. Les informations trompeuses arborent le visuel de médias reconnus pour donner de la crédibilité à l'information. Le sixième niveau concerne les contenus manipulés qui se basent sur un contenu authentique mais le modifie à des fins trompeuses. Enfin le dernier niveau est celui des contenus fabriqués et donc entièrement faux, ce que désigne le terme « fake news » à l'origine. On peut aussi citer les « deepfake ».

A partir de ces éléments, nous pouvons construire une typologie sous forme de tableau des troubles informationnels sur les réseaux sociaux en tenant compte des distinctions faites par les auteurs³⁹ (b).

b) Typologie

Stratégies manipulatoires		Méthodes	Effets
Mésinformations	Partage d'une information fausse mais sans voir sa nature trompeuse		Propagation de fausses informations involontairement
	Satire ou parodie	Partage d'une information fausse sur le ton de la moquerie	Peut induire involontairement en erreur

³⁸ <https://www.leparisien.fr/seine-saint-denis-93/gagny-paris-l-affaire-de-l-eboueur-licencie-pour-une-photo-de-sieste-fait-scandale-sur-les-reseaux-14-01-2020-8236080.php>

³⁹ Information Disorder Toward an interdisciplinary framework for research and policymaking, Claire Wardle, Hossein Derakhshan, with research support from Anne Burns and Nic Dias, September 2017

	Fausse connexion	Ecart entre le titre et le contenu de l'article, ou les visuels	Attirer les lecteurs avec un titre aguicheur
	Contenu trompeur	Utilisation trompeuse d'informations pour formuler un problème	Mettre en avant un argument dans un débat à partir d'informations trompeuses
	Sans contexte	Une information véritable est partagée mais sans le contexte	Cadrer une information d'un certain point de vue qui serait différent avec le contexte
Désinformations	Faux contexte	Une information véritable est partagée mais avec un contexte faux (Cf Annexe n°00)	Cadrer une information de manière malhonnête pour manipuler l'effet produit
	Contenu imposteur	Une source authentique est usurpée (Cf annexe n°3)	Donner l'impression d'être une source fiable
	Contenu manipulé	Contenu authentique mais modifié sans le notifier aux utilisateurs	Faire croire qu'une personne a fait ou dit quelques chose
	Contenu fabriqué	Créer et partager sciemment des faits inventés, de fausses déclarations, des événements n'ayant jamais eu lieu, tout en	Nuire à l'image d'un candidat/ d'une institution en le discréditant +

		faisant croire qu'ils sont véridiques + Manipulations audio-visuelles comme les deepfake : Contenus audiovisuels falsifiés faisant croire à des événements non réels ou création de vidéos ultra-réalistes où des figures publiques semblent dire ou faire des choses⁴⁰	Transformer des sujets en « problèmes publics » (ex : immigration) + Mobiliser émotionnellement l'électorat + Faire croire qu'une personnalité a dit ou fait des choses qu'elle n'a pourtant jamais dites ou faits (usurpation d'identité) + Faire croire que des événements se sont produits sans que cela soit vrai
Désinformation et/ou mal- information	Trolling et cyber-harcèlement	Intimider, discriminer, provoquer, insulter de manière récurrente une personne à l'aide de raids (vagues organisées et coordonnées de harcèlement par des militants ou des bots)	Intimider (notamment les femmes) afin de les réduire au silence ou de les faire se retirer d'une compétition politique + Porter atteinte à la réputation + Propager de fausses informations

⁴⁰ Exemple de deepfake : <https://www.leparisien.fr/high-tech/qui-sont-amandine-le-pen-et-lena-marechal-ces-deepfakes-qui-font-la-promotion-de-lextreme-droite-sur-tiktok-13-04-2024-ZPPCZKLDDFAKVE4FU4ZV44ZJRE.php>

	Search Engine Optimization (SEO) négatif	Noyer les informations positives bien référencées par un flot de contenus négatifs ou faux sur un candidat ou un parti (Cf. Annexe n°4)	Porter atteinte à la réputation d'un candidat + Nuire à la campagne de son adversaire
	Campagne négative	Diffusion par un candidat d'informations (véritables ou non) négatives sur un adversaire (Cf. Annexe n°6)	Porter atteinte à la réputation de son adversaire Mobiliser émotionnellement l'électorat et le manipuler

Le terme de trouble informationnel est donc bien plus approprié que celui de « fake news » pour mettre en avant la complexité des manipulations électorales. Ces troubles informationnels peuvent avoir un impact important sur une élection dès lors qu'ils sont massivement diffusés dans toute la société (2).

2. Les mécanismes de propagation et d'amplification des troubles informationnels

Les manipulations électorales sont amplifiées stratégiquement à l'aide d'usines à trolls et de bots par les cabinets de conseil politique, ou des milices étrangères comme a pu le faire Wagner pour la Russie (a). Mais les algorithmes des réseaux sociaux favorisent eux-mêmes l'efficacité et l'amplification des troubles informationnels en conduisant les utilisateurs à s'enfermer dans des bulles de filtre et des chambres d'écho (b).

a) Les usines à trolls et les bots

Les usines à trolls- ou ferme à trolls- sont des termes inventés dans le cadre de l'enquête The Agency du New York Times en 2015⁴¹ sur une organisation russe chargée de promouvoir des messages pro-russes sur les réseaux sociaux. Ces usines sont des regroupements de hackers, d'individus rémunérés et de bots chargés de diffuser des messages massivement sur internet pour semer des troubles informationnels. Ces usines peuvent être issues de l'initiative de puissances étatiques ou privées à des fins politiques⁴².

De plus en plus, ces usines sont basées sur des « bots » - diminutif de « robots » - c'est-à-dire des intelligences artificielles qui simulent une activité humaine⁴³. Pour le dire autrement, ce sont de faux comptes tenus par des intelligences artificielles. Ces comptes automatisés permettent d'augmenter la vitesse de propagation des troubles informationnels (viralité) mais aussi d'augmenter leur crédibilité en augmentant la popularité d'un sujet. Ces opérations favorisent une amplification inauthentique, voir malhonnête.

S'il était possible pendant longtemps de reconnaître ces faux comptes par leurs contenus hétéroclites, rédigés en plusieurs langues, et généralement sans photo de profil, depuis février 2018 et l'annonce de Twitter de nouvelles règles pour limiter les bots, ces derniers sont moins reconnaissables. Ben Nimmo explique que les « éleveurs de bots » sont plus discrets, ils noient les messages conçus pour leurs opérations parmi des contenus sans rapport avec la campagne⁴⁴. L'objectif étant de faire croire à un soutien massif des citoyens alors que seuls quelques individus s'intéressent vraiment au sujet. C'est ce qu'on appelle de l'« astroturfing » - ou « similitantisme »- que Sophie Boulay définit comme « *une stratégie de communication dont la source réelle est*

⁴¹ Adrian Chen, The New York Times, "The Agency", 2 juin 2015 : <https://www.nytimes.com/2015/06/07/magazine/the-agency.html>

⁴² Mick Krever, Anna Chernova, CNN, *Wagner chief admits to founding Russian troll farm sanctioned for meddling in US elections*, 14 février 2023 : <https://edition.cnn.com/2023/02/14/europe/russia-yevgeny-prigozhin-internet-research-agency-intl/index.html>

⁴³ NIMMO Ben, « Chapitre 3. Les techniques d'amplification sur les réseaux sociaux », *Les guerres de l'information à l'ère numérique*, Presses Universitaires de France, Paris cedex 14, coll. « Hors collection », 2021, p. 87-103, [https://doi.org/10.3917/puf.maran.2021.01.0087].

⁴⁴ *Ibid.*

occultée et qui prétend à tort être d'origine citoyenne »⁴⁵. Les raids de désinformation utilisant des bots correspondent à cette définition : l'émetteur est caché et un engouement citoyen est simulé. Soit un adversaire politique est l'objet de nombreuses critiques pour faire croire qu'il est en baisse de popularité, soit un candidat est encensé afin d'augmenter sa visibilité et faire croire à un nombre important de soutien, soit une information est massivement republiée pour faire croire un intérêt des citoyens sur le sujet.

Au-delà de l'amplification organisée par les bots et les usines à troll lors de raids ayant pour objectif de faire monter artificiellement un trouble informationnel, les algorithmes des plateformes favorisent aussi leur propagation (b).

b) Les algorithmes : chambres d'écho et bulles de filtre

Les chambres d'écho sont un mécanisme produit par les algorithmes des plateformes qui consiste à diffuser à ceux qui partagent les mêmes points de vue des contenus similaires qui confirment leurs opinions (biais de confirmation). Quattrocchi compare des chambres d'écho pro-science et pro-complotisme sur Facebook. Il montre que les utilisateurs commentent en majorité ce qui renforcent leurs opinions, et ne s'intéressent pas à ce qui les réfutent⁴⁶. Les utilisateurs trient les informations en fonction de ce qui renforce leurs opinions préexistantes, et les algorithmes participent à cette logique en soumettant un contenu qui plaît à l'utilisateur. En d'autres termes, les plateformes réduisent la visibilité de contenus nuancés et favorisent les contenus polarisés⁴⁷. Selon Divina Frau Meigs, ces théories fonctionnent particulièrement pour « *un sous-groupe réduit d'internautes parmi les plus convaincus et les plus actifs, c'est-à-dire pour des personnes susceptibles de visiter des sites de désinformation de manière disproportionnée par*

⁴⁵ Boulay S., 2015, *Usurpation de l'identité citoyenne dans l'espace public. Astroturfing, communication et démocratie*, Québec, Presses de l'université du Québec.

⁴⁶ Walter Quattrocchi, Antonio Scala, Cass Sunstein, « Echo chambers on Facebook », Cambridge (MA), Harvard Law School, Discussion Paper n° 877. PDF téléchargeable à l'adresse suivante : http://www.law.harvard.edu/programs/olin_center/papers/pdf/Sunstein_877.pdf.

⁴⁷ NIMMO Ben, « Chapitre 3. Les techniques d'amplification sur les réseaux sociaux », *op. cit.*, 2021, p. 87-103.

rapport à la population générale »⁴⁸. Les internautes les plus radicalisés sont donc ceux le plus touchés par les effets des algorithmes.

Cette notion de chambre d'écho rejoint celle de « bulle de filtre » de Eli Pariser⁴⁹. L'auteur explique par cette notion que l'utilisateur se retrouve « enfermé » dans un écosystème numérique façonné par les algorithmes des réseaux sociaux, consommant du contenu ciblé en fonction de son identité numérique. Cette bulle filtre renforce la vision du monde et les croyances de l'utilisateur et l'empêche de voir d'autres réalités. Les croyances des utilisateurs sont façonnées par l'interface des réseaux sociaux et le contenu suggéré par les I.A. Amnesty International a ainsi publié en novembre 2023 une étude mesurant l'impact de Tiktok sur la santé mentale des enfants⁵⁰. Les résultats sont édifiants : « *l'étude technique réalisée en partenariat avec l'Algorithmic Transparency Institute et AI Forensics au moyen de comptes automatisés a révélé que, au bout de cinq ou six heures passées sur la plateforme, près d'une vidéo sur deux était relative à la santé et potentiellement nocive, soit un volume 10 fois plus important que celui présenté aux comptes n'ayant indiqué aucun intérêt pour le sujet* ». Cette étude tend donc à valider la théorie de bulle-filtre et pourrait être transposée sur d'autres sujets que la santé mentale.

En résumé, les révélations sur Cambridge Analytica mettent en lumière les atteintes à la vie privée des utilisateurs découlant de ses pratiques de collecte de données, dévoilées tant par les médias que par les informateurs. Les experts du numérique alertent néanmoins que la collecte et la vente de données des utilisateurs dépasse le vol de données sur Facebook par une firme. Ils mettent ainsi en garde contre les risques pour la vie privée provoqués par la collecte des données personnelles. De plus, les révélations sur Cambridge Analytica ne se limitent pas à la collecte frauduleuse de données, mais englobent également ses pratiques manipulatrices, notamment en ce

⁴⁸ FRAU-MEIGS Divina, « Chapitre 14. Les enjeux de la réception : comment mesurer l'influence de la désinformation ? », *Les guerres de l'information à l'ère numérique*, Presses Universitaires de France, Paris cedex 14, coll. « Hors collection », 2021, p. 14 323-345, [<https://doi.org/10.3917/puf.maran.2021.01.0323>].

⁴⁹ PARISER Eli, *The filter bubble: what the Internet is hiding from you*, Viking, London, 2011.

⁵⁰ <https://www.amnesty.org/fr/latest/news/2023/11/tiktok-risks-pushing-children-towards-harmful-content/>

qui concerne les troubles informationnels. Ces derniers, comme définis par Claire Wardle dans le rapport du Conseil de l'Europe, comprennent différents types de contenus mensongers, tels que la désinformation, la mésinformation et la mal-information, ce dernier terme étant privilégié pour éviter l'usage trop répandu et ambigu du terme « fake news ». Mais qu'en est-il de l'efficacité de ces troubles informationnels ? (II).

II. L'efficacité des manipulations électorales numériques questionnée

Dans la deuxième partie de ce mémoire, nous nous plongerons dans le débat crucial qui anime le champ académique : celui de l'efficacité de la propagande et des manipulations électorales à l'ère numérique.

Deux perspectives principales s'affrontent dans ce débat : d'une part, le courant déterministe qui met en avant le poids des structures sociales sur le vote, et d'autre part, le courant cognitiviste qui met en lumière l'importance de la campagne politique dans les choix des électeurs. En réalité, ces deux courants sont plus complémentaires qu'il n'y paraît. Les électeurs volatiles sont de plus en plus nombreux. Ils sont de moins en moins déterminés par le poids des structures, l'influence de la campagne est donc plus importante sur ce type d'électeurs. Le rôle du marketing politique est alors crucial. Les interrelations entre publicité et propagande questionnent sur la notion d'électeur. Peut-on considérer l'électeur comme un consommateur politique influencé par des stratégies marketing sophistiquées (A) ?

Par la suite, nous nous pencherons sur le microciblage politique comme un facteur déterminant de l'efficacité des manipulations numériques. En d'autres termes, nous analyserons les

techniques utilisées dans le microciblage politique et leurs implications sur le processus électoral. Ainsi que les conséquences du consentement souvent non-éclairé des utilisateurs à ce type de ciblage. Nous poserons enfin la question de l'efficacité du microciblage, en abordant les critiques quant à son efficacité ainsi que les preuves indirectes qui témoignent de son impact sur les comportements des utilisateurs (B).

A. Le débat réitératif de l'efficacité de la propagande électorale

L'efficacité de la propagande électorale est un débat de longue date en science politique. Les électeurs ne choisiraient pas pour qui voter mais seraient « décidés » par les structures sociales, cela signifie que les caractéristiques socio-démographiques et l'appartenance de classes seraient le facteur déterminant du vote. Pourtant, d'autres courants mettent en avant l'importance du choix pour l'électeur et le rôle des campagnes politiques. Ces théories méritent d'être discutées et actualisées au regard des évolutions du numérique (1).

Les structures sociales restent, certes, importantes dans l'explication des choix électoraux, néanmoins le nombre d'électeurs volatiles augmentent. Et la propagande électorale fonctionnant mieux sur les électeurs indécis, le marketing politique est devenu un instrument incontournable pour améliorer les stratégies communicationnelles des candidats et ainsi persuader les électeurs volatiles, pivots du résultat de l'élection (2).

1. Le choix des électeurs entre poids des structures sociales et poids de la campagne

Quelle est l'influence des campagnes politiques dans le choix électoral ? Les modèles déterministes expliquent que les comportements électoraux sont déterminés par les structures sociales (a). Pourtant les facteurs sociologiques ne permettent plus d'expliquer les choix électoraux dans la mesure où le vote de classe se réduit, l'abstention augmente tout comme la volatilité des électeurs qui votent pour un camp politique ou un autre selon les scrutins. Le courant cognitiviste et constructiviste montre alors l'influence de la campagne politique sur le choix électoral (b).

Cette partie est basée sur l'article très détaillé et complet de Frédéric Dosquet sur le comportement des électeurs et la persuasion électorale⁵¹.

⁵¹ DOSQUET Frédéric, « Chapitre 3. Comportement des électeurs et persuasion électorale », *Marketing et communication politique*, EMS Editions, Caen, coll. « Questions de société », vol.2e éd., 2017, p. 125-182, [<https://doi.org/10.3917/ems.dosqu.2017.01.0125>].

a) Courant déterministe : le poids des structures sociales sur le vote

Les courants déterministes « *mettent l'accent sur les structures et les régularités du comportement électoral. Ils cherchent à expliquer l'orientation du vote par l'appartenance des individus à une époque, une société, un territoire ou un milieu donné* »⁵². Ainsi, pour les tenants de l'Ecole de Columbia ou de l'Ecole de Michigan, le déterminisme social et familial est à l'origine du comportement électoral. Les électeurs seraient incompetents politiquement, ils distinguent peu les différents partis et candidats, et ont une faible connaissance des enjeux. Les campagnes auraient peu d'effet sur le vote.

Paul Lazarsfeld appartenant à l'Ecole de Columbia a montré que les variables lourdes qui caractérisent l'individu (âge, classe sociale, niveau de revenu, religion, ethnie, etc...) sont déterminante dans le vote. Ces variables lourdes déterminent l'appartenance sociale des électeurs – c'est-à-dire leurs appartenances à différents groupes sociaux comme la classe sociale. Or les appartenances sociales sont au cœur du vote, dans la mesure où l'électeur vote comme le reste de son groupe social. La socialisation primaire est alors très importante dans ces courants.

Ainsi, dans les années 1970, on pouvait observer un vote partisan reposant sur la classe sociale. Les ouvriers urbains votaient pour le parti communiste puis socialiste, alors que les familles aisées ou les ruraux catholiques votaient à droite.

L'université du Michigan justifie les choix électoraux et leur stabilité par le concept de l'« *identification partisane* ». Frédéric Dosquet explique que l'identification partisane n'est pas seulement le fruit de l'appartenance sociale, c'est aussi un « *attachement affectif* », qu'il définit comme « *une loyauté quasiment identitaire construite depuis l'enfance* »⁵³.

Pourtant, en 2007, les ouvrières sans diplôme ont voté plus pour Sarkozy que pour Ségolène Royal, ce qui contrevient aux théories déterministes⁵⁴. Les électeurs sont de plus en plus volatiles

⁵² Mayer N. (1997), « Introduction », In Boy D., Mayer N., *L'électeur a ses raisons*, Presses de Sciences Po.

⁵³ DOSQUET Frédéric, « Chapitre 3. Comportement des électeurs et persuasion électorale », *op. cit.*, 2017, p. 125-182.

⁵⁴ Dosquet, Frédéric. « Chapitre 3. Comportement des électeurs et persuasion électorale », Frédéric Dosquet éd., *Marketing et communication politique. 2^e édition*. EMS Editions, 2017, pp. 125-182.

et le sentiment d'appartenance à une classe sociale de moins en moins fort, les effets de la campagne sont alors plus importants (b).

b) Le courant cognitiviste : le poids de la campagne sur le vote

Le courant cognitiviste rompt avec les théories déterministes. Loïc Blondiaux explique que les électeurs sont certes peu compétents politiquement -comme pour le courant déterministe- mais le contexte est jugé comme pouvant influencer le choix du vote -plus que les structures sociales⁵⁵. En effet, le contexte socio-économique, les éléments les plus accessibles pour l'électeur, ainsi que les émotions suscitées par le candidat et les appartenances partisane et religieuse influenceraient le choix de l'électeur. Ce modèle laisse une place plus importante à l'efficacité de la propagande électorale puisque l'électeur indécis et peu compétent se base sur des éléments simples et à sa portée pour se décider.

Le courant constructiviste met en avant la construction de l'information comme influence du choix électoral. Les médias n'exerceraient pas une influence directe et immédiate mais plus discrète et rusée. Trois techniques de persuasion sont mises en avant par les chercheurs en science politique :

Le « Framing » permet de cadrer un sujet d'une certaine manière pour faire ressortir un enjeu plutôt qu'un autre. Cela permet de définir un problème d'une façon particulière (ex : crise de l'immigration ou crise de l'accueil des migrants ?), et de proposer des liens de causes à effets (ex : augmentation de la délinquance et immigration). Le cadrage permet de guider la réflexion de l'électeur en lui proposant un point de vue sur un sujet et une interprétation. La pauvreté peut être traitée comme la conséquence d'une responsabilité individuelle ou collective par exemple, ce qui conduit à des réponses politiques très différentes. La manière dont est présenté un sujet, en réduisant les enjeux complexes à des dimensions limitées, permet d'orienter la manière dont l'auditeur construit ses opinions.

Le « priming » d'Iyengar et Kinder théorise l'idée que certains sujets ont plus de poids dans une campagne et servent de point de jugement pour les électeurs. Cela conduit à un « vote sur

⁵⁵ Blondiaux L., *La Fabrique de l'Opinion : une Histoire Sociale des Sondages*, Paris, Seuil, 1998.

enjeux ». On va voter pour le candidat qui répond le mieux à la problématique qui nous intéresse le plus.

Or généralement les sujets qui nous intéressent le plus sont ceux « mis à l'agenda » (*agenda setting*) selon le concept de Mc Combs et Shaw. Plus un sujet est couvert médiatiquement, plus il est important pour l'électeur pour faire son choix. Il n'est pas nécessaire de dire quoi penser mais « à quoi » il faut penser. Ce concept est à mettre en parallèle avec celui du déni d'agenda, qui consiste à ne pas traiter de sujets qui pourtant sont importants pour certains électeurs, ou qui pourraient servir pour départager des candidats. Les médias, ou les politiques censurent certains sujets.

Ces trois mécanismes participent ensemble à influencer les choix des électeurs dans le cadre d'une campagne politique. A l'heure des réseaux sociaux leurs effets se prolongent en ligne.

Les courants déterministes et constructivistes sont complémentaires. En effet, les structures déterminent encore majoritairement le vote (niveau de diplôme, âge, patrimoine économique, appartenance au secteur privé ou public), mais pour les électeurs plus volatiles la campagne peut exercer une influence d'où la mise en place de stratégie marketing en politique par les partis (2).

2. Le marketing politique

Le marketing et les sciences sociales sont liés et se renforcent l'un l'autre. Les acteurs politiques se sont saisis du marketing politique pour améliorer l'efficacité de leurs campagnes en se basant sur les techniques commerciales (a). Mais peut-on considérer un candidat politique comme un produit de consommation pour autant (b) ?

a) Interrelation entre publicité et propagande

Sciences sociales et marketing sont entremêlés depuis longtemps comme le montre Kurt Lewin⁵⁶. Ainsi, durant la seconde guerre mondiale, le gouvernement étasunien cherchait une

⁵⁶ Dortier, Jean-François. « La publicité nous manipule-t-elle ? », Jean-François Dortier éd., *La Communication. Des relations interpersonnelles aux réseaux sociaux*. Éditions Sciences Humaines, 2016, pp. 230-238.

solution pour promouvoir les abats lors d'une pénurie de viande. Kurt Lewin démontre alors que des femmes réunies en petits groupes discutant de la manière de cuisiner les abats changent plus leurs habitudes alimentaires (32%) que celles qui ont entendu à la radio une autorité scientifique en vanter les mérites (seules 3% ont changé leurs habitudes). Le résultat de cette étude est donc que l'influence d'un petit groupe est bien plus importante qu'un message diffusé massivement.

Cette étude fait écho à celle de Paul Lazarsfeld qui démontre dans son modèle « two step flow » que l'influence des médias agit par l'intermédiaire d'un leader d'opinion-première étape-qui retransmet le message médiatique à son entourage-seconde étape. L'influence des proches est donc primordiale dans la formation de ses opinions. La théorie de la « seringue hypodermique » de Harold Lasswell selon laquelle les médias auraient une influence directe et immédiate sur les opinions des individus est dépassée, les médias ne sont pas tout puissants sur la formation de l'opinion. Même si l'on a pu croire pendant les Trente Glorieuses que la publicité endoctrinait les consommateurs et poussaient à l'achat, en réalité, le contexte économique et historique favorisait la consommation même sans la publicité. La publicité ne permet pas de faire acheter quelque chose qu'on ne désire pas, comme la propagande électorale ne peut pas faire voter pour quelqu'un pour qui l'on ne voterait pas d'ordinaire.

Le véritable effet de la publicité est de faire connaître un produit, une marque. Si l'on désire acheter un produit, on va se tourner vers l'un qui nous est familier. La propagande fonctionne de la même manière et touche donc plus fortement les électeurs indécis.

Le modèle du « Two-step flow » à l'ère numérique :

Le modèle du « two-step flow » de Lazarsfeld est particulièrement intéressant pour étudier la formation des opinions en ligne, et plus précisément sur les réseaux sociaux.

L'électeur économise son temps et sa réflexion en basant son opinion sur celle d'un proche qu'il juge compétent sur la question. Plutôt que de s'informer personnellement sur chaque sujet, l'électeur fait confiance à la retranscription de l'information d'un autre qui *de facto* transmet une interprétation de l'information.

Sur les réseaux sociaux, on peut faire l'hypothèse que le leader d'opinion n'est plus seulement un proche mais une personne que l'on suit.

- 1) Cela peut notamment être un « influenceur » - un créateur de contenu rémunéré – que l'on suit assidument et de manière active. Les influenceurs parviennent à influencer les modes de vie de ses followers qui achètent les produits recommandés, consomment les mêmes activités, visitent les mêmes lieux, etc... Alors pourquoi ne façonneraient-ils pas également la vision du monde des followers ? On peut supposer que les influenceurs sont une forme de leaders d'opinion, et que les électeurs fondent leurs opinions sur la leur, et sur leur traduction des informations.

Ainsi par exemple, le créateur de contenu HugoDécrypte s'est spécialisé dans le tri des informations et leurs explications à ses followers. Ainsi, HugoDécrypte met à l'agenda certains sujets, en omet d'autres, et en propose un cadrage et une interprétation que ses followers peuvent reprendre à leur compte.

- 2) Mais le leader d'opinion peut ne pas être un influenceur, cela peut être un compte militant d'une personne qu'on ne connaît qu'à travers les réseaux sociaux. Ces comptes militants proposent une interprétation de l'actualité et des informations à leurs followers. La construction d'une opinion sur certains sujets peut se faire à partir de leur traitement par des comptes militants, comme nous avons pu l'observer de manière à travers notre propre usage des réseaux sociaux. Cela a notamment été le cas en suivant des comptes féministes qui ont permis la découverte des questions de transidentité et de genre, jusqu'alors ignorées. Ces comptes ont mis à l'agenda des sujets qui étaient déniés par les médias classiques. Leur cadrage de ces sujets ainsi que leurs interprétations ont participé à la formation des opinions des utilisateurs. Mais d'autres cadrages ont conduit à la formation d'opinions très différentes en suivant les comptes des féministes dites TERF (Trans-exclusionary radical feminist) qui ne reconnaissent pas les théories de genre et rejettent les personnes trans.
- 3) Claire Wardle, spécialiste des troubles informationnels, écrit « *La taille moyenne d'un groupe WhatsApp au Brésil est de six personnes. En ce qui concerne les fausses informations que nous repérons, elles circulent dans tout type de groupes. Elles peuvent partir d'un groupe important puis se transmettre à des groupes de plus en plus petits, par*

le biais des transferts de messages effectués par les utilisateurs. Elles atterrissent finalement dans des groupes WhatsApp vraiment petits, mais où les gens se font vraiment confiance. »⁵⁷. Les plateformes sont particulièrement adaptées à la théorie du two-step flow, et notamment les groupes de messagerie où circulent de nombreuses informations entre des individus proches. Comme l'explique C. Wardle, les groupes Whatsapp sont constitués d'en moyenne 6 personnes proches qui se partagent des contenus venus d'autres groupes. Cela favorise la transmission d'informations, et l'on fait confiance à celui qui nous la transmet pour croire l'information.

b) L'électeur comme consommateur politique

Le microciblage commercial est une forme avancée de la publicité. Il permet d'adresser la publicité à un public qu'on sait être intéressé par notre produit ou qui en aurait besoin. Ainsi, par exemple, si l'on est une marque spécialisée dans les baskets de running pour sportif expérimenté, il est bien plus intéressant de s'adresser à des sportifs qui sont susceptibles d'acheter notre produit qu'à l'ensemble de la population qui comprend des personnes qui détestent le sport. Mais qu'en est-il des candidats politiques ? Peut-on les comparer à un produit de consommation ?

L'électeur-consommateur est un modèle théorisé par Himmelweit, Humphreys, Jaeger, et Katz⁵⁸. L'élection serait un marché avec des candidats en situation de concurrence. Les électeurs auraient des habitudes d'achat (habitude de voter pour un parti) et des préférences pour certaines marques comme l'explique Mayer. Mais pour Isabel Kusche⁵⁹ sociologue spécialisée en communication politique, les élections n'offriraient des options « *qu'entre des produits très complexes, regroupant des croyances idéologiques, des engagements spécifiques et des déclarations politiques relatives aux compétences en matière de gouvernance* ». Selon elle, il y a «

⁵⁷ « « Infox » au Brésil : comment les fausses informations ont inondé WhatsApp », *Le Monde.fr*, 25/10/2018. : https://www.lemonde.fr/pixels/article/2018/10/25/infox-au-bresil-comment-les-fausses-informations-ont-inonde-whatsapp_5374637_4408996.html

⁵⁸ Himmelweit, H. T., Humphreys, P., Jaeger, M., & Katz, M. (1981). How voters decide: A longitudinal study of political attitudes and voting extending over fifteen years. *European Monographs in Social Psychology*, 27, 276.

⁵⁹ Isabel Kusche, The conversation, 7 mai 2019 : <https://theconversation.com/pourquoi-le-micro-ciblage-politique-pourrait-saper-la-democratie-116319>

un très long chemin à parcourir entre persuader des personnes de cliquer sur une publicité politique et les persuader d'opter le jour de l'élection pour un parti ou un candidat qu'ils n'auraient pas choisi autrement ».

On peut critiquer la vision d'Isabel Kusche comme étant trop idéalisée. Tous les électeurs ne sont pas nécessairement compétents politiquement, ils ne sont pas informés sur les différents programmes et candidats. Ils fondent leurs choix sur des discussions avec des proches, une représentation du candidat qui est plus ou moins proche de la réalité⁶⁰. Ainsi, le choix d'un candidat ne repose pas forcément plus sur un choix très complexe que sur la visibilité d'un candidat et l'opinion qu'on s'en fait – qu'elle soit basée sur des faits ou non. De plus, le microciblage permet de s'adresser à des personnes qui y seront réceptives. L'enjeu n'est donc pas de « *persuader d'opter le jour de l'élection pour un candidat qu'ils n'auraient pas choisi autrement* » mais plutôt de pousser à voter ou ne pas voter pour un candidat si l'électeur est volatile. Il est effectivement peu probable que l'on puisse convaincre un électeur fermement républicain de voter démocrate (ou inversement), qu'importe les manipulations. Mais en s'adressant à un électeur indécis, il est possible d'orienter son vote à l'aide de différentes techniques.

En résumé, la propagande fonctionne à la marge, les structures sociales déterminent encore majoritairement le vote. Elle ne fonctionne que sur les électeurs indécis qui sont plus attentifs et réceptifs aux campagnes politiques, c'est pourquoi la pratique du microciblage est efficace (B).

⁶⁰ Taghavi, Babak. « SPEL, *Les sens du vote. Une enquête sociologique (France 2011-2014)*, Rennes, Presses universitaires de Rennes, coll. « Res publica », 2016, 229 p. », *Politix*, vol. 119, no. 3, 2017, pp. 175-179.

B. Le microciblage politique comme facteur d'efficacité des manipulations numériques

Le microciblage politique permet de segmenter les électeurs en catégories très fines, ce qui permet de leur diffuser des publicités personnalisées alors même que leur consentement n'est pas éclairé (1). Mais est-ce que ces publicités ciblées et personnalisées sont plus efficaces que la publicité classique (2) ?

1. Les techniques et implications du microciblage politique pour la vie privée

Le microciblage politique permet de mettre en place des publicités individualisées et personnalisées visant un groupe très spécifique (a). Pour ce faire, les plateformes récoltent les données des utilisateurs, en leur extirpant leur consentement (b).

a) Analyse du microciblage politique

Le microciblage est une stratégie publicitaire qui vise à identifier un groupe spécifique d'individus susceptibles d'être intéressés par le produit vendu. Pour cela, les databrokers – firmes qui collectent et vendent les données sous forme brute ou transformées en données prédictives utilisent la délégation logicielle pour combiner données démographiques (âge, sexe, éducation, lieu d'habitation), économiques (type d'emploi, niveau de revenu, dépenses, habitudes d'achat), sociales et politique (genre, réseaux de l'individu, politisation, valeurs), comportementales (attitudes, intérêts, « lifestyle »), psychologiques (peur, motivation, etc) et ainsi dresser des listes de groupes d'intérêts et de mode de vie différents. L'objectif est d'influencer le comportement du consommateur pour lui vendre un produit en le ciblant précisément avec un contenu personnalisé en fonction de son profil psychologique et social.

En résumé, le microciblage repose premièrement sur la collecte de données diverses et variées ; deuxièmement sur la segmentation du marché en très petit groupe homogène ; et troisièmement, sur la personnalisation du message diffusé aux différents segments.

L'objectif du microciblage est de toucher la personne ciblée, captiver son intérêt et la pousser à agir dans le sens souhaité. Cela permet aux entreprises d'améliorer leur stratégie marketing et de mieux dépenser leurs budgets publicitaires.

Cette pratique est aussi utilisée en marketing politique dans le cadre notamment de campagnes électorales. Les campagnes sont habituellement de la communication publique c'est-à-dire que tout le monde y a accès. Le candidat peut communiquer à un segment de la population mais les autres individus l'écoutent aussi. La démocratie repose sur la confrontation des intérêts, tout le monde ne peut pas avoir ce qu'il veut car les intérêts des citoyens sont contradictoires. Le risque avec le microciblage est de faire du clientélisme numérique et de faire à chaque segment ciblé des promesses contradictoires sans que les électeurs ne s'en rendent compte.

Le microciblage participe à l'efficacité des troubles informationnels. Par exemple, dans le cadre de la « mal-information », les contenus fabriqués peuvent l'être pour un segment très précis dans un objectif très spécifique. Ce contenu n'aurait sûrement jamais été pris au sérieux par d'autres personnes. Comme il est fabriqué pour un profil-type, son efficacité est bien plus importante que s'il était diffusé largement. Cambridge Analytica dans une présentation de vente⁶¹ de ses services a ainsi mis en avant l'élection de Trinité-et-Tobago (Caraïbes) pour laquelle ils ont été embauchés par le parti indien pour gagner contre le parti afro-antillais. Ils ont évalué que l'élection pouvait être renversée par les jeunes. La méthode adoptée a été de développer le mouvement « *do so* » chez les jeunes (des deux côtés) en contestation contre la politique et le vote en général, ce qui avait pour objectif de promouvoir l'abstentionnisme comme geste de résistance. Les jeunes ont beaucoup investi ce mouvement (tag sur la maison du premier ministre, vidéos en ligne, manifestation, ...). Cambridge Analytica affirme qu'ils savaient que les jeunes afro-caraïbéens n'iraient pas voter en raison du mouvement *Do so*, mais que les jeunes indiens iraient. Cambridge Analytica explique que les jeunes indiens, même en ayant participé au mouvement, n'iront pas à l'encontre de la

⁶¹ Présentation de vente révélée par l'ancienne directrice du développement commercial de Cambridge Analytica, Brittany Kaiser dans le documentaire *The Great Hack* sur Netflix.

volonté de leurs parents. La différence d'abstention chez les jeunes de 18 à 35 ans était de 40%, ce qui selon Cambridge Analytica a fait basculer les résultats de 6%, permettant au parti indien de remporter le scrutin.

Le microciblage permet donc de diffuser un contenu avec efficacité et de créer une réaction attendue (influencer un comportement), ce qui peut rendre les troubles informationnels bien plus efficaces et dangereux pour la démocratie.

b) Les implications du consentement non-éclairé de l'utilisateur au microciblage

Shoshana Zuboff utilise la notion de « décontrat » pour critiquer le recueil du consentement des plateformes par leur Conditions Générales d'Utilisation (CGU). Quand l'utilisateur consent à utiliser une plateforme, il consent à la collecte de ses données et leurs traitements.

Le contrat est à la base de l'échange. Il protège à la fois celui qui fournit un bien ou un service et celui qui le reçoit. Juridiquement, pour qu'un contrat soit valide, il est nécessaire que les stipulations contractuelles soient légales, que les contractants soient capables juridiquement et enfin que leur consentement soit libre et éclairé comme le dispose l'article 1128 du Code Civil français. Les CGU sont des « contrats d'adhésion », c'est-à-dire qu'ils ne sont pas négociables et imposent les stipulations unilatéralement. Cela engendre nécessairement un déséquilibre entre les contractants que sont les plateformes et les utilisateurs.

Le RGPD prévoit dans son article 4 alinéa 11 une définition du consentement « *« consentement » de la personne concernée, toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement* »⁶².

Nous allons nous concentrer sur la notion de « consentement éclairé ». Le consentement éclairé signifie que le contractant donne son accord en ayant connaissance des informations

⁶² RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) : <https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679>

constitutives du contrat. En d'autres termes, l'utilisateur doit avoir connaissance de toutes les informations nécessaires pour qu'il fonde sa décision. Les informations doivent être complètes et comprises par le contractant. Le consentement du contractant ne doit pas être vicié par un manque d'informations. Or, les CGU sont floues et complexes pour l'utilisateur qui consent sans même les lire. Un acteur embauché par l'association des consommateurs australienne « Choices » a mis huit heures cinquante-neuf minutes pour lire les CGU d'Amazon Kindle⁶³. Cette expérience montre la longueur excessive des CGU et leur inintelligibilité, notamment vis-à-vis des stipulations relatives à la collecte de données, leur traitement et leur partage à des tiers ⁶⁴.

Pourtant, les utilisateurs n'ont pas le choix de consentir sous la pression des contraintes sociales. Par exemple, pour trouver un emploi, les recherches se font en ligne via des plateformes dédiées (Indeed) ou des réseaux sociaux comme LinkedIn. Les individus communiquent dans des groupes Whatsapp ou Messenger (Meta). Il est difficile d'être militant pour un parti sans utiliser les plateformes pour s'organiser avec les autres militants. Il y a donc des pressions économiques et relationnelles pour utiliser ces services, la personne risquerait sinon le stigmatisme voire l'exclusion du groupe social. Nous devenons alors tous dépendants des plateformes et cédon aux CGU plutôt que nous y consentons.

Le règlement européen sur les marchés numériques prévoit que les plateformes n'ont plus le droit d'utiliser les données des utilisateurs sans leur consentement explicite. Néanmoins, le groupe Meta a tenté de trouver une parade : proposer un abonnement payant pour supprimer les publicités, ou consentir à partager ses données à des fins de publicités ciblées. L'image ci-contre est le choix proposé par Meta aux utilisateurs depuis novembre 2023. Meta est ainsi très clair, ce n'est pas la publicité qui est la source de ses revenus, mais la collecte de données et la personnalisation, c'est-à-dire le microciblage publicitaire. Des plaintes ont été déposées par des organisations civiles pour violation

Vous pouvez utiliser nos produits avec ou sans publicités

Utiliser gratuitement avec de la publicité
Découvrez des produits et des marques grâce à des publicités personnalisées, tout en utilisant votre compte Instagram gratuitement. Vos informations seront utilisées pour les publicités.
Votre choix actuel

S'abonner pour utiliser sans publicités
Abonnez-vous pour utiliser votre compte Instagram sans publicités, à partir de 9,99 €/mois (taxes applicables incluses). Vos informations ne seront pas utilisées pour les publicités.

 Vous pouvez modifier votre choix à tout moment

⁶³ Choice, « How Long Does It Take to Read Amazon Kindle's Terms and Conditions? », YouTube, 17 mars 2017 : <https://www.youtube.com/watch?v=sxygkyskucA>

⁶⁴ MANOKHA Ivan, « Le scandale Cambridge Analytica contextualisé », *op. cit.*, 2018, p. 39-59.

présumée du RGPD. Pour l'instant, aucune décision n'a été rendue. L'abonnement est ainsi toujours proposé.

Ce microciblage est-il aussi efficace que les acteurs de CA ou les journalistes le racontent (2) ?

2. Les effets du microciblage sur les médias sociaux

Il existe des discussions sur l'efficacité du microciblage et leurs impacts, notamment depuis l'affaire CA. Les GAFAM cherchent publiquement à rassurer leurs utilisateurs : les manipulations seraient inefficaces et les publicités ciblées ne servent qu'à leur présenter des produits ou services pertinents pour eux (a). Mais les électeurs sont soumis à des publicités personnalisées qui les ciblent très spécifiquement en fonction de leurs données, exploitant leurs peurs et leurs valeurs. Dès lors le microciblage semble être un outil très efficace pour manipuler les électeurs comme le montrent de nombreuses preuves indirectes (b).

a) Les critiques quant à l'efficacité du microciblage

Certains auteurs contestent l'efficacité du microciblage politique. Ils affirment que son efficacité ne serait pas démontrée par des études quantitatives. Ainsi, Jessica Baldwin-Philippi, du département des sciences de la communication et des médias à l'université de Fordham aux Etats-Unis, avance que le microciblage politique est plus efficace pour mobiliser des militants que persuader des électeurs⁶⁵. Le problème est la vision de l'efficacité de la persuasion par les auteurs. Ces auteurs considèrent que la persuasion serait efficace seulement si le microciblage parvient à faire changer d'avis un électeur quant à ses opinions politiques. Le microciblage fonctionnerait seulement s'il sert à convaincre un électeur démocrate depuis toujours de voter pour un candidat républicain. Evidemment dans cette optique, le microciblage et les manipulations sont inefficaces. Les effets sont beaucoup plus limités et insidieux, il s'agit de renforcer une opinion déjà présente.

⁶⁵ Baldwin-Philippi, Jessica. "Data campaigning: between empirics and assumptions". Internet Policy Review 8.4 (2019). Web. 26 Apr. 2024.

Le microciblage permet de cibler les électeurs indécis et de personnaliser un contenu pour les convaincre de ne pas voter pour le candidat adverse. Par exemple, un électeur qui hésite à aller voter pour le candidat démocrate aura un contenu qui le dissuade (ex : crooked Hillary). Alors qu'un électeur qui hésite à voter pour le candidat républicain aura un contenu l'incitant à se rendre aux urnes. L'idée n'est pas de convaincre ceux qui sont déjà décidés, mais de viser ceux qui ne le sont pas pour les influencer.

Une autre étude menée par plusieurs universitaires⁶⁶ montre que le microciblage politique, en se basant sur un critère (ex : âge), surpasse de 70% les contenus diffusés sans ciblage. Néanmoins, dès lors qu'on ajoute plusieurs critères de ciblage, il n'y aurait pas de gains supplémentaires. Plus de 5 000 participants ont été exposés à différentes stratégies publicitaires. Certains ont vu les publicités les plus performantes d'une première phase de l'enquête, d'autres des publicités choisies au hasard, et d'autres encore des publicités microciblées sélectionnées à l'aide d'un modèle d'apprentissage automatique entraîné sur les données de la première phase. Les résultats ont montré que la stratégie de microciblage était plus efficace que d'autres tactiques publicitaires largement utilisées, mais qu'il n'y avait pas de différence significative entre les publicités microciblées basées sur une seule caractéristique des électeurs et celles basées sur plusieurs caractéristiques. Les chercheurs ont réalisé cette étude après le scandale CA afin d'offrir une « évaluation rigoureuse de son impact potentiel dans le monde réel » (en d'autres termes, l'objectif est de démontrer que CA et Facebook n'auraient pas réussi à manipuler les élections). Mais on peut noter que les conditions de l'étude sont très différentes de la réalité. Entre voir une fois une vidéo et être soumis plusieurs heures par jour à des contenus ciblés est très différent. De plus, il est nécessaire de soulever un conflit d'intérêt : des travaux de Rand et de Berinsky ont été financés par Google et Meta⁶⁷. En prouvant l'efficacité des manipulations, et les risques inhérents au microciblage, ces chercheurs auraient pu se mettre à dos leurs financeurs.

⁶⁶ Tappin, Ben M et al. "Quantifying the potential persuasive returns to political microtargeting." *Proceedings of the National Academy of Sciences of the United States of America* vol. 120,25 (2023)

⁶⁷ Les auteurs le signalent eux-mêmes au sein de l'article dans la catégorie « conflits d'intérêts » : "Other research by A.J.B. and D.G.R. is funded by gifts from Google and Meta" issu de « Tappin, Ben M et al. "Quantifying the potential persuasive returns to political microtargeting." *Proceedings of the National Academy of Sciences of the United States of America* vol. 120,25 (2023) »

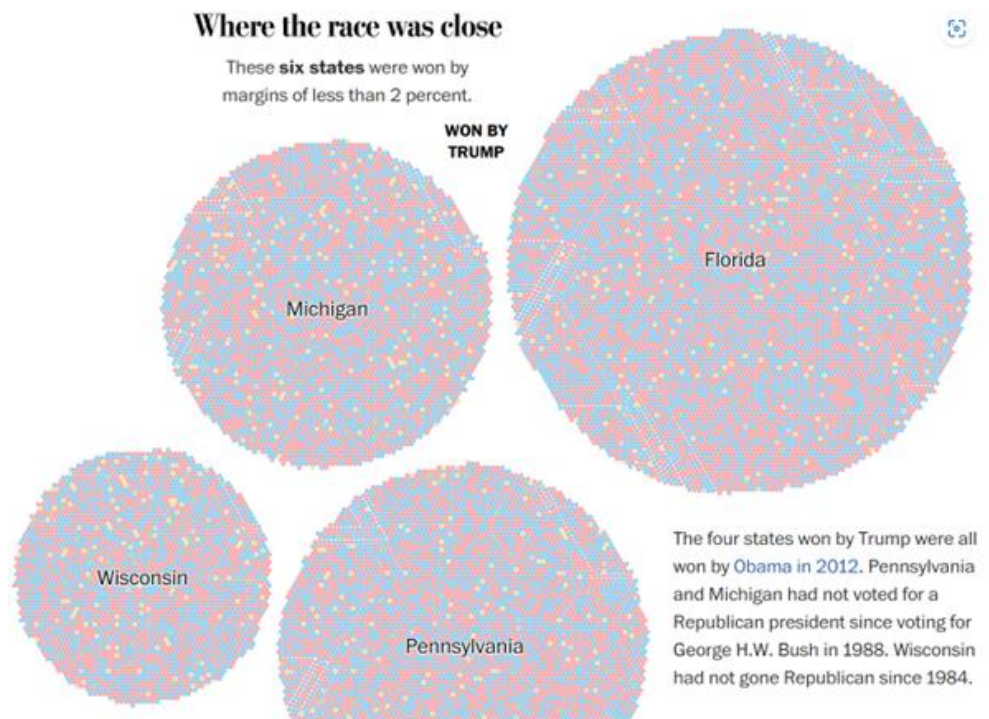
Il semble impossible de prouver l'efficacité du microciblage et des manipulations de manière formelle, en prenant en compte tous les contenus qu'un électeur visionne pendant le temps de campagne. Il faudrait pouvoir voir le fort-intérieur des personnes pour savoir ce qui est à l'origine de leurs choix électoraux. On peut donc seulement essayer de dresser un faisceau d'indices concordants (b).

b) Les preuves indirectes de l'efficacité du microciblage

Ainsi on constate une baisse des revenus du marché publicitaire traditionnel et une nette augmentation du marché du microciblage (voir Annexe n°10). Or les acteurs économiques sont rationnels dans le sens où leurs décisions sont orientées vers la recherche du profit. S'ils investissent dans ce type de publicité, c'est qu'ils observent une augmentation de leurs ventes⁶⁸. Ce marché publicitaire est dominé par deux grands géants du numérique : Google et Facebook. En 2017, ils hébergeaient 61% de l'ensemble de la publicité digitale⁶⁹.

Par ailleurs, en s'intéressant à la campagne de Trump en 2016, on peut remarquer certaines curiosités sociologiques.

Dans un article du Washington Post (dont est issu l'infographie ci-dessous)⁷⁰, nous pouvons voir que l'élection s'est jouée sur quatre Etats remportés par Trump qui pourtant étaient historiquement

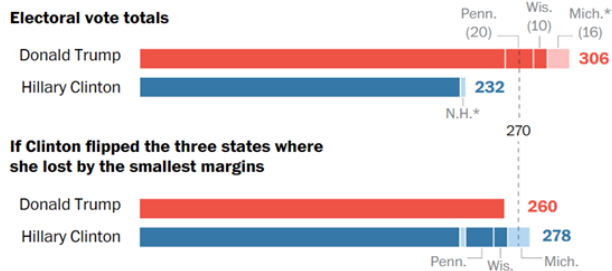


⁶⁸ VALLUY Jérôme, « HUMANITÉ ET NUMÉRIQUE(S) », 2023.

⁶⁹ CARDON Dominique, « La publicité en ligne », *Culture numérique*, Presses de Sciences Po, Paris, coll. « Les petites humanités », 2019, p. 310-320.

⁷⁰ Tim Meko, Denise Lu, Lazaro Gamio, Washington post, *How Trump won the presidency with razor-thin margins in swing states*, nov 2016 : <https://www.washingtonpost.com/graphics/politics/2016-election/swing-state-margins/>

des bastions démocrates. Ainsi, il a remporté le Michigan et la Pennsylvanie qui n’avaient pas voté républicain depuis 1988 (soit 28 ans) et le Wisconsin depuis 1984. De plus, la victoire de Trump dans ces Etats tient à moins de 2%. Au final l’élection a basculé par le vote de 107 000 citoyens américains selon le Washington post sur 136 753 936 votants, soit moins de 0,08% de l’électorat.



Note: Includes Michigan and New Hampshire, which are not officially called as of Nov. 11.

This election was effectively decided by **107,000 people** in these three states. Trump won the popular vote there by that combined amount. That amounts to 0.09 percent of all votes cast in this election.

Dans ce contexte, l’impact du microciblage et des manipulations a pu être très important. Il a fallu réussir à convaincre seulement une centaine de milliers d’électeurs indécis à tendance républicaine de se rendre aux urnes pour voter pour Trump, et pour ceux indécis à tendance démocrate de ne pas voter. La campagne de dénigrement envers Hillary Clinton a pu notamment avoir un impact très important.

Le microciblage semble ainsi avoir une efficacité importante pour convaincre un petit groupe d’électeurs d’aller -ou de ne pas aller- voter. Malgré un impact important sur le scrutin, le microciblage n’est pas réglementé, sauf vis-à-vis des mineurs.

Cela est une autre preuve indirecte de l’efficacité du microciblage. L’Union européenne a interdit la pratique du microciblage à des fins de publicités personnalisées dans le Digital Services Act à son article 28⁷¹.

« Article 28

Protection des mineurs en ligne

1. Les fournisseurs de plateformes en ligne accessibles aux mineurs mettent en place des mesures appropriées et proportionnées pour garantir un niveau élevé de protection de la vie privée, de sûreté et de sécurité des mineurs sur leur service.
2. Les fournisseurs de plateformes en ligne ne présentent pas sur leur interface de publicité qui repose sur du profilage, tel qu’il est défini à l’article 4, point 4), du

⁷¹ RÈGLEMENT (UE) 2022/2065 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques) : <https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32022R2065>

règlement (UE) 2016/679 en utilisant des données à caractère personnel concernant le destinataire du service dès lors qu'ils ont connaissance avec une certitude raisonnable que le destinataire du service est un mineur. (...) »

L'Union européenne interdit donc le microciblage qu'elle considère comme contrevenant à la garantie d'un « *niveau élevé de protection de la vie privée, de sûreté et de sécurité* » (alinéa 1 de l'article 28). Les mineurs sont considérés comme plus influençables et plus réceptifs qu'un adulte aux manipulations, pourquoi l'Union européenne interdirait le microciblage des mineurs s'il n'avait aucune efficacité et ne comportait aucun risque ?

En résumé, le vote est déterminé historiquement par l'influence des structures sociales, mais ce constat est de moins en moins vrai. Les électeurs sont de plus en plus volatiles, changeant de camp selon les élections et les candidats. Les effets des campagnes électorales ont plus d'influence sur ces électeurs volatiles qui ne sont pas décidés par des considérations partisans. Les partis politiques et les candidats se sont alors saisis du marketing et de ses techniques pour persuader le plus d'électeurs de voter pour eux. Or, parmi ces pratiques, le microciblage est apparu comme la plus efficace.

Le microciblage politique permet de segmenter les électeurs en catégories très fines pour leur diffuser des publicités personnalisées basées sur leurs données numériques. Le traitement de ces données permet d'avoir une connaissance très précise de l'électeur. On peut alors dresser son profil psychologique et connaître ses leviers de persuasion (la peur, la colère, l'attachement aux valeurs traditionnels, etc). Il suffit alors de lui adresser des publicités basées dessus.

Mais pour recueillir ces données si précieuses, les plateformes sont obligées de recueillir le consentement des utilisateurs, du moins dans l'Union européenne, ou au moins un consentement à leur CGU pour les utilisateurs du reste du monde. Mais les CGU sont complexes et floues, les utilisateurs ne les lisent pas et ne comprennent pas ce qu'il sera fait de leurs données. Leur consentement n'est pas éclairé. Pour les utilisateurs européens, depuis le RGPD de 2016, leur consentement doit être recueilli spécifiquement pour collecter leurs données et les traiter. Mais un ultimatum peut être fixé par les plateformes, si les utilisateurs ne consentent pas, ils ne peuvent pas

accéder aux services. Le consentement est donc arraché aux utilisateurs qui ne peuvent vivre socialement sans utiliser ces plateformes que ce soit dans leur vie personnelle ou professionnelle.

Les plateformes pour rassurer les utilisateurs sur les publicités ciblées affirment qu'elles ne servent qu'à fournir un contenu plus pertinent pour l'utilisateur. En parallèle des études financées par ces grandes plateformes démontrent l'inefficacité du microciblage politique après le scandale de CA. De plus, les sciences sociales, dominées par l'école des usages⁷², sont réticentes à affirmer que les effets des médias de masse seraient directs et immédiats sur la formation de l'opinion depuis les résultats de Lazarsfeld démontrant l'inexistence de la seringue hypodermique. Les chercheurs minimisent les effets des médias pour mettre en avant la réception active des utilisateurs. Ainsi, la science sociale a tendance à contester l'efficacité des manipulations électorales sur les médias sociaux. Pourtant, reconnaître les effets du microciblage ne revient pas à reconnaître la théorie de la seringue hypodermique, au contraire. Le microciblage réussit à cibler très spécifiquement les électeurs indécis, qui sont les plus réceptifs aux effets de la campagne. Le contenu publicitaire personnalisé qui leur est attribué tient compte de leur profil psychologique pour les persuader en utilisant notamment leurs peurs. La persuasion ne s'adresse donc pas à tous les électeurs, mais à ceux qui y sont réceptifs. De nombreuses preuves indirectes permettent de le démontrer comme les comportements rationnels des acteurs économiques qui renoncent à la publicité classique pour favoriser celle numérique, ou encore les interdictions de l'Union européenne de cibler les enfants, et enfin la victoire de Trump aux Etats-Unis dans des bastions démocrates avec une marge de moins de 2%.

Mais au-delà de la victoire de Trump, ou de ceux qui ont bénéficié comme lui du microciblage politique, ce sont les plateformes et le capitalisme de surveillance qui sont renforcés et institutionnalisés par l'usage du microciblage dans le domaine politique (III).

⁷² FRAU-MEIGS Divina, « Chapitre 14. Les enjeux de la réception : comment mesurer l'influence de la désinformation ? », *op. cit.*, 2021, p. 323-345.

III. Les grands gagnants du microciblage comme cheval de Troie : les GAFAM et le capitalisme de surveillance et d'influence

Dans la troisième et dernière partie de notre plan, nous plongerons au cœur du fonctionnement de ce système complexe, en mettant en lumière le rôle central du microciblage politique comme cheval de Troie du capitalisme de surveillance et d'influence.

Le surplus comportemental est la principale source de revenus des géants du numérique. Il est à la base du fonctionnement du marché publicitaire. C'est par la transformation du surplus-comportemental que le microciblage est possible. Et c'est grâce au microciblage que les GAFAM peuvent prospérer sur le marché publicitaire numérique (A).

Le microciblage politique et commercial sont étroitement liés. Les interconnexions étroites entre les acteurs des GAFAM et les acteurs politiques, ainsi que le rôle crucial du marché électoral comme porte d'entrée au marché commercial en sont l'illustration. Les GAFAM sont des acteurs incontournables et désormais indispensables dans le paysage politique et économique. Les acteurs politiques dépendent de plus en plus des données des plateformes pour mener leur campagne. Cela participe à l'institutionnalisation du capitalisme de surveillance, caractérisée par une politique du laisser-faire de l'Etat (B).

A. Le microciblage politique ou le cheval de Troie du capitalisme de surveillance et d'influence

Le capitalisme de surveillance est le grand vainqueur du microciblage politique comme cheval de Troie car les acteurs politiques en utilisant le microciblage politique deviennent dépendants des plateformes et de l'utilisation des données, ils ne peuvent dès lors plus contester l'usage des données par ces dernières. En effet, le Capitalisme de surveillance se nourrit de la collecte et la transformation de ces données, les politiques ne sont plus en position de réguler ce capitalisme en devenant dépendant des outils qu'il leur fourni.

Dans cette partie, nous verrons que les données sont ce que Shoshana Zuboff conceptualise sous le terme de surplus-comportemental (1). Ce concept est central pour comprendre le fonctionnement du capitalisme de surveillance, et du microciblage.

Nous verrons enfin, qu'en utilisant le microciblage dans le domaine politique, les candidats favorisent à légitimer le microciblage dans son utilisation commerciale. Cela permet d'accroître la puissance économique et politique des GAFAM, lesquels deviennent ainsi des acteurs indispensables (2).

1. Le surplus comportemental au cœur du capitalisme de surveillance

Le surplus-comportemental⁷³ est la source de revenu principale des plateformes (a). En effet, le succès publicitaire des GAFAM repose sur sa capacité à accaparer l'expérience humaine et la transformer en modèle prédictif. Ces modèles prédictifs permettent de cibler avec précision les consommateurs pour influencer leur comportement et les pousser à consommer (b).

⁷³ Zuboff Shoshana, *L'âge du capitalisme de surveillance*, op. cit., 2022.

a) Le surplus-comportemental comme source principale de revenu des GAFAM

Le moteur de recherche « Google », lors de sa création en 1998, est pensé comme un outil à la disposition de tous. Il est accessible gratuitement et sans publicité.

Néanmoins, en 2001, Google est au bord de la faillite. En effet, la crise des DOT-COM⁷⁴ de 2001 impacte fortement les firmes financées en capital-risque. Google ne peut plus rembourser les investisseurs. Dans le même temps, Apple expérimente sur l'Ipod l'usage des « cookies » pour cibler les goûts musicaux des utilisateurs. Les « cookies », utilisés d'abord par le moteur de recherche « Netscape » en 1994⁷⁵, permettent aux sites de récolter des données sur les utilisateurs (temps passé sur la page web, combien de temps entre plusieurs sessions, garder en mémoire le contenu d'un panier entre deux sessions, ...). Dans ce contexte, Google décide pour gagner de l'argent d'utiliser les données générées par les utilisateurs, ce que Shoshana Zuboff appelle « surplus comportemental »⁷⁶.

Le terme de surplus-comportemental fait référence au concept marxiste de « plus-value ». La plus-value est la différence entre la valeur ajoutée par le travailleur à la marchandise et la valeur de la force de travail nécessaire pour la produire. Le travailleur crée une valeur « en plus » qui enrichit son employeur (détenteur du capital). Selon le courant marxiste, l'ouvrier travaille une partie du temps pour couvrir son salaire, et le reste du temps est un travail gratuit qui crée la « plus-value ». Dans le cas du « surplus-comportemental », ce sont les données comportementales récoltées « en plus » de celles nécessaires à la production ou l'amélioration du service fourni, et qui produisent un revenu pour la firme. La « plus-value » est le fruit de l'exploitation de la force de travail du salarié, et le « surplus-comportemental » est le fruit de l'exploitation de « l'expérience humaine »⁷⁷ et de la vie privée des utilisateurs.

⁷⁴ La crise des DOT COM est une bulle spéculative qui en éclatant à affecter la valeur des nouvelles technologies.

⁷⁵ VALLUY Jérôme, « HUMANITÉ ET NUMÉRIQUE(S) », *op. cit.*, 2023.

⁷⁶ Zuboff Shoshana, *L'âge du capitalisme de surveillance*, *op. cit.*, 2022.

⁷⁷ Zuboff Shoshana, *L'âge du capitalisme de surveillance*, *op. cit.*, 2022.

Ces données fournissent un revenu considérable aux GAFAM qui les collectent et les vendent sous forme de données prédictives sur le marché « des comportements futurs »⁷⁸. Concrètement une entreprise qui souhaite vendre son produit - disons des chaussures de running produites à partir de matières recyclées en France – s’adresse à Google qui lui fournit une liste de personnes qui pourraient acheter son produit. Ces personnes seraient probablement des jeunes (30 ans), sportifs, de classes supérieures – les fameux « jeunes cadres dynamiques ». Ces prédictions sont modélisées par des intelligences artificielles qui analysent des milliards de données – le surplus comportemental. Dans notre exemple, l’entreprise pourra cibler un public sensible aux problèmes environnementaux, sportif et aisé qui sera plus à même d’acheter ce type de basket. Le microciblage publicitaire est ainsi la source de revenu principale des GAFAM⁷⁹. Les GAFAM ne vendent pas les données personnelles – cela serait comme vendre un gisement plutôt que vendre le pétrole qu’on en extrait- mais leurs prédictions publicitaires.



Ivan Manokha s’est aussi intéressé aux données au regard de la théorie marxiste. Selon le sociologue, les données seraient une nouvelle « marchandise fictive » telle que définie par Karl Polanyi, en plus de la terre, de la monnaie et du travail⁸⁰. Les données sont selon cette théorie des marchandises « *qui ne sont pas initialement produites pour la vente, mais qui sont objectifiées dans le capitalisme* »⁸¹. Le capitalisme de surveillance existe parce qu’il utilise les données comme

⁷⁸ Zuboff Shoshana, *L’âge du capitalisme de surveillance*, op. cit., 2022.

⁷⁹ En 2023, 25,2% des revenus de Facebook devraient être générés par la publicité digitale contre 7,1% pour Amazon. En 2021, le chiffre d’affaires publicitaire de Google s’élevait à 209,49 milliards de dollars et la publicité digitale comptait pour 28,6% de ses revenus. Source : Statista, Maxime Gautier, octobre 2023 - <https://fr.statista.com/statistiques/1368090/publicite-digitale-part-revenus-entreprises/>

⁸⁰ Polanyi K., *The Great Transformation: The Political and Economic Origins of Our Time*, New York, Farrar & Rinehart, 1944.

⁸¹ MANOKHA Ivan, « Le scandale Cambridge Analytica contextualisé », op. cit., 2018, p. 39-59.

matière première et les transforme en quelque chose de monétisable créant une plus-value au passage.

Pour ces deux auteurs, les données sont donc la matière première du capitalisme de plateforme (pour Manokha) et de surveillance (pour Zuboff) en permettant aux GAFAM de s'enrichir sur le marché publicitaire (b).

b) Le fonctionnement du marché publicitaire

Le marché publicitaire est basé en partie (un quart) sur la méthode du « real time bidding ». Le profil de l'internaute est mis aux enchères pendant qu'il charge une page web, les annonceurs paramètrent des algorithmes pour remporter le bandeau publicitaire. Les algorithmes ne surenchérissent que s'ils calculent, à partir des données fournies, que l'internaute a une forte probabilité de cliquer sur la publicité. Google a mis en place le système publicitaire digital le plus efficace et rentable avec le service Google Ads comme l'explique Cardon⁸². Les recherches des internautes sont mises aux enchères. Les publicitaires se disputent l'emplacement publicitaire en haut des résultats de recherche. Le système d'enchères est celui de Vickrey qui consiste pour le gagnant de l'enchère à ne payer la mise que du second. Les publicités ressemblent à une information avec un lien hypertexte pour accéder à un site internet. Enfin, l'annonceur ne paie Google que si l'internaute clique sur le lien, on parle de coût par clique. La norme du marché est plutôt le coût pour mille affichages. Google ne se rémunère donc que si la publicité fonctionne. Cela montre bien encore une fois l'efficacité du microciblage (cf Annexe n°9) qui montre l'augmentation des revenus publicitaires de Google). Le contenu de la page publicitaire doit être pertinent au regard de la requête de l'utilisateur sinon Google se réserve le droit de faire apparaître en premier une publicité qui correspond mieux aux attentes de l'utilisateur même si le publicitaire a payé moins.

Enfin Cardon conclut sur le service Google Ads que : « *Ce que nous écrivons dans la barre recherche du moteur, c'est une question, une demande, une chose que nous ne savons pas, que nous aimerions connaître ou faire. Les données sur le futur de l'utilisateur, sur ses intentions, ses*

⁸² CARDON Dominique, « La publicité en ligne », *op. cit.*, 2019, p. 310-320.

souhaits et ses désirs sont pour les annonceurs bien plus pertinentes que le profilage des données antérieures. Voilà comment le modèle de Google a détruit tous les équilibres entre acteurs sur le marché publicitaire ». Le modèle publicitaire de Google se fonde donc sur le microciblage, sur la capacité de prévoir le comportement des consommateurs et de l'influencer. Tristan Nitot, ancien membre de la CNIL décrit ainsi le microciblage comme un phénomène qui « *rend difficilement perceptible l'ampleur de la collecte de données et de la surveillance qui en découle, puisque cette collecte est indolore, invisible, largement faite à notre insu (...)* »⁸³.

Ainsi, le surplus comportemental est au cœur du capitalisme de surveillance car une fois transformé, il permet de cibler les consommateurs de manière précise avec des publicités personnalisées. Le surplus comportemental est donc à la base du microciblage politique et commercial.

Plus les GAFAM ont du surplus-comportemental, plus elles peuvent affiner et perfectionner leurs outils de microciblage. Nous allons dorénavant étudier - pour comprendre comment le microciblage politique est le cheval de Troie du capitalisme de surveillance- la porosité entre le champ politique et commercial (2).

2. La convergence entre champ politique et champ commercial

Le champ politique et le champ commercial convergent en de nombreux points. Tout d'abord, il existe une porosité entre ces deux milieux permettant aux acteurs de naviguer d'un champ à l'autre, servant des intérêts communs (a). Ensuite, les pratiques similaires des deux champs permettent leur renforcement mutuel, ainsi le microciblage politique permet d'ouvrir la voie au marché commercial pour les cabinets de conseils (b).

⁸³ PEREZ LAGOS Camila, « Rendre visibles les conséquences de la surveillance numérique. Le cas du « scandale » Cambridge Analytica », *Communication*, vol. 37, 2020, [<https://doi.org/10.4000/communication.13252>].

a) Les interconnexions entre les acteurs des GAFAM et les acteurs politiques

Shoshana Zuboff explique que Barack Obama a tiré profit pour ses élections des « compétences » de Google pour prédire et modeler les comportements électoraux⁸⁴. En effet, Eric Schmidt -PDG de Google de 2001 à 2011- a tenu un rôle important dans la campagne d'Obama en mettant en place la stratégie de microciblage comportemental de l'équipe. Et une fois Obama élu, Schmidt est apparu à ses côtés lors de sa première conférence de presse. Il a aussi été nommé pour rejoindre le Siège du Conseil économique de transition (Transition Economic Advisory Board)⁸⁵. Schmidt est donc devenu un conseiller proche d'Obama, notamment sur les questions économiques et de data. Google Transparency Project- GTP- (devenu « Tech Transparency Project ») – mené par l'ONG « Campaign for Accountability »⁸⁶ - expose les liens entre Google et le gouvernement. GTP a publié un rapport sur les mouvements de personnel entre Google (et les entreprises qui lui sont affiliées) et le gouvernement Obama de 2008 à 2016⁸⁷. Les résultats de ce rapport montrent une porosité entre ces deux milieux. Shoshana Zuboff le résume ainsi : 197 personnes issues du gouvernement (dont 22 fonctionnaires de la Maison-Blanche) ont rejoint Google et à l'inverse 61 employés de la firme ont intégré le gouvernement dont 31 cadres ont rejoint la Maison-Blanche ou les conseils consultatifs fédéraux en rapport direct avec l'activité de Google.

On peut supposer que le personnel de Google ayant rejoint le gouvernement ait pu être favorable aux politiques de développement des data ou de « laisser faire » pour ne pas entraver l'innovation. En effet, en ayant évolué dans un environnement tel que Google, pendant des années, le personnel a développé des valeurs cohérentes avec les intérêts de la firme. Ces liens réciproques entre le gouvernement et la firme favorisent l'inaction du gouvernement en matière de régulation des données, sous couvert de ne pas entraver l'innovation. Civis Analytics est aussi une illustration de ces liens comme le révèle Tech Transparency Project⁸⁸. L'unique investisseur de cette entreprise

⁸⁴ ZUBOFF Shoshana, *L'âge du capitalisme de surveillance*, op. cit., 2022.

⁸⁵ Robert Reich, « Obama's Transition Economic Advisory Board : The Full List », US News & World Report, November 7, 2008. - <https://www.nytimes.com/2008/11/08/us/politics/08advisors.html>

⁸⁶ <https://campaignforaccountability.org/>

⁸⁷ <https://www.techtransparencyproject.org/articles/googles-revolving-door-us>

⁸⁸ <https://www.techtransparencyproject.org/articles/civis-analytics>

est Eric Schmidt. Il a recruté au moins 27 des experts en data analytics ayant travaillé pour la campagne d'Obama, selon les données compilées par le Google Transparency Project. En octobre 2013, la réforme des soins de santé d'Obama prévoit la mise en place du site « HealthCare.gov » qui a crashé dès son lancement. Todd Park - responsable des technologies de la Maison Blanche- a alors demandé de l'aide à Civis pour réparer le site. Cela a donc permis la présence d'anciens employés de Google à la Maison Blanche pour aider à mettre en œuvre des politiques du gouvernement. Google, à travers Schmidt, a réussi à s'intégrer dans l'élaboration et l'exécution des politiques. Associated Press en 2015 a révélé que le site HealthCare.gov a partagé des données personnelles des utilisateurs à des sociétés tierces comme Google⁸⁹, reste à savoir si les techniciens de Civis ont permis cette fuite de données.

L'importance de Schmidt ne réside donc pas seulement dans son intervention dans la campagne d'Obama mais aussi dans sa capacité à être devenu un allié du Président l'aidant à avancer sur ses priorités. Son influence dépasse la présidence d'Obama puisqu'il devient président de la « Defense Innovation Board » de 2016 à 2020) et de la Commission de sécurité nationale sur l'intelligence artificielle de 2018 à 2021.

Ainsi, Obama n'est pas le seul à avoir tissé des liens avec les GAFAM. Les GAFAM ont obtenu depuis leur création des contrats avec le département de la Défense⁹⁰. De plus, les GAFAM financent les campagnes de candidats politiques depuis 1990 et ont un budget très important pour le lobbying avec une nette augmentation ces dernières années (multiplication de ces dépenses par 19 en moyenne depuis 2010). Ces chiffres sont issus de l'article de Charles Thibout sur les GAFAM et l'Etat⁹¹ : Alphabet (Google) a contribué à hauteur de 4,4 millions de dollars au comité de campagne de Joe Biden en 2020, Microsoft a hauteur de 2,4 millions, Amazon 2,3 millions, Apple 1,9 million, et Facebook 1,6 million. L'auteur nous apprend aussi que 82% des lobbyistes recrutés

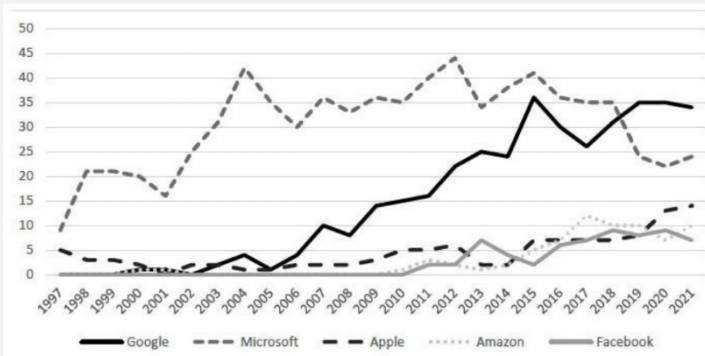
⁸⁹ <https://www.theguardian.com/us-news/2015/jan/23/obama-release-customer-data-healthcare-gov>

⁹⁰ THIBOUT Charles, « Les GAFAM et l'État : réflexion sur la place des grandes entreprises technologiques dans le champ du pouvoir », *Revue internationale et stratégique*, n° 1, vol. 125, 2022, p. 75-88, [https://doi.org/10.3917/ris.125.0075].

⁹¹ *Ibid.*

par les plateformes sont d'anciens employés du Congrès, de la Maison blanche, ou des agences fédérales.

Figure n° 3
EMPLOYÉS DES GAFAM MEMBRES DE COMITÉS CONSULTATIFS FÉDÉRAUX (1997-2021)



— Source : données FACA - ©Charles Thibout

Les employés des GAFAM sont aussi des membres des comités consultatifs fédéraux, conseillant ainsi les politiques directement.

La porosité des relations entre l'Etat, les politiques et les GAFAM démontre à la fois le pouvoir d'influence des GAFAM et témoigne de la dépendance institutionnelle et politique envers eux.

S'il existe une porosité des relations entre l'Etat et les GAFAM, il existe également une porosité entre le marché électoral et celui commercial (b).

b) Le marché électoral comme porte d'entrée au marché commercial

Les instituts de sondage, tout comme les GAFAM, vendent leurs capacités de prédiction. Ils travaillent sur deux pans du « marché des comportements futurs ». Ils font des prédictions, en effet, à la fois, dans le champ politique et à la fois dans le champ commercial. Les sondages politiques, en annonçant à l'avance le vainqueur d'une élection, démontrent l'efficacité de leur prédiction. Cela leur permet de promouvoir leurs services et de les vendre sur le marché commercial – plus rémunérateur.

Le marché électoral est certes peu rémunérateur, mais il donne une légitimité aux instituts pour ensuite vendre leurs services de prédiction à des entreprises privées. On peut étendre cette analyse aux databrokers qui vendent eux aussi leur capacité de prédiction. Le marché électoral est alors un tremplin vers le marché privé plus rémunérateur. Les acteurs économiques sont rationnels, ils sont à la recherche de profits, ils se tournent donc vers la technique publicitaire la moins couteuse et la plus efficace : le microciblage.

Kaiser témoigne au sujet du travail à CA après la victoire de Trump, qu'ils recevaient des appels incessants pour collaborer avec eux. Cela démontre que le marché politique ouvre la voie au marché commercial bien plus lucratif. Elle écrit « *Au lendemain de la victoire de Trump, nous avons enfin pu commencer à faire de la publicité pour le rôle que nous avons joué dans la campagne - et maintenant tout le monde voulait que nous fassions la même chose pour eux (...) Des PDG de grandes entreprises américaines et étrangères nous ont demandé de faire des campagnes commerciales - Unilever, MGM, Mercedes...* »⁹². Une autre citation de Kaiser témoigne du plan de CA d'utiliser le marché politique pour conquérir celui commercial : « *Je suppose que j'aurais dû m'en douter : comment Cambridge Analytica Commercial pourrait-il décoller sans plus d'une victoire très médiatisée de Cambridge Analytica ?* »⁹³.

En résumé, le microciblage politique permet de cibler les électeurs susceptibles d'être réceptifs à l'influence électorale. Des publicités personnalisées constituent des manipulations numériques possibles grâce au microciblage politique basé sur le surplus-comportemental. Les cabinets de conseil à l'origine de ce ciblage politique peuvent capitaliser leur victoire dans leur argumentaire de vente pour intégrer le marché commercial plus lucratif que celui électoral, ce qui renforce le capitalisme de surveillance. Mais l'utilisation du microciblage en politique renforce surtout le capitalisme de surveillance, en rendant les politiques dépendants à cet outil fourni par les plateformes. Les politiques sont alors dépendants des plateformes et ne remettent pas en question la collecte du surplus-comportemental. Leur dépendance se traduit même par une porosité entre les deux champs.

Ainsi ce sont surtout les plateformes qui bénéficient de l'usage du microciblage politique. Elles deviennent indispensables aux campagnes électorales et peuvent continuer de collecter des données qui sont l'élément fondateur de leur modèle économique (B).

⁹² Traduction de "In the aftermath of Trump's victory, we were finally able to start advertising the role we'd had in the campaign—and now everyone wanted us to do the same for them (...) CEOs of major U.S. and foreign corporations wanted us for commercial campaigns— Unilever, MGM, Mercedes" KAISER Brittany, *L'affaire Cambridge Analytica*, op. cit., 2020.

⁹³ "Traduction de l'extrait : "I suppose I should have seen it coming: how could Cambridge Analytica Commercial get off the ground without more than one high-profile win from Cambridge Analytica Political?" KAISER Brittany, *L'affaire Cambridge Analytica*, op. cit., 2020.

B. Les GAFAM : des acteurs incontournables devenus indispensables

Les GAFAM sont des acteurs incontournables du numérique et de l'économie. Mais ils sont également devenus des acteurs indispensables grâce au microciblage politique. En effet, les candidats politiques et les cabinets de conseil dépendent des données de ces plateformes et de leur capacité publicitaire (1).

Cette dépendance permet d'institutionnaliser le capitalisme de surveillance, en laissant les GAFAM agir dans le silence du droit (2).

1. La dépendance des acteurs politiques aux données

La dépendance des acteurs politiques aux données se traduit par une standardisation des campagnes électorales en ligne (a), puisque les candidats font appel à des cabinets de conseil politique disposant des mêmes ressources (b).

a) La standardisation des campagnes électorales en ligne

Le digital est un passage obligatoire pour la communication des politiques aujourd'hui. Au-delà des pratiques communicationnelles sur les réseaux sociaux, c'est l'usage des données et du microciblage qui s'est répandu. Le microciblage et les données ne sont pas utilisées de la même manière dans l'Union européenne et aux Etats-Unis (cf. b).

La France a notamment importé les pratiques de microciblage politique avec des data brokers comme LiegeyMullerPons (LMP) ou encore la plateforme NationBuilder⁹⁴ utilisée par

⁹⁴ NationBuilder existe depuis 2009 et a été utilisé par Obama en 2012.

Jean-Luc Mélenchon en 2017 ou Bruno Le Maire pour la primaire de la droite en 2016⁹⁵. NationBuilder propose de créer une interface avec tous les éléments essentiels de la campagne au même endroit et qui communiquent entre eux : crowdfunding, organisation des militants, base de données, communication. Par exemple, NationBuilder recherche les réseaux sociaux de toutes les personnes présentes dans la base à partir de leur adresse mail. NationBuilder importe les informations publiques accessibles. À partir de là, les individus peuvent être segmentés par profession, âge, activités, etc, et ciblés en fonction. Cette fonctionnalité a été interdite en France par la CNIL⁹⁶. LMP proposait quant à elle le logiciel de gestion 50+1 (devenu Explain). Hollande et Macron ont fait appel à leurs services pour remporter leur élection présidentielle. Les fondateurs de cette agence sont G. Liegey, A. Muller et V. Pons. Ils se sont rencontrés aux États-Unis à Harvard et ont participé bénévolement à la campagne d'Obama en 2008 découvrant la science des données.

Que cela soit aux États-Unis, en France, ou dans le reste du monde, les candidats se reposent de plus en plus sur la science des données pour remporter une élection. On assiste à une externalisation de la communication politique à des entreprises privées. Les politiques deviennent dépendants des data brokers et des logiciels d'analyse de données. L'utilisation du microciblage par les candidats conduit à un renforcement de la collecte et de l'utilisation des données, qui est à la base du capitalisme de surveillance. Se pose aussi la question du stockage de données personnelles à des fins politiques dans les serveurs d'entreprises privées comme le soulève Philippe Haag : « finalement, l'entreprise privée se retrouve indirectement détentrice sous contrat de millions de données relatives à des utilisateurs personnels, par l'intermédiaire de clients qui ne pensent pas nécessairement à la problématique de la géographie du stockage des données. »⁹⁷. C'est le cas de NationBuilder qui devient détentrice de données des utilisateurs et électeurs français.

En novembre 2016, la CNIL a critiqué sévèrement la fonctionnalité de NationBuilder permettant de recouper les données en utilisant les informations accessibles sur les réseaux sociaux

⁹⁵ THEVIOT Anaïs et TREILLE Éric, « Mobiliser par les données. Les stratégies numériques de campagne des candidats à la primaire de la droite et du centre de 2016 », *Politiques de communication*, n° 1, vol. 12, 2019, p. 71-96, [<https://doi.org/10.3917/pdc.012.0071>].

⁹⁶ THEVIOT Anaïs, « Usages électoraux des big data. Un modèle américain ? », *Revue internationale de politique comparée*, n° 2-3, vol. 29, 2022, p. 157-190, [<https://doi.org/10.3917/ripc.292.0157>].

⁹⁷ Philippe Haag. La communication numérique électorale : nouvelle étape de la marchandisation du politique ?. Sciences de l'information et de la communication. Université Bourgogne Franche-Comté, 2022. Français.

des électeurs. Elle a aussi critiqué l'application « Knockin » utilisé par Nicolas Sarkozy pendant la primaire⁹⁸.

b) La collecte de données multiples par les différents data brokers

Les données sont la matière première du capitalisme de surveillance devenant dès lors une marchandise. Les violations de la vie privée sont nécessaires et inévitables dans ce modèle économique. Une partie de l'économie toujours plus importante repose sur cette atteinte à la vie privée. Fabrice Rochelandet a établi dès 2010 une classification précise des données personnelles collectées et des techniques pour y parvenir⁹⁹.

De nombreuses données sont accessibles publiquement, Explain en a fait sa spécialité. D'autres sont achetées à des entreprises. Les data brokers se vendent entre eux les données et collaborent avec les plateformes pour accéder à certaines données. Les plateformes bénéficient aussi de ces échanges en élargissant ses bases de données. Les plateformes achètent le plus de start-up et de plateformes possibles afin de continuer d'augmenter leurs bases de données comme Google avec Youtube, ou Facebook avec Instagram¹⁰⁰.

⁹⁸ THEVIOT Anaïs et TREILLE Éric, « Mobiliser par les données », *op. cit.*, 2019, p. 71-96.

⁹⁹ ROCHELANDET Fabrice, Économie des données personnelles et de la vie privée. La Découverte, « Repères », 2010 : <https://www-cairn-info.ezpaarse.univ-paris1.fr/Economie-des-donnees-personnelles-et-de-la-vie-pri--978270715765>

¹⁰⁰ MANOKHA Ivan, « Le scandale Cambridge Analytica contextualisé », *op. cit.*, 2018, p. 39-59.

Tableau 1 : Une classification des informations individuelles

Données objectives	
Données d'identification et de contact	Identité civile ; adresse postale ; numéro de téléphone ; numéro d'immatriculation d'un véhicule ; numéro du permis de conduire ; adresse électronique ; références bancaires ; numéro de carte bancaire ; numéro de Sécurité sociale ; pseudonyme sur Internet...
Données physiques et de signalement	Taille ; poids ; couleur et écart entre les yeux ; état de santé ; maladies contagieuses ; vaccins ; empreintes digitales ; photographie ; voix...
Données sociodémographiques	Date de naissance ; âge ; genre ; statut marital ; nombre d'enfants ; niveau d'études ; profession...
Données juridiques	Capacité juridique ; casier judiciaire ; amendes...
Données financières et foncières	Solde du compte bancaire ; crédits et dettes ; fréquence des impayés ; interdit bancaire ; allocations sociales ; pensions alimentaires versées/reçues ; propriété foncière ; hypothèques...
Données subjectives	
Préférences et centres d'intérêt	Orientation sexuelle ; préférences alimentaires, vestimentaires et culturelles ; destinations touristiques préférées...
Opinions et activités politiques, religieuses ou syndicales	Opinions politiques émises publiquement ; adhésion à un syndicat ; croyances intimes déclarées ou manifestées publiquement ; signature d'une pétition...
Données comportementales	Apparence ; élocution et style de langage ; types d'achat et établissements fréquentés ; pratiques et fréquences des loisirs ; consommation d'électricité ou d'eau ; utilisation d'un service public ; données de connexion et navigation sur Internet ; consommation de drogues (alcools, tabac, stupéfiants)...
Données géographiques	Lieux de retraits d'argent et de paiement par carte bancaire (péage...) ; bornes d'enregistrement par puces sans contact ; identification Bluetooth...
Données relationnelles	Taille du réseau social ; fréquence des rencontres ; nombre d'amis, de partenaires sexuels ; participation à un club ou à une association ; appels téléphoniques, e-mails, SMS reçus et envoyés quotidiennement...

Extrait de : ROCHELANDET Fabrice, *Économie des données personnelles et de la vie privée*. La Découverte, « Repères », 2010 : <https://www-cairn-info.ezpaarse.univ-paris1.fr/Economie-des-donnees-personnelles-et-de-la-vie-pri-9782707157652.htm>

Tableau 2 - Exemples de techniques de collecte et d'exploitation de données personnelles

Techniques de collecte	
Formulaires	- Formulaires d'abonnement à un service, à une revue, etc. - Données de transaction lors d'un achat en ligne (adresse de livraison, données bancaires, âge, genre, préférences, etc.)
Informations divulguées publiquement	- Blogs personnels - Pages sur un réseau social - Life logging (forme d'exhibition de soi)
Traces collectées à l'insu de la personne et tromperie	- Cookies, fichiers log de connexion à un site Internet - Données enregistrées et associées à un identifiant (sur des newsgroups, des forums...) - Géolocalisation - Logiciels espions, piratage de bases de données, de réseaux de collecte - Hameçonnage (phishing), lettres-chaînes...
Informations divulguées par des tiers	- Commentaires ou notations sur des réseaux sociaux, newsgroups... - Achat de bases de données auprès d'entreprises
Données obtenues par recoupement, autogénération, recherche automatisée, etc.	- DP obtenues via le fonctionnement de services en ligne (réseautage social) - Exemple des détails très précis de la vie privée de « Marc L. » (revue <i>Le Tigre</i>, nov.-déc. 2008)
Modes d'exploitation	
Exposition de soi, de sa vie privée	- Réseaux sociaux (les anciens copains...) - Blogs intimes
Recherche d'informations sur des tiers, surveillance, renseignement, notation	- Interrogation d'une base de données - Requête sur un moteur de recherche - Fichage par les administrations (police, assurance sociale...) ou par certaines entreprises (banques, assurances...)
Revente de DP	- Données marketing - Listes d'e-mails - Bases de numéros de cartes de crédit - Data brokers (ChoicePoint...)
Personnalisation de l'offre	- Gestion de la relation client - Services Web 2.0 - Discrimination par les prix - Conditions d'embauche - Polices d'assurance
Offre contextualisée	- Mise en relation de personnes en mobilité - Promotion de services à proximité et/ou à un moment précis du déplacement d'un individu
Exploitation marketing	- Envoi massif de messages non sollicités - Promotion personnalisée
Utilisations illégales ciblées	- Usurpation d'identité - Fraude bancaire - Extorsions, chantage...

Extrait de : ROCHELANDET Fabrice, *Économie des données personnelles et de la vie privée*. La Découverte, « Repères », 2010 : <https://www-cairn-info.ezpaarse.univ-paris1.fr/Economie-des-donnees-personnelles-et-de-la-vie-pri-9782707157652.htm>

Les services gouvernementaux notamment de la Défense -mais on peut aussi penser aux services de police et aux services fiscaux- sont intéressés par ces données. A titre d'exemple, en 2013 Edward Snowden a révélé le système de partage de données des GAFAM à la NSA, laquelle avait alors accès aux données personnelles de millions d'utilisateurs. Un autre exemple est celui de

l'entreprise israélienne Terrogeance qui a élaboré une base de données de reconnaissance faciale à partir des sources des plateformes¹⁰¹.

Il existe certes des vols de données comme a pu le pratiquer CA avec des données Facebook. Mais les données étant une marchandise, les immixtions dans la vie privée des utilisateurs dépassent le cadre du vol. En effet, c'est la vie privée des utilisateurs qui, d'une certaine façon, est monétisée. C'est pourquoi Zuboff parle d'accapuration de « l'expérience humaine à des fins commerciales »¹⁰².

Les plateformes chercheront toujours à contourner la législation et à l'amoindrir car elles dépendent de la collecte de données, leur modèle économique repose sur la violation de la vie privée des utilisateurs. Manokha écrit très justement : « à cet égard, si ceux qui s'indignent de l'action de Cambridge Analytica ne remettent pas en cause toute forme de collecte de données, ils contribueront à renforcer la normalisation des pratiques de surveillance adoptées par le capital de plateforme et ses partenaires et, ce faisant, serviront involontairement leurs intérêts »¹⁰³. En d'autres termes s'indigner des vols de données, mais ne pas questionner la collecte de données en elle-même revient à dédouaner les plateformes de leur responsabilité et ainsi faire perdurer le capitalisme de surveillance (2).

2. L'institutionnalisation du capitalisme de surveillance

L'institutionnalisation du capitalisme de surveillance est permise par la politique du « laisser-faire » de l'Etat, notamment américain. L'Etat est dépendant des plateformes à la fois stratégiquement, politiquement et économiquement. L'Etat et les politiques ne souhaitent pas amoindrir le pouvoir de collecte des GAFAM alors même qu'ils dépendent de ces données (a).

¹⁰¹ Terrogeance, « Biometric Database Enhancement », en ligne sur <https://www.terrogeance.com/capabilities/biometric-database-enhancement/> issu de *Ibid*.

¹⁰² ZUBOFF Shoshana, *L'âge du capitalisme de surveillance*, op. cit., 2022.

¹⁰³ MANOKHA Ivan, « Le scandale Cambridge Analytica contextualisé », op. cit., 2018, p. 39-59.

Enfin, les GAFAM ont un pouvoir d'influence sans précédent avec les Etats-Unis comme allié. Elles dépensent des millions d'euros dans des stratégies de plaidoyer pour s'assurer une législation favorable (b).

a) Une politique du laisser faire

La vitesse de développement des technologies laisse à penser que l'Etat serait dépassé. En effet, ce dernier serait dépassé par les évolutions technologiques et leur expansion sociétale. En réalité, comme le montre Jérôme Valluy, l'Etat est un acteur du « laisser-faire », notamment les différents gouvernements étasuniens¹⁰⁴.

L'Etat américain a toujours eu un lien particulier à l'informatique. Les grandes entreprises de la tech sont nées aux Etats-Unis, notamment après qu'IBM ait créé la carte perforée en 1890 qui permet d'informatiser le recensement. Les Etats-Unis ont longtemps été les premiers consommateurs d'informatiques. Ils ont encouragé l'innovation et l'ont accompagnée comme avec le Decency-Act qui prévoit l'irresponsabilité juridiques des plateformes en 1996. Mais c'est devenu d'autant plus marquant après les attentats du 11 septembre 2001¹⁰⁵.

Cet événement a profondément marqué les Etats-Unis qui, pour la première fois, ont subis une attaque sur leur territoire. La guerre contre le terrorisme est alors une priorité absolue pour les Etats-Unis. La lutte anti-terroriste devient une excuse à la surveillance de masse qui commençait déjà aux Etats-Unis. En effet, William Binney, ancien employé de la NSA est devenu lanceur d'alerte en 2001 lorsqu'il a dénoncé le « gaspillage » d'argent de la NSA dans des programmes qu'il juge inefficaces¹⁰⁶. Son équipe et lui travaillaient sur le logiciel « ThinThread » qui permettait de crypter des informations relevant de la vie privée des personnes tout en identifiant les risques et menaces pesant sur les Etats-Unis à l'aide d'IA. Ainsi, selon les experts de la NSA, ce logiciel avait fait ses preuves et était opérationnel. Mais trois semaines avant les attentats du 11 septembre 2001, Michael V. Hayden fait annuler le projet au profit du logiciel « Trailblazer » bien plus coûteux et

¹⁰⁴ VALLUY Jérôme, « HUMANITÉ ET NUMÉRIQUE(S) », *op. cit.*, 2023.

¹⁰⁵ *Ibid.*

¹⁰⁶ <https://www.newyorker.com/magazine/2011/05/23/the-secret-sharer> et <https://www.zdnet.com/article/nsa-whistleblowers-security-thinthread-largest-failure-in-nsa-history/>

moins respectueux des libertés individuelles mais qui a permis à la NSA d'obtenir une ligne budgétaire bien plus conséquente qu'avec le logiciel ThinThread. En 2007 le projet est abandonné, ce qui conduit au logiciel PRISM. Ce dernier crée un système que J. Valluy nomme le « Système NSA/GAFAM »¹⁰⁷. Le SNG permet à la NSA d'accéder à toutes les bases de données des GAFAM. Ces bases de données stockent les milliards de données concernant les utilisateurs du monde entier dont des informations très privées (messages, photos, écoute téléphonique, etc).

Les intérêts de l'Etat et ceux des acteurs privés se sont ainsi rencontrés à la suite des attentats de 2001. D'une part, les Etats-Unis voulaient récolter un maximum de données et d'informations à travers le monde (officiellement pour lutter contre le terrorisme, mais les révélations Snowden ont permis de montrer également un intérêt économique des Etats-Unis à espionner les autres pays), et d'autre part les GAFAM et plateformes avaient un intérêt économique à récolter un maximum de données – qu'importe qu'il faille les partager au gouvernement. L'argument de Larry Page ne tient plus face à un tel système de surveillance de masse : *« en général, il est préférable que nos données soient entre les mains d'entreprises comme Google plutôt qu'entre celles d'un État dénué de réglementation pour obtenir ces données, car nous nous soucions manifestement de notre réputation. Je ne suis pas sûr que le gouvernement s'en soucie autant »*¹⁰⁸. Ce système montre la collaboration entre les services de l'Etat et les GAFAM. Il n'est alors plus possible de penser le renoncement des Etats à réguler les plateformes comme un signe de faiblesse et de dépassement. Les Etats choisissent de ne pas réglementer un système qui sert leurs intérêts en récoltant des informations qui pourraient leur servir.

Les candidats politiques eux-mêmes en ayant recours aux plateformes et au microciblage participent à la légitimation de ce nouveau capitalisme. En effet, la collecte de données leur permet de mieux connaître les électeurs à cibler et convaincre, facilitant de fait, le travail de campagne. Les candidats incorporent dans les pratiques démocratiques des pratiques marketing qui ne permettent pas un fonctionnement efficace de la Démocratie, et dont ils deviennent dépendants pour faire campagne.

¹⁰⁷ VALLUY Jérôme, « HUMANITÉ ET NUMÉRIQUE(S) », *op. cit.*, 2023.

¹⁰⁸ *Ibid.*

De plus, les Etats-Unis dépendent grandement du succès et du monopole des GAFAM. Ils leur permettent de s'imposer d'un point de vue technique, scientifique, économique et politique à travers le monde en diffusant leurs technologies. En légiférant sur la collecte des données, en limitant les revenus de ces plateformes, les Etats-Unis s'en prendraient à leurs « enfants chéris »¹⁰⁹ et s'affaibliraient économiquement. Charles Thibout résume judicieusement « *mais, au fond, quel responsable politique et directeur d'administration centrale, quel président et directeur d'agence ; bref, quels agents dominants des champs politique et bureaucratique auraient intérêt et se risqueraient à en finir avec les GAFAM ?* »¹¹⁰.

Les GAFAM ont ainsi un poids très important sur la création du droit (b).

b) L'influence des GAFAM sur la création et l'évolution du cadre juridique relatif aux données

Il est nécessaire de d'abord rappeler le poids des différences culturelles et juridiques entre les pays de l'Union européenne et les Etats-Unis. Kaiser écrit à ce propos :

*« Alexander and I both knew French law: as long as users opted in to share their data, they made a conscious, informed, and legal decision. The same was true in Britain. "This is not America," one of the men said. No, it was not, I thought. In America, users are automatically opted in through legislation that allows their unfettered data collection; there are few protections in the United States like those in France and the United Kingdom »*¹¹¹.

En Europe, sous l'impulsion de l'Allemagne, le droit à la vie privée est considéré comme un droit fondamental, absolu et inaliénable. La vie privée est protégée à l'échelle européenne par la Convention européenne des Droits de l'Homme à son article 8 :

« Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. Il ne peut y avoir ingérence d'une autorité publique

¹⁰⁹ Quessard, Maud. « Enfants chéris et enfants terribles des États-Unis », *Pouvoirs*, vol. 185, no. 2, 2023, pp. 31-38.

¹¹⁰ THIBOUT Charles, « Les GAFAM et l'État : réflexion sur la place des grandes entreprises technologiques dans le champ du pouvoir », *op. cit.*, 2022, p. 75-88.

¹¹¹ KAISER Brittany, *L'affaire Cambridge Analytica*, *op. cit.*, 2020.

dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. »

Aux États-Unis, le droit à la vie privée n'est pas explicitement mentionné dans la Constitution. Mais le quatrième amendement a été interprété comme une protection contre les perquisitions et les saisies abusives. Le droit à la vie privée est ainsi perçu comme une protection contre l'État avant tout. De plus, elle est mise en balance avec la liberté d'expression qui est beaucoup moins régulée qu'en Europe. En France, la liberté d'expression ne permet pas de tenir des propos discriminants alors qu'aux États-Unis, seul le « fighting word », c'est-à-dire l'incitation directe à la violence, est condamnable¹¹². Aux États-Unis, la liberté d'expression et d'information peut donc peser plus dans la balance que la protection de la vie privée en France. Les cultures juridiques de ces deux pays sont différentes, ce qui explique que la question de la protection des données personnelles ne soit pas traitée de la même manière. Ainsi, l'Union européenne s'est dotée d'un règlement relatif aux données (RGPD) mais pas les États-Unis. Certains États des États-Unis ont pu décider de légiférer et d'encadrer l'usage des données, mais ce n'est pas une loi fédérale. Les gouvernements successifs restent silencieux face aux évolutions des plateformes et de l'utilisation des données personnelles. C'est que Jean Carbonnier nomme le « non-droit ». Ce que la loi n'interdit pas est autorisé. Dans le silence de la loi, il est possible de faire, ainsi les GAFAM peuvent agir en utilisant ce flou juridique. Kaiser témoigne : « *It was a uniquely American opportunity. Data laws in countries such as the United Kingdom, Germany, and France don't allow such freedoms. That's why America was such fertile ground for Cambridge Analytica, and why Alexander had called the U.S. data market a veritable "Wild West"* »¹¹³. Elle explique avoir rencontré avec A. Nix l'équipe de campagne de N. Sarkozy pour leur proposer leurs services.

¹¹² BADOUARD Romain, « La régulation des contenus sur Internet à l'heure des "fake news" et des discours de haine », *Communications*, n° 1, vol. 106, 2020, p. 161-173, [<https://doi.org/10.3917/commu.106.0161>].

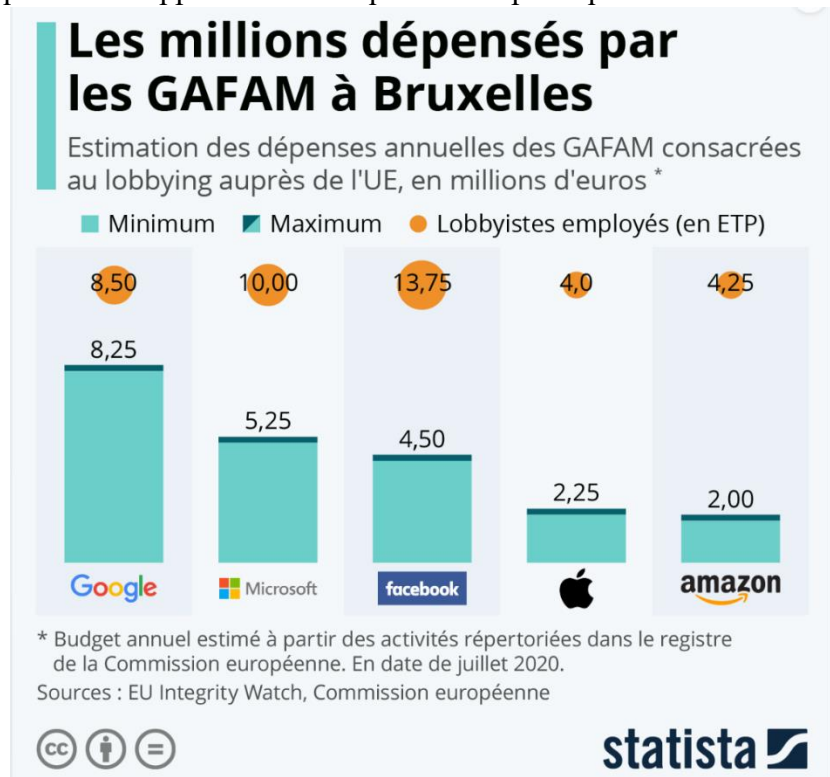
¹¹³ KAISER Brittany, *L'affaire Cambridge Analytica*, op. cit., 2020.

L'équipe aurait refusé d'utiliser leur solution car cela ferait un scandale si les Français apprenaient que N. Sarkozy avait utilisé les données personnelles des citoyens pour remporter l'élection.

« Some clients got dazed during the data analytics portion of a pitch, but the two executives seemed more keenly interested. They had questions about how CA obtained data, what we did with it in-house, and how microtargeting was done. But when Alexander finished up and asked if there were any questions, there was a decidedly dead pause. One of the men cleared his throat. "Non," he said. "This simply will not work." The other executive shook his head in agreement. "It is impossible," he said. "The French will never accept it." Alexander was as genuinely puzzled as I. "Because . . . ?" he asked. "The data, of course," one of the men said. "If people knew a candidate was doing this, it would mean defeat for certain. »¹¹⁴.

Ce manque de législation aux Etats-Unis permet aux GAFAM de continuer d'accaparer les données personnelles des utilisateurs à des fins commerciales. Les Etats-Unis décident de laisser faire le Capitalisme de surveillance dès lors qu'il leurs rapporte économiquement et politiquement une position dominante sur le reste du monde qui dépend des plateformes américaines.

Quand l'Union européenne a décidé de légiférer et d'encadrer la collecte des données, les plateformes et GAFAM se sont dressés contre de telles mesures. Le lobbying au Parlement européen a été intense et l'est toujours. Le graphique ci-contre montre les dépenses des GAFAM en lobbying au Parlement européen.



¹¹⁴ Ibid.

Google et Microsoft arrivent en tête des entreprises dépensant le plus d'argent en lobbying au Parlement européen, devant Shell. Facebook serait troisième. Bayer ne dépenserait que la moitié des dépenses de Google en termes de lobbying au Parlement.



Certains auteurs comme Patrick Pharo s'étonnent que les données numériques ne soient pas traitées comme une partie du corps humain tel que le sang ou les gamètes. En effet, le Parlement européen a décidé que les données ne pouvaient être des « marchandises »¹¹⁵. Ainsi, les plateformes ne peuvent pas payer les utilisateurs pour leur acheter leurs données. Mais alors que sont les données ? Pourquoi ne les protège-t-on pas comme faisant partie de l'intégrité du corps humain dès lors qu'elles relèvent de l'intimité morale de l'individu (profil psychologique, préférences, peurs, information sur l'état de santé, orientation sexuelle, ...) ? Et pourquoi les plateformes peuvent-elles les monétiser si elles ne sont pas une marchandise ?¹¹⁶. La réponse de l'auteur est que l'on y consent par l'acceptation des CGU. Pourtant, même si une personne qui donne un organe -elle ne peut pas le vendre car ce n'est pas une marchandise- consent à ce que l'intermédiaire le revende,

¹¹⁵ Directive (UE) 2019/770 du Parlement européen et du Conseil relative à certains aspects concernant les contrats de fourniture de contenus numériques et de services numériques, 20 mai 2019, art. 24.

¹¹⁶ PHARO Patrick, « Chapitre 1. Big data et évolution sociale », *Les data contre la liberté*, Presses Universitaires de France, Paris cedex 14, coll. « Hors collection », 2022, p. 19-106.

jamais le contrat ne sera valide aux yeux de la loi. Pourquoi traiter les données autrement ? La réponse est simple, le capitalisme de surveillance s'effondrerait. Or, aujourd'hui, de trop nombreux acteurs dépendent des GAFAM et de leur pouvoir de prévision et d'influence.

Conclusion

Dans cette analyse du microciblage politique et des manipulations électorales numériques, nous avons plongé au cœur du capitalisme de surveillance et d'influence, ce système complexe où la collecte de données, le microciblage politique et l'influence s'entremêlent pour façonner nos démocraties et nos sociétés.

Dans une première partie, nous nous étions demandé comment l'affaire Cambridge Analytica était révélatrice à la fois des pratiques de collecte de données sur Internet, et à la fois des dérives du microciblage politique ?

À travers l'affaire Cambridge Analytica, nous avons pris conscience de l'ampleur des pratiques de collecte de données et de leur impact sur le processus électoral, bien au-delà du scandale lui-même. En effet, l'économie des plateformes et d'Internet en général repose sur le marché publicitaire, or ce dernier utilise le microciblage pour être toujours plus performant et rentable. Dès lors les plateformes cherchent à collecter toujours plus de données sur les utilisateurs afin d'améliorer sans cesse leurs outils de prédiction. Par ailleurs, le cas de Cambridge Analytica

et la diffusion de leaks sur les campagnes publicitaires de la firme, nous ont permis d'examiner les mécanismes des troubles informationnels et de leur amplification sur les réseaux sociaux pour mieux comprendre les risques qu'ils posent pour la Démocratie. La mis-information, la désinformation et la mal-information forment le trio des troubles informationnels. Ces techniques sont utilisées pour manipuler les électeurs, notamment dans le cadre d'une campagne de dénigrement d'un adversaire politique. Ces troubles ne permettent pas un choix éclairé des électeurs qui croulent sous un trop-plein informationnel. Ils peuvent être orchestrés par des usines à trolls automatisés qui font monter artificiellement le référencement de certains sujets, faisant croire à une forme de crédibilité de l'information et une amplification du phénomène par effet boule de neige.

Dans notre seconde partie, nous nous étions interrogés sur l'efficacité du microciblage et des manipulations électorales numériques.

Nous avons alors confronté les perspectives du courant déterministe et du courant cognitiviste, tout en explorant le rôle central du marketing politique et du microciblage dans la persuasion des électeurs. Nous en retenons que les électeurs sont de moins en moins déterminés par l'influence des structures, ils sont volatiles et sensibles aux campagnes électorales. Dans ce contexte, les candidats ont tout intérêt à viser ces électeurs à l'aide du microciblage et d'une communication personnalisée basée sur le marketing politique. Pourtant, les utilisateurs ne consentent pas de manière libre et éclairée à ce microciblage et à ces intrusions dans leur vie privée.

Enfin, dans une dernière partie, nous nous sommes plongés au cœur du capitalisme de surveillance et d'influence. Nous avons mis en lumière l'influence des GAFAM et leur rôle central dans la collecte et l'exploitation des données à des fins politiques et commerciales.

En conclusion, le microciblage politique favorise la mise en place d'un cercle vicieux renforçant le capitalisme de surveillance :

Le capitalisme de surveillance fonctionne grâce à la collecte massive de données personnelles. Ces données, analysées par les logiciels de délégation, alimentent des modèles prédictifs. Ces modèles permettent un microciblage ultraprécis, utilisé à des fins politiques pour influencer les électeurs et remporter des élections. C'est un outil particulièrement efficace en permettant aux candidats de diffuser des publicités personnalisées. Ce système profite avant tout aux cabinets de conseil qui développent et vendent ces outils de microciblage, se légitimant par leur efficacité électorale. Les acteurs politiques, quant à eux, sont peu enclins à réglementer la

collecte de données et les plateformes qui leur ont permis de gagner des élections et dont ils dépendent. Ces plateformes profitent de cette situation de dépendance. Elles continuent de collecter massivement des données, source de leur richesse et de leur influence.

Ainsi, le capitalisme de surveillance et le microciblage politique s'inscrivent dans un cercle vicieux où la collecte de données alimente le ciblage, lequel devient indispensable à de nombreux acteurs. Ces derniers, sous dépendance, participent à l'institutionnalisation de la collecte de données, et ce, au détriment de la vie privée des utilisateurs. Cette constatation nous permet d'affirmer que le microciblage politique est le cheval de Troie du capitalisme de surveillance, ceux y ayant recours ne pouvant plus en contester les risques et l'encourageant même.

Cette analyse a pour finalité de soulever des questions cruciales sur la protection de la vie privée, la transparence des processus électoraux et la régulation des plateformes numériques. Face à ces enjeux, il est impératif que les citoyens aient conscience de ce qui est fait de leurs données et les risques pour leur vie privée et la Démocratie.

Annexe :

1. **Brittany Kaiser**

Brittany Kaiser est une militante démocrate qui a travaillé bénévolement au profit de la campagne de Barack Obama en 2008. Elle oriente sa carrière vers la protection des droits de l'Homme et fait de nombreuses missions de bénévolat à l'étranger dans cet objectif. Sa famille connaissant des difficultés financières après la crise de 2008, elle accepte de travailler pour Alexander Nix -PDG de CA- en 2014 notamment dans l'optique de travailler sur des missions à caractères sociales. Cependant, elle finit par devenir une sorte de commerciale vendant les solutions de CA à travers le monde, à la fois à des gouvernements, des partis politiques et des entreprises. Elle passe 3 ans au service de CA. En 2018, elle ne perçoit pas la commission qu'elle espérait et se dispute avec A. Nix. A la même période, CA connaît des difficultés financières et politiques (début des révélations). Le jour où A. Nix comparait au Parlement, B. Kaiser est écartée. A. Nix lui écrit que « de toute évidence leur relation n'est plus viable professionnellement ». Par la suite, elle devient « lanceuse d'alerte » et écrit un ouvrage au sujet de l'affaire CA, qui ressemble plus à une tentative de justification de sa part qu'à un témoignage fidèle des événements. Son récit reconstruit ses trois ans à CA, tombant par moment dans l'illusion biographique.

En dehors de son livre, elle a surtout diffusé des centaines de documents sur CA (*leaks*) qui permettent de sortir de cette « dictature du témoignage ». La fuite de données sur Twitter est diffusée à partir du compte « Hindsight is 2020 ». Le choix du pseudo n'est pas anodin, puisque

cette expression signifie « revenir sur un événement passé avec un regard plus éclairé sur la situation ». Les liens des leaks étaient néanmoins endommagés. A l'aide du site Internet Archive et de son outils « wayback machine »¹¹⁷, nous avons pu télécharger les fichiers et les exploiter.

Au total, cela fait plus d'un millier de page de documents à étudier. Nous nous sommes donc concentrés sur les *leaks* concernant les Etats-Unis et plus précisément la communication de CA pour vendre ses services.

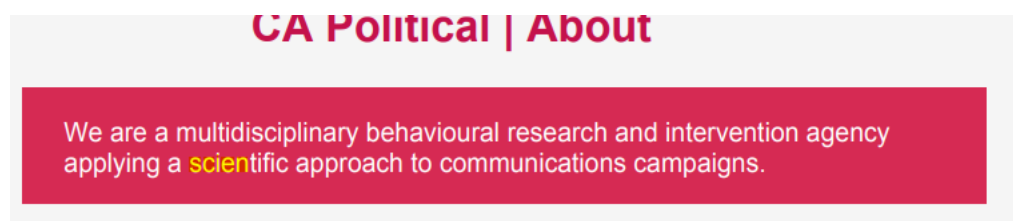
2. La communication de Cambridge Analytica

Déjà, l'accent est mis sur l'opposition entre la communication classique qui serait dépassée et le ciblage comportemental. La seconde option permettrait d'envoyer le « bon



message aux bonnes personnes au bon moment ». Ainsi, ils mettent en avant leurs capacité à identifier très précisément le public cible de leur client à l'aide de l'analyse de data et l'utilisation de modélisation psychologique (la segmentation psychographique). Ils peuvent ainsi « comprendre les personnalités complexes » et les influencer.

Ensuite, les membres de CA insiste sur la démarche



¹¹⁷ <https://web.archive.org/>

scientifique de leurs méthodes. Ce terme apparaît 68 fois dans les présentations de CA. En utilisant l'argument de la scientificité comme argument d'autorité, CA légitime ses méthodes par l'appui extérieur de la science. Cela serait la distinction avec ses concurrents.

3. Publicité sous forme d'article de presse

Notable Ad Formats: Native



Politico Native Ads

Sponsored content pieces saw 2-4% higher engagement than display or video; average engagement time of 4 minutes

<http://www.politico.com/sponsor-content/2016/08/inconvenient-truths-about-clinton-foundation>



Kaiser explique qu'une publicité a été mise en ligne sur le site *Politico* pour une liste d'électeurs indécis dans des Etats clés pour remporter l'élection. Cette publicité ressemblait à un article journalistique listant les « 10 vérités compromettantes au sujet de la Fondation Clinton » - accessible au lien suivant : <https://www.politico.com/sponsor-content/2016/08/inconvenient-truths-about-clinton-foundation>. L'objectif étant de décrédibiliser Clinton.

4. Publicité sous forme de sites internet référencés par Google

Des publicités google ont également été achetées pour faire remonter des résultats pro-Trump, ou surtout anti-Clinton.

Persuasion Search Advertising



Search Query: *Trump Iraq War*

Hillary Voted For The Iraq War - Donald Trump Opposed It
Ad www.donaldjtrump.com/Iraq
Crooked Hillary voted for the war in Iraq as a New York Senator. Bad Judgment!



Control The First Impression

Search Query: *Hillary Trade*

Hillary Clinton Supports NAFTA - She Will Ship Jobs Overseas
Ad www.lyingcrookedhillary.com
Hillary Clinton's Trade Deals Destroy American Jobs. No More Bad Deals.



Go Negative on Hillary's Positions and Expose Scandals

Search Query: *Trump Economic Plan*

Donald Trump For President - See His Full Economic Plan
Ad www.donaldjtrump.com/Economy
Donald Trump will fix America's rigged economy. See the full plan here.



Drive Traffic To Relevant Issue

5. Vidéo authentique mais sans contexte

Une vidéo de Michelle Obama a été massivement relayée dans laquelle elle déclarait « Si vous ne savez pas tenir votre maison, comment voulez-vous en faire autant avec la Maison Blanche ? ». Sortie de son contexte cette réplique semble être une attaque envers H. Clinton mais en réalité elle expliquait qu'elle et son mari continuaient de s'occuper de leurs enfants même en pleine campagne. Cette vidéo a permis de réduire les chances pour les femmes de centre-gauche de voter pour la candidate, leurs profils révélant un léger conservatisme notamment au regard de la famille et des valeurs traditionnelles, toujours selon Brittany Kaiser dans son livre « *l'affaire*

Four major television buys were placed over the course the DCH.

1. Cut, 10/9
2. Can't Run Her House (Michelle Obama Ad), 10/24-11/1
3. Race of a Lifetime (Drugs Ad), 10/24-11/1
4. Questions, 11/2-11/8

'Cut' ran for one night, during the second Presidential debate, in Ohio and Pennsylvania. The goal was to reach a maximum number of Principal Audience households, within our budget. 'Cut' bracketed the debate running either directly before, or directly after, depending on the exact station. The ad delivered 1.5M impressions in its' one night.

'Can't Run Her House' ran for two weeks in Florida. The buy was placed following an Ad Recall and Impact Survey conducted by CA. The survey indicated the ad moved women away from Clinton,

swinging Clinton's unfavorables by nearly 16 points among some demographics. Using this data, CA isolated persuadable women in FL based on the Principal Audience, then selected the networks - cable or broadcast - and carrier (Comcast, Charter, etc.) to best serve 'Can't Run Her House' to these audiences. The Communications team at both MAN1 and CA worked together to place multiple stories about the buy and the metrics behind it. MAN1 even drew a Cease and Desist from the Clinton campaign, a true sign of the effectiveness of this ad.

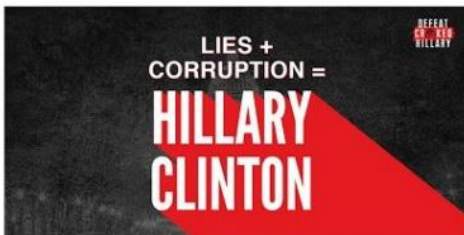
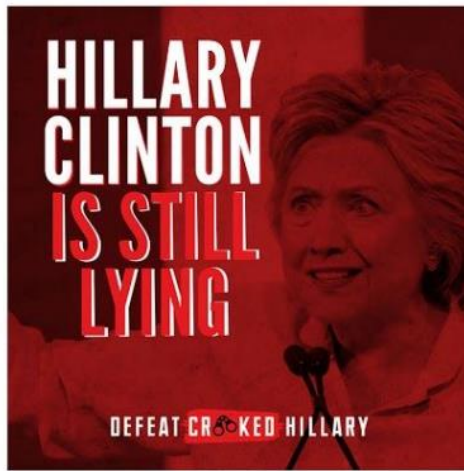
'Race of a Lifetime' ran for two weeks in Florida. The buy was placed in the Panhandle, in high density conservative areas. Similar to the above, CA used the Principal Audience to isolate regions where high Republican turnout is imperative to the outcome statewide. 'Race of a Lifetime' and 'Can't Run Her House' ran during the first week of Early Vote. Panhandle was delivered to nearly 1.6 million voters.

Facebook

Over the course of the campaign our ads were seen 81 million times, reaching 13.2 million voters, on average more than six times each. Of those 13.2 million voters, more than half took an action (click, like, comment, etc.) on our ads, higher than other successful campaigns. 9.84 million times users viewed more than 10 seconds of our videos. On average users watched 20.4 percent of our videos, more than five percentage points above similar campaigns. Overall, our ads drove 429,699 visits to defeatcrookedhillary.com.

Video	Impressions	Reach	Freq.	10s Views	10s View Rate	Link Clicks	CPC	CTR	Spend
Do Nothing	6,250,663	2,270,711	2.75	1,079,583	16.59%	31,968	\$4.15	0.51%	\$132,579.03
NAFTA	5,158,057	2,080,126	2.48	529,648	9.75%	28,932	\$3.43	0.56%	\$99,186.21
Can't Run Her House	2,310,081	1,229,935	1.88	237,663	8.04%	13,025	\$4.56	0.56%	\$59,418.32
Equal Pay	6,716,760	2,062,332	3.26	946,799	18.12%	11,171	\$12.21	0.17%	\$136,404.48
Benghazi	3,729,888	1,853,954	2.01	650,286	19.71%	25,480	\$2.54	0.68%	\$64,776.33
SCOTUS-Evangelicals	2,465,506	742,781	3.32	314,201	12.74%	9,689	\$7.26	0.39%	\$70,346.12
How To Lie	2,300,861	442,868	5.2	243,438	10.58%	-	\$7,778.37	-	\$54,448.56
FALN	2,353,011	454,780	5.17	263,642	11.20%	-	\$18,149.85	-	\$54,449.54
NAFTAv2	615,368	331,201	1.86	107,113	17.41%	2906	\$2.84	0.47%	\$8,250.00
SCOTUS	4,657,418	1,792,089	2.6	637,720	10.10%	18168	\$3.23	0.39%	\$58,745.02
Shut It Down	1,660,268	971,520	1.71	296,643	17.87%	10457	\$3.59	0.63%	\$37,499.83
The Cut	1,691,831	1,012,334	1.67	333,300	19.70%	11023	\$1.70	0.65%	\$18,747.15
Obama-The Game	3,062,342	908,024	3.37	400,038	13.06%	-	\$7,223.28	-	\$79,456.09
Bernie Never	1,492,966	1,153,878	1.29	338,421	21.18%	3914	\$5.22	0.26%	\$20,425.93

6. Campagne négative à l'encontre d'H. Clinton



7. Les pays où Cambridge Analytica est intervenu

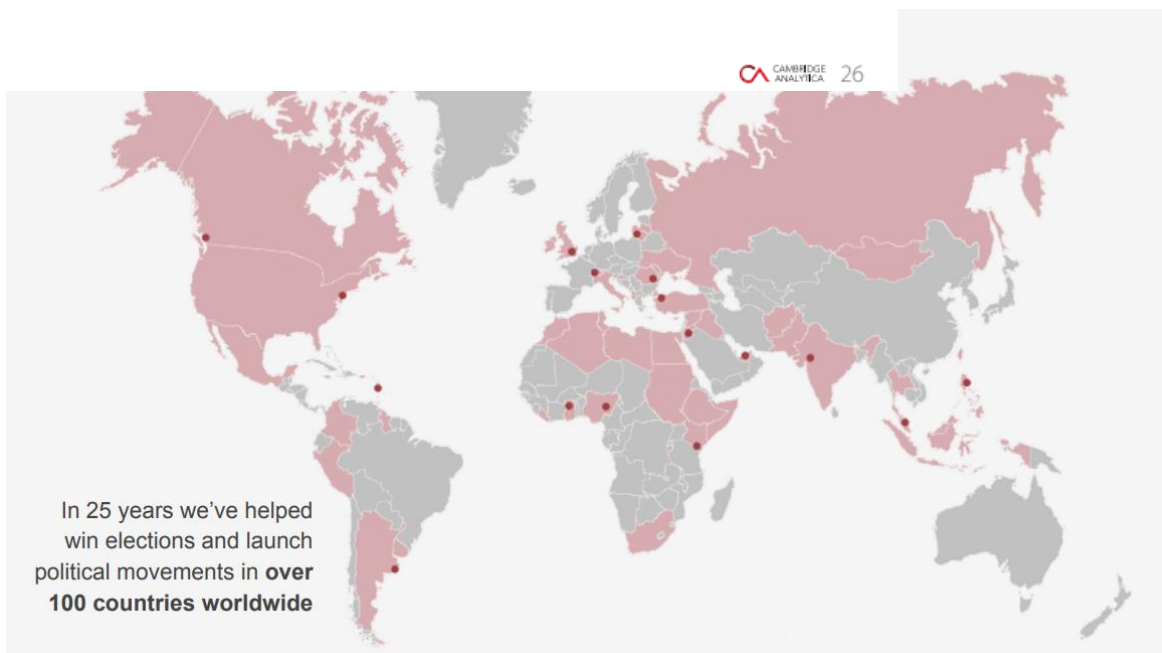


Des *leaks* sur le Brésil, la Malaisie, le Kenya, l'Iran, le Ghana, et les Etats-Unis sont accessibles mais il n'est pas possible de dresser la liste des 68 pays où CA aurait travaillé. Les documents font état d'une liste de 43 pays

« seulement ».

D'autres font état de plus d'une centaine de pays.

Albania	Grenada	Moldova	St. Lucia
Antigua	Guyana	Nepal	St. Vincent
Bahamas	India	Nigeria	Taiwan
Canada	Indonesia	Pakistan	Thailand
Cayman Islands	Italy	Peru	Trinidad & Tobago
Colombia	Iraq	Philippines	United Kingdom
Cyprus	Kenya	Poland	United States
D.R. Congo	Latvia	Romania	Ukraine
Ethiopia	Libya	Russia	Uruguay
Gabon	Lithuania	South Africa	Zambia
Ghana	Mauritius	St. Kitts & Nevis	



8. Harcèlement organisé par Cambridge Analytica à l'encontre d'H. Clinton

Une publicité mise en place par Cambridge Analytica sur Twitter propose de tweeter automatiquement en cliquant sur l'un des quatre choix un hashtag à l'encontre d'H. Clinton. Par exemple le quatrième est #SheCantTellTheTruth. Cela contribue à la vague de harcèlement et de haine subit par la candidate.



Donald J. Trump @realDonaldTrump · Sep 26
What is Hilary's Worst Lie? Vote Now!



Tweet #BathroomServer

Tweet #PayToPlay

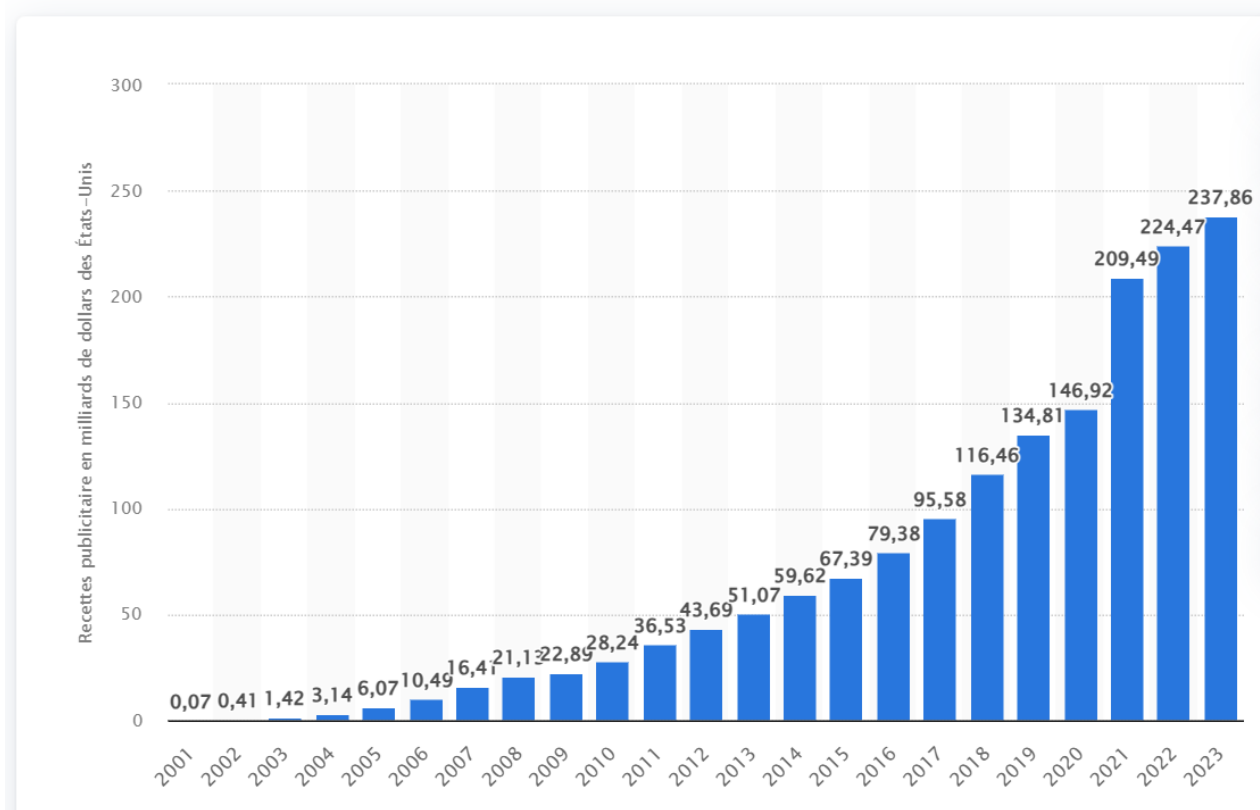
Tweet #Benghazi

Tweet #SheCantTellTheT...

9. Graphique 2 : Le chiffre d'affaires publicitaire de Google de 2001 à 2023

Chiffre d'affaires publicitaire Google de 2001 à 2023

(en milliards de dollars des États-Unis)

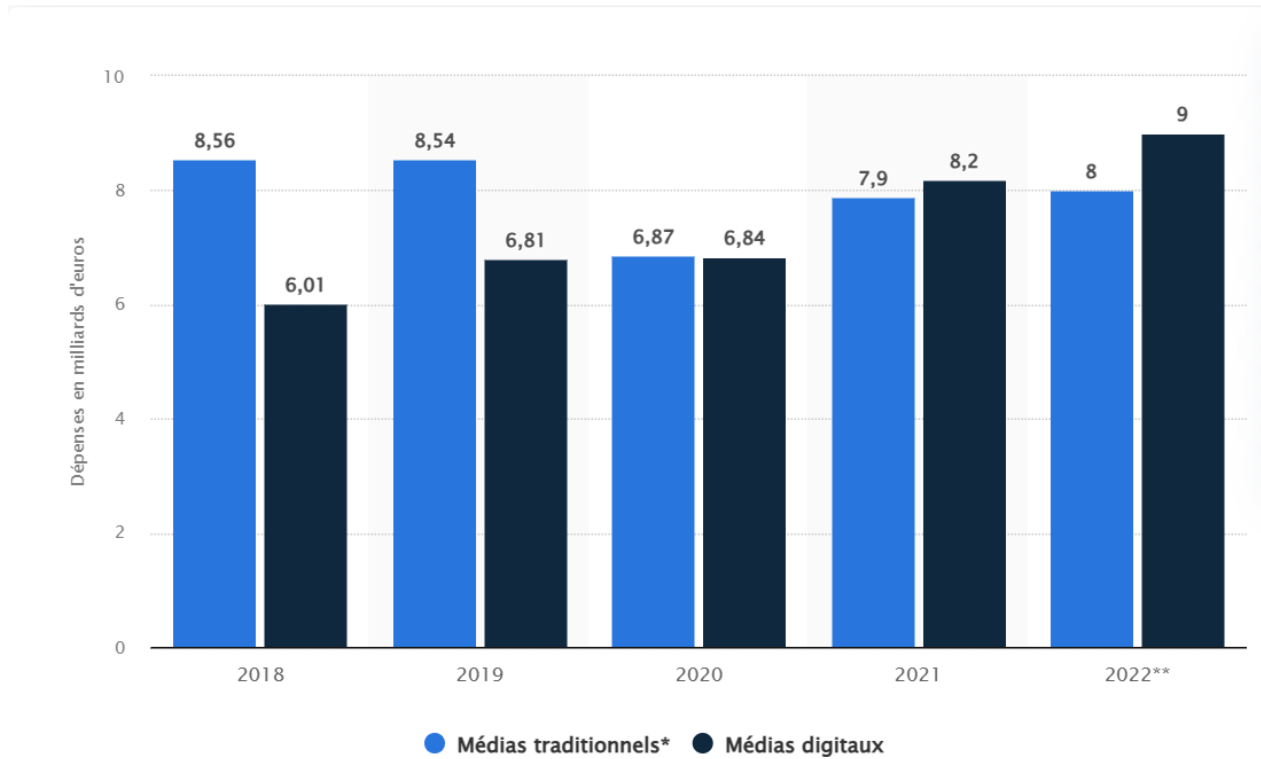


Chiffre d'affaires publicitaire annuel de Google 2001–2023

Publié par Statista Research Department, 29 févr. 2024

« Cette statistique représente le chiffre d'affaires publicitaire annuel de Google entre 2001 et 2023. En 2023, les revenus publicitaires de Google s'élevaient à 237,86 milliards de dollars américains. Cette année-là, la publicité a compté pour la majorité du chiffre d'affaires total de l'entreprise en ligne ».

10. Graphique 3 : Répartition des dépenses publicitaires par type de média en France de 2018 à 2022(en milliards d'euros), publié par Maxime Gautier, le 15 déc. 2023 sur Statista



« Ce graphique indique la répartition des dépenses publicitaires par type de média en France de 2018 à 2022 en milliards d'euros. Sur l'ensemble de la période la part des dépenses publicitaires dans la publicité digitale a connu une croissance constante pour même dépasser la part des médias traditionnels en 2021. En 2022 la publicité digitale a généré des recettes de plus de 8 milliards d'euros en France.

* La source indique que les médias traditionnels incluent la publicité extérieure, la télévision, la radio et le cinéma. »

11. Expérience à partir de mes données Instagram

Ce passage est rédigé à la première personne, ayant réalisé l'expérience à partir de mes propres données et ne prétendant pas à la généralisation de ces résultats.

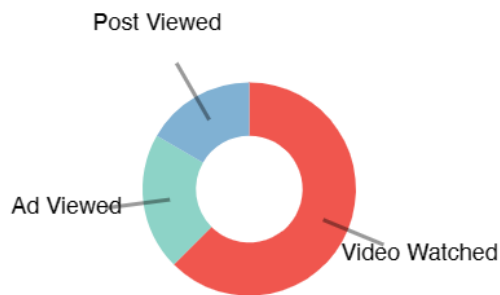
J'ai testé le programme de l'UFC Que Choisir dans le cadre de sa campagne « respecte mes datas »¹¹⁸. Cet outil permet d'en savoir plus sur nos données. Pour cela il est nécessaire de demander à la plateforme choisie (Instagram dans mon cas) de me transmettre mes données, en demandant leur téléchargement via les réglages de mon compte. Il m'a fallu cinq jours pour les obtenir.

Mes données étudiées sont celles du 22 avril au 29 avril sur Instagram. En notant, que j'ai très peu utilisé ce réseau social durant cette période.

Environ un quart des contenus que j'ai visionné été un contenu publicitaire. Et j'aurais cliqué sur un peu plus d'un quart d'entre eux (en sachant que j'essaye en général de ne pas cliquer sur les contenus publicitaires).

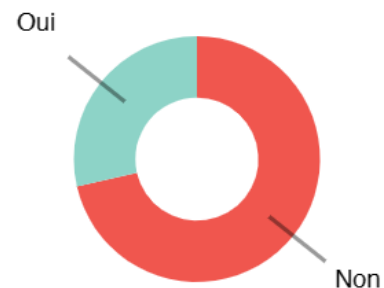
Type de contenu

Filtre actuel :



Annonce cliquer

Filtre actuel :



¹¹⁸ <https://experiences.respectemesdatas.fr/experience/instagram>

Enfin l'outil m'indique que 255 entreprises auraient utilisé mes données.

advertiserName ▼	hasDataFileCustomAudience ▼	hasRemarketingCustomAudience ▼	hasInPersonStoreVisit
Salto	Oui	Non	Non
Zenith Media Australia	Oui	Non	Non
ELECTRO DEPOT	Oui	Non	Non
BZB	Oui	Non	Non
Doriconsas	Oui	Non	Non

Lignes par page : 5 ▼ 1-5 de 255 < >

Un autre logiciel peut être utilisé en complément « Apply Magic Sauce »¹¹⁹ développé par des chercheurs de l'Université de Cambridge. Il permet à partir de données, de nous indiquer la perception que les publicitaires peuvent avoir de nous. Nos données sont partagées dans le cadre de la recherche scientifique de ces chercheurs, mais nous pouvons demander la suppression de nos données (ce que j'ai fait). L'outil analyse les données LinkedIn, Facebook et Twitter, trois réseaux sociaux que j'utilise très peu. Mes résultats me semblent donc faux mais sont basés sur 2 post Facebook, aucune données Twitter et très peu de LinkedIn (194 mots). Il serait intéressant de faire cette expérience avec un utilisateur qui utilise régulièrement ces réseaux sociaux.

Mes données révéleraient que je suis un homme de 28 ans, alors que je suis une femme de 23 ans. Ma personnalité serait INTP (voir ci-dessous le résumé), je pense que cela peut être correct car je me décrirais comme une personne plutôt réservée. Mais il serait nécessaire de lire les autres types de personnalité existants pour comparer.

Cet outil est très intéressant, mais il faudrait le tester plus longuement avec des données plus complètes pour avoir des résultats plus crédibles.

Néanmoins, il permet de voir ce que les publicitaires peuvent savoir de nous à partir des données qu'ils collectent, voir comment ils nous « profilent ».

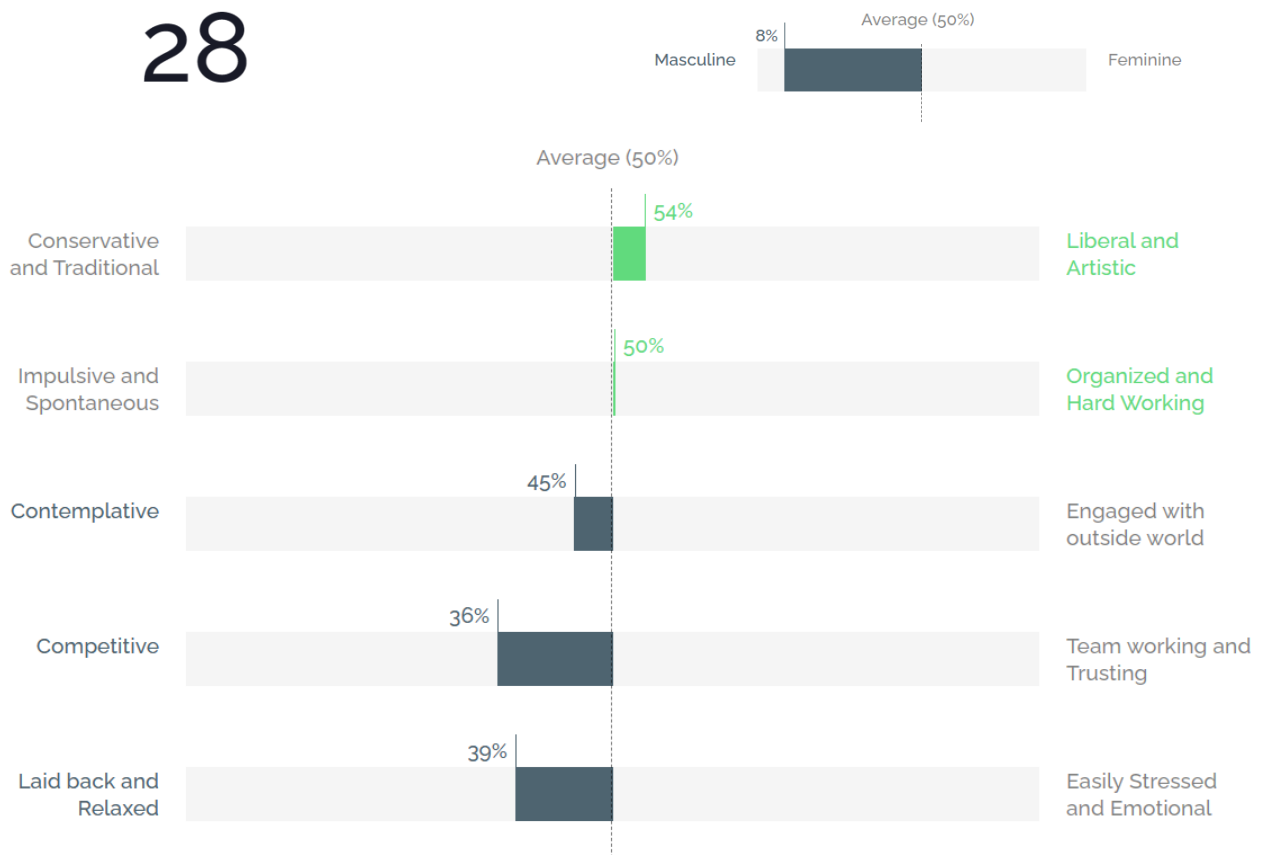
¹¹⁹ <https://applymagicsauce.com/about-us>

The following prediction is based on **2** Facebook posts and **194** words from LinkedIn text

Age

28

Psychological Gender



Openness to experience describes a dimension of personality that distinguishes imaginative, creative people from down-to-earth, conventional people.

Your digital footprint suggests that you are aware of your own feelings but don't get carried away with your imagination either. You might say that you embrace change when it is necessary while still resisting it when you think it is not, and that beauty is important to you, but it's not everything.

Conscientiousness concerns the way in which we control, regulate, and direct our impulses.

Your digital footprint suggests that you are random and fun to be around but can also plan and persist when life requires it. It appears that depending on the situation, you can make quick decisions or deliberate for longer if necessary.

Extraversion is marked by pronounced engagement with the external world, versus being comfortable with your own company.

Your digital footprint suggests that you enjoy and actively seek out social occasions, but would say that they're not everything. You might say that sometimes it is nice to step back for a while and have a quiet night in.

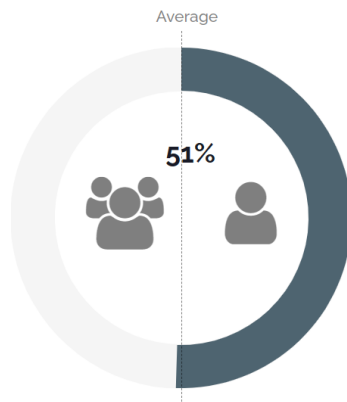
Agreeableness reflects individual differences in concern with cooperation and social harmony.

Your digital footprint suggests that you can find it difficult to get along with others when you first meet them. You might be suspicious of others' motives in this situation. It also looks like people warm to you over time, and you to them, although that doesn't stop you telling them "how it is".

Neuroticism refers to the tendency to experience negative emotions.

Your digital footprint suggests that you are calm and emotionally stable. You come across as someone who is rarely bothered by things, and when they do get you down the feeling does not persist for very long.

Leadership Potential



Jungian Personality Type

Introverted iNtuitive Thinking Perceiving

INTPs are quiet, thoughtful, analytical individuals who don't mind spending long periods of time on their own, working through problems and forming solutions. INTPs tend to be less at ease in social situations and the "caring professions" although they enjoy the company of those who share their interests. They also tend to be impatient with the bureaucracy, rigid hierarchies, and politics prevalent in many professions, preferring to work informally with others as equals.

INTPs' extraverted intuition often gives them a quick wit, especially with language, and they can defuse the tension in gatherings by comical observations and references. They can be charming, even in their quiet reserve, and are sometimes surprised by the high esteem in which their friends and colleagues hold them.

Bibliographie

Ouvrages et articles scientifiques :

AÏM Olivier, *Les théories de la surveillance. Du panoptique aux Surveillance Studies*, Paris, Armand Colin, coll. « Collection U », 2020.

AKPINAR Mustafa, « A REVIEW ON THE RELATIONSHIP OF BIG DATA AND CAMBRIDGE ANALYTICA », vol. 2, 2022, p. 56-63, [<https://doi.org/10.7456/100201100/006>].

AMIEUX Gabriel, « Nos données, leurs intérêts ? Coralie Lemke, Ma santé, mes données, Premier Parallèle, 2021, 182 p., 17€ », *Revue Projet*, n° 2, vol. 387, 2022, p. 93-94, [<https://doi.org/10.3917/pro.387.0093>].

ARTIGUELONG Maryse, « Numérique et société de contrôle », *Alternatives Non-Violentes*, n° 2, vol. 199, 2021, p. 16-18, [<https://doi.org/10.3917/anv.199.0016>].

AUMAITRE Aurélie et LETOQUEUX Hervé, « Apprivoiser les preuves numériques : la réception française de l'OSINT », *Délibérée*, n° 2, vol. 19, 2023, p. 49-55, [<https://doi.org/10.3917/delib.019.0049>].

BACHERT-PERETTI Audrey, « La protection constitutionnelle des données personnelles : les limites de l'office du Conseil constitutionnel face à la révolution numérique », *Revue française de droit constitutionnel*, n° 2, vol. 118, 2019, p. 261-284, [<https://doi.org/10.3917/rfdc.118.0261>].

BADOUARD Romain, « La régulation des contenus sur Internet à l'heure des "fake news" et des discours de haine », *Communications*, n° 1, vol. 106, 2020, p. 161-173, [<https://doi.org/10.3917/commu.106.0161>].

BALDWIN-Philippi, Jessica. "Data campaigning: between empirics and assumptions". Internet Policy Review 8.4 (2019). Web. 26 Apr. 2024.

BLONDIAUX L., *La Fabrique de l'Opinion : une Histoire Sociale des Sondages*, Paris, Seuil, 1998.

BONICHOT Jean-Claude, « Données personnelles : l'invention européenne d'un monde nouveau », *Pouvoirs*, n° 2, vol. 185, 2023, p. 97-109, [<https://doi.org/10.3917/pouv.185.0097>].

BOULAY S., 2015, *Usurpation de l'identité citoyenne dans l'espace public. Astroturfing, communication et démocratie*, Québec, Presses de l'université du Québec.

BOYADJIAN Julien et THEVIOT Anaïs, « Chapitre 12. La politique à l'heure des réseaux sociaux », *Nouvelle sociologie politique de la France*, Paris, Armand Colin, coll. « Collection U », 2021, p. 165-175, [<https://doi.org/10.3917/arco.frina.2021.01.0165>].

BOZDAG Engin, « Bias in algorithmic filtering and personalization », *Ethics and Information Technology*, , 2013, [<https://doi.org/10.1007/s10676-013-9321-6>].

BRANELLEC Gurvan et SOMMIER Béatrice, « De la règle du jeu aux jeux sur la règle : l'utilisation des données numériques personnelles dans la présidentielle française de 2017 », *Gestion et management public*, n° 2, 11 / 2, 2023, p. 69-99, [<https://doi.org/10.3917/gmp.112.0069>].

BRASSEUR Christophe, *Enjeux et usages du big data*, 2e éd., Paris, Lavoisier-Hermès, coll. « Information numérique », 2016.

BULLICH Vincent, « Plateforme, platformiser, platformisation : le péril des mots qui occultent ce qu'ils nomment », *Questions de communication*, n° 2, vol. 40, 2021, p. 47-70, [<https://doi.org/10.4000/questionsdecommunication.27413>].

BULLICH Vincent, « La délégation logicielle et la reconfiguration des pratiques rédactionnelles : le cas meltygroup », *Communication & management*, n° 2, vol. 17, 2020, p. 51-65, [<https://doi.org/10.3917/comma.172.0051>].

CARDON Dominique, *Culture numérique*, Paris, Presses de Sciences Po, coll. « Les petites humanités », 2019.

CLUZEL-METAYER Lucie, « Contrôler les contenus ? », *Pouvoirs*, n° 2, vol. 185, 2023, p. 111-122, [<https://doi.org/10.3917/pouv.185.0111>].

CNIL, *La forme des choix. Données personnelles, design et frictions désirables*, coll. « Dossier thématique dans les Cahiers IP ».

CYTERMANN Laurent, « Promesses et risques de l'open et du big data : les réponses du droit », *Informations sociales*, n° 5, vol. 191, 2015, p. 80-90, [<https://doi.org/10.3917/inso.191.0080>].

DELERUE François, « Chapitre 15. Les menaces numériques en période électorale », *Les guerres de l'information à l'ère numérique*, Paris cedex 14, Presses Universitaires de France, coll. « Hors collection », 2021, p. 347-363, [<https://doi.org/10.3917/puf.maran.2021.01.0347>].

DELFORGE Antoine, « Big data : une mine d'or, mais à quel prix pour notre vie privée ? », *La Revue Nouvelle*, n° 4, vol. 4, 2017, p. 40-49, [<https://doi.org/10.3917/rn.174.0040>].

DESRUMAUX Clément et LEFEBVRE Rémi, « Pour une sociologie des répertoires d'actions électorales », *Politix*, n° 1, vol. 113, 2016, p. 5-16, [<https://doi.org/10.3917/pox.113.0005>].

DORTIER Jean-François, « La publicité nous manipule-t-elle ? », *La Communication*, Auxerre, Éditions Sciences Humaines, coll. « Synthèse », 2016, p. 230-238, [<https://doi.org/10.3917/sh.dorti.2016.02.0230>].

DOSQUET Frédéric, « Chapitre 3. Comportement des électeurs et persuasion électorale », *Marketing et communication politique*, Caen, EMS Editions, coll. « Questions de société », 2017, p. 125-182, [<https://doi.org/10.3917/ems.dosqu.2017.01.0125>].

DOUBLET Yves-Marie, *Désinformation et campagnes électorales*, Strasbourg, Conseil de l'Europe, 2019.

DOUZET Frédérick, LIMONIER Kévin, MIHOUBI Selma et RENE Élodie, « Cartographier la propagation des contenus russes et chinois sur le Web africain francophone », *Hérodote*, n° 2-3, vol. 177-178, 2020, p. 77-99, [<https://doi.org/10.3917/her.177.0077>].

EUROPEAN PARLIAMENT. DIRECTORATE GENERAL FOR PARLIAMENTARY RESEARCH SERVICES., *Les principaux risques des médias sociaux pour la démocratie: risques liés à la surveillance, à la personnalisation, à la désinformation, à la modération et au microciblage.*, LU, Publications Office, 2021.

FARCHY Joëlle et TALLEC Steven, « De l'information aux industries culturelles, l'hypothèse chahutée de la bulle de filtre », *Questions de communication*, n° 1, vol. 43, 2023, p. 241-268.

FRANKLIN FOWLER Erika, RIDOUT Travis N. et FRANZ Michael M., « Political Advertising in 2016: The Presidential Election as Outlier? », *The Forum*, n° 4, vol. 14, 2016, [<https://doi.org/10.1515/for-2016-0040>].

FRAU-MEIGS Divina, « Chapitre 14. Les enjeux de la réception : comment mesurer l'influence de la désinformation ? », *Les guerres de l'information à l'ère numérique*, Paris cedex 14, Presses Universitaires de France, coll. « Hors collection », 2021, p. 323-345, [<https://doi.org/10.3917/puf.maran.2021.01.0323>].

HAAG Phillipe, *La communication numérique électorale : nouvelle étape de la marchandisation du politique ?*. Sciences de l'information et de la communication. Université Bourgogne Franche-Comté, 2022.

HARCOURT Bernard E. et RENAUT Sophie, *La société d'exposition: désir et désobéissance à l'ère numérique*, Paris, Éditions du Seuil, coll. « La couleur des idées », 2020.

HEINDERYCKX François, « Obama 2008 : l'inflexion numérique », *Hermès, La Revue*, n° 1, vol. 59, 2011, p. 135-136, [<https://doi.org/10.3917/herm.059.0135>].

HIMMELWEIT, H. T., HUMPHREYS, P., JAEGER, M., & KATZ, M. (1981). How voters decide: A longitudinal study of political attitudes and voting extending over fifteen years. *European Monographs in Social Psychology*, 27, 276.

HOUDE Olivier, « Chapitre IV. L'intelligence artificielle », , Paris cedex 14, Presses Universitaires de France, coll. « Que sais-je ? », 2023, p. 404-425.

HUNEMAN Philippe, *Les sociétés du profilage: évaluer, optimiser et prédire*, Paris, Payot, 2023.

ISAAC Henri, « Pour en finir avec l'acronyme GAFAM », *Pouvoirs*, n° 2, vol. 185, 2023, p. 7-17, [<https://doi.org/10.3917/pouv.185.0007>].

ISSENBERG Sasha, *The victory lab: the secret science of winning campaigns*, 1. ed., New York, Crown Publ, 2012.

JAMMET Thomas, « Portrait de l'internaute en cible marchande : La construction algorithmique d'une rhétorique publicitaire innovante », in Anaïs THEVIOT (dir.), *Gouverner par les données ? Pour une sociologie politique du numérique*, Lyon, ENS Éditions, coll. « Gouvernement en question(s) », 2023, p. 95-112, [<https://doi.org/10.4000/books.enseditions.44888>].

LE COZ Armel, « Amis ou ennemis de la démocratie ? », *Après-demain*, n° 2, N ° 66, NF, 2023, p. 19-21, [<https://doi.org/10.3917/apdem.066.0019>].

LIMONIER Kévin, « Des cyberespaces souverains ? Le cas de la Russie », *La Cyberdéfense*, Paris, Armand Colin, coll. « Collection U », 2023, p. 167-173, [<https://doi.org/10.3917/arco.taill.2023.01.0167>].

LOVELUCK Benjamin, « Internet, une société contre l'État ? Libéralisme informationnel et économies politiques de l'auto-organisation en régime numérique », *Réseaux*, n° 4, vol. 192, 2015, p. 235-270, [<https://doi.org/10.3917/res.192.0235>].

MANOKHA Ivan, « Le scandale Cambridge Analytica contextualisé: le capital de plateforme, la surveillance et les données comme nouvelle « marchandise fictive » », *Cultures & Conflits*, n° 109, 2018, p. 39-59, [<https://doi.org/10.4000/conflits.19779>].

MASSIT-FOLLEA Françoise, « De l'utopie internet aux défis d'un monde numérisé. Information et connaissance, liberté individuelle et vivre ensemble », *Ramses 2018*, Paris, Institut français des relations internationales, coll. « Ramses », 2017, p. 144-149.

MAYER N. (1997), « Introduction », In Boy D., Mayer N., *L'électeur a ses raisons*, Presses de Sciences Po.

MELKA Lionel, *Big Data et plateformes. La nouvelle économie des données*, Louvain-la-Neuve, De Boeck Supérieur, coll. « Business School », 2022.

MHALLA Asma, « Les Big Tech, de nouveaux États parallèles ? », *Pouvoirs*, n° 2, vol. 185, 2023, p. 69-81, [<https://doi.org/10.3917/pouv.185.0069>].

MOAWI Hazim, *Predicting voting behaviors and election results using digital trace data and Twitter.*, 2023, [<https://doi.org/10.13140/RG.2.2.23867.28965>].

MONDOUX André, MENARD Marc, GRONDIN-ROBILLARD Laurence et BONNEAU Jonathan, « Automatisation des messages et publicités à caractère politique dans les médias socionumériques : Le cas de Facebook », in Anaïs THEVIOT (dir.), *Gouverner par les données ? Pour une sociologie politique du numérique*, Lyon, ENS Éditions, coll. « Gouvernement en question(s) », 2023, p. 113-127, [<https://doi.org/10.4000/books.enseditions.44898>].

NEIHOUSER Marie, BOYADJIAN Julien et THEVIOT Anaïs, « “Campagnes électorales et numérique : regards croisés à l’international” – Avant-propos », *Revue internationale de politique comparée*, n° 2-3, vol. 29, 2022, p. 7-29, [<https://doi.org/10.3917/ripc.292.0007>].

NELSON Richard Alan, *A Chronology and Glossary of Propaganda in the United States*, Greenwood Press, 1996.

NIMMO Ben, « Chapitre 3. Les techniques d’amplification sur les réseaux sociaux », *Les guerres de l’information à l’ère numérique*, Paris cedex 14, Presses Universitaires de France, coll. « Hors collection », 2021, p. 87-103, [<https://doi.org/10.3917/puf.maran.2021.01.0087>].

PANDEY Supragya, KATIYAR Devesh et GOEL Gaurav, « Predicting Elections with Big Data », *International Journal for Research in Applied Science and Engineering Technology*, vol. 10, 2022, p. 1155-1158, [<https://doi.org/10.22214/ijraset.2022.46379>].

PARISER Eli, *The filter bubble: what the Internet is hiding from you*, London, Viking, 2011.

PECH Yannick, « Le hacking comme opération spéciale permanente des guerres de l’information », *Revue internationale d’intelligence économique*, n° 1, vol. 13, 2021, p. 93-118.

PEREZ LAGOS Camila, « Rendre visibles les conséquences de la surveillance numérique. Le cas du « scandale » Cambridge Analytica », *Communication*, vol. 37, 2020, [<https://doi.org/10.4000/communication.13252>].

PEREZ LAGOS Camila, « Anaïs Theviot, Big Data électoral. Dis-moi qui tu es, je te dirai pour qui voter. Lormont, Éd. Le Bord de l’eau, coll. Territoires du politique, 2019, 200 pages », *Questions de communication*, n° 1, vol. 37, 2020, p. 464-466, [<https://doi.org/10.4000/questionsdecommunication.23102>].

PERROT Sandrine, POMMEROLLE Marie-Emmanuelle et WILLIS Justin, « La fabrique du vote : placer la matérialité au cœur de l’analyse », *Politique africaine*, n° 4, vol. 144, 2016, p. 5-26, [<https://doi.org/10.3917/polaf.144.0005>].

PHARO Patrick, *Les data contre la liberté*, Paris, PUF, 2022.

POLANYI K., *The Great Transformation: The Political and Economic Origins of Our Time*, New York, Farrar & Rinehart, 1944.

POMMEROLLE Marie-Emmanuelle et JOSSE-DURAND Chloé, « Le roi est nu : crise électorale et anatomie du pouvoir au Kenya (2017) », *Politique africaine*, n° 4, vol. 148, 2017, p. 169-181, [https://doi.org/10.3917/polaf.148.0169].

QUATTROCIOCCHI Walter, SCALA Antonio, SUNSTEIN Cass, « Echo chambers on Facebook », Cambridge (MA), Harvard Law School, Discussion Paper n° 877. PDF téléchargeable à l'adresse suivante : http://www.law.harvard.edu/programs/olin_center/papers/pdf/Sunstein_877.pdf

QUESSARD Maud, « Enfants chéris et enfants terribles des États-Unis », *Pouvoirs*, n° 2, vol. 185, 2023, p. 31-38, [https://doi.org/10.3917/pouv.185.0031].

ROCHELANDET FABRICE, ÉCONOMIE DES DONNEES PERSONNELLES ET DE LA VIE PRIVEE. LA DECOUVERTE, « REPERES », 2010 : [HTTPS://WWW-CAIRN-INFO.EZPAARSE.UNIV-PARIS1.FR/ECONOMIE-DES-DONNEES-PERSONNELLES-ET-DE-LA-VIE-PRI--978270715765](https://www-cairn-info.ezpaarse.univ-paris1.fr/ECONOMIE-DES-DONNEES-PERSONNELLES-ET-DE-LA-VIE-PRI--978270715765)

ROCHER Fanny, « L'influence des réseaux sociaux en période électorale: le cas de WhatsApp durant la campagne présidentielle au Brésil de 2018 ».

RONAI Maurice, « Les campagnes présidentielles à l'heure du big data », *L'Économie politique*, n° 2, vol. 94, 2022, p. 60-71.

SALMONA Laure, « Des lendemains qui déchantent : de la promesse d'un espace horizontal à un espace qui creuse les inégalités », *Politiser les cyberviolence*, Paris, Le Cavalier Bleu, coll. « Convergences », 2023, p. 19-32.

SERGE BACHIMONT Bruno & BOUCHARDON, « Revue Intelligibilité du numérique », *Revue Intelligibilité du numérique*, , 2020.

SIRE Guillaume, « Cinq questions auxquelles Google n'aura jamais fini de répondre », *Hermès, La Revue*, n° 3, vol. 73, 2015, p. 201-208, [https://doi.org/10.3917/herm.073.0201].

SMYRNAIOS Nikos, « Les GAFAM, entre emprise structurelle et crise d'hégémonie », *Pouvoirs*, n° 2, vol. 185, 2023, p. 19-30, [https://doi.org/10.3917/pouv.185.0019].

SOUPIZET Jean-François, « Alexandre Olivier, La Tech. Quand la Silicon Valley refait le monde, Paris : Seuil, mars 2023, 560 p. », *Futuribles*, n° 4, vol. 455, 2023, p. 120-122, [https://doi.org/10.3917/futur.455.0111d].

SOUPIZET Jean-François, « Les États face aux géants du Net. Vers une alliance de raison ? », *Futuribles*, n° 3, vol. 454, 2023, p. 5-23, [https://doi.org/10.3917/futur.454.0005].

STENGER Thomas et COUTANT Alexandre, « Introduction », *Hermès, La Revue*, n° 1, vol. 59, 2011, p. 9-17, [<https://doi.org/10.3917/herm.059.0009>].

TAPPIN, BEN M et al. “Quantifying the potential persuasive returns to political microtargeting.” *Proceedings of the National Academy of Sciences of the United States of America* vol. 120,25 (2023)

TAGHAVI, BABAK. « SPEL, *Les sens du vote. Une enquête sociologique (France 2011-2014)*, Rennes, Presses universitaires de Rennes, coll. « Res publica », 2016, 229 p. », *Politix*, vol. 119, no. 3, 2017, pp. 175-179.

THEVIOT Anaïs, « Usages électoraux des big data. Un modèle américain ? », *Revue internationale de politique comparée*, n° 2-3, vol. 29, 2022, p. 157-190, [<https://doi.org/10.3917/ripc.292.0157>].

THEVIOT Anaïs et TREILLE Éric, « Mobiliser par les données. Les stratégies numériques de campagne des candidats à la primaire de la droite et du centre de 2016 », *Politiques de communication*, n° 1, vol. 12, 2019, p. 71-96, [<https://doi.org/10.3917/pdc.012.0071>].

THIBOUT Charles, « Les GAFAM et l'État : réflexion sur la place des grandes entreprises technologiques dans le champ du pouvoir », *Revue internationale et stratégique*, n° 1, vol. 125, 2022, p. 75-88, [<https://doi.org/10.3917/ris.125.0075>].

TISSERANT Virginie, *Comment l'usage de vos données peut influencer les élections*, [<http://theconversation.com/comment-lusage-de-vos-donnees-peut-influencer-les-elections-140001>].

TOLEDANO Joëlle, « La Commission européenne, la norme et sa puissance », *Pouvoirs*, n° 2, vol. 185, 2023, p. 83-95, [<https://doi.org/10.3917/pouv.185.0083>].

VALLUY JEROME, *HUMANITE ET NUMERIQUE(S) – DE L'HISTOIRE DE L'INFORMATIQUE EN EXPANSION SOCIETALE... AU CAPITALISME DE SURVEILLANCE ET D'INFLUENCE (1890-2023)*, TERRA-HN-EDITIONS, COLLECTION HNP, 2023, 255 p. : [HTTP://WWW.RESEAU-TERRA.EU/ARTICLE1347.HTML](http://www.reseau-terra.eu/article1347.html)

VALLUY Jérôme, *Sur L'âge du capitalisme de surveillance (2019) de Shoshana Zuboff et sa difficile réception* | *Cahiers Costech*, [<https://www.costech.utc.fr/CahiersCostech/spip.php?article153>].

VEDEL Thierry, « Chapitre 5 - L'internet et la démocratie : une liaison difficile », *La démocratie de l'entre-soi*, Paris, Presses de Sciences Po, coll. « Académique », 2017, p. 73-88, [<https://doi.org/10.3917/scpo.perri.2017.01.0073>].

WARDLE Claire, DERA KHSHAN Hossein, with research support from Anne Burns and Nic Dias, *Information Disorder Toward an interdisciplinary framework for research and policymaking*, September 2017

ZUBOFF Shoshana, *L'âge du capitalisme de surveillance: le combat pour un avenir humain face aux nouvelles frontières du pouvoir*, trad. Bee Formentelli et trad. Anne-Sylvie Homassel, Paris, Éditions Zulma, coll. « Z a », 2022.

ZUBOFF Shoshana, « Un capitalisme de surveillance », *Études*, trad. Sean Rose, n° 2, Février, 2021, p. 57-66, [<https://doi.org/10.3917/etu.4279.0057>].

Les informateurs :

Kaiser Brittany, *L'affaire Cambridge Analytica, Les dessous d'un scandale planétaire*, Harpercollins., 2020.

Wylie Christopher, *Mindfuck: le complot Cambridge analytica pour s'emparer de nos cerveaux*, trad. Aurélien Blanchard, Paris, Bernard Grasset, 2020.

Articles journalistiques :

Affaire « Team Jorge » : il est temps de s'attaquer sérieusement aux menaces numériques à la démocratie, [<https://www.radiofrance.fr/franceinter/podcasts/geopolitique/geopolitique-du-jeudi-16-fevrier-2023-7148974>].

Le lobbying de Facebook en Europe dévoilé par des mémos internes, [<https://www.france24.com/fr/20190304-europe-lobby-facebook-rgpd-sheryl-sandberg-memo>].

Boyen Pascale, Courrier International, 3 mai 2018 :
<https://www.courrierinternational.com/article/cambridge-analytica-une-vraie-fausse-faillite>

Cadwalladr Carole, Emma Graham Harrison, The Guardian, 17 mars 2018 :
<https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>

Chen Adrian, The New York Times, "The Agency", 2 juin 2015 :
<https://www.nytimes.com/2015/06/07/magazine/the-agency.html>

Davies Harry, « Ted Cruz campaign using firm that harvested data on millions of unwitting Facebook users », The Guardian, 11 décembre 2015 : <https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data>

Doward Jamie, Cadwalladr Carole, Watchdog to launch inquiry into misuse of data in politics, The Guardian, 4 mars 2017 : <https://www.theguardian.com/technology/2017/mar/04/cambridge-analytics-data-brexite-trump>

Mayer Jane, The New Yorker, “The secret sharer”, 23 mai 2011 : <https://www.newyorker.com/magazine/2011/05/23/the-secret-sharer>

Krever Mick, Chernova Anna, CNN, *Wagner chief admits to founding Russian troll farm sanctioned for meddling in US elections*, 14 février 2023 : <https://edition.cnn.com/2023/02/14/europe/russia-yevgeny-prigozhin-internet-research-agency-intl/index.html>

Meko Tim, Lu Denise, Gamio Lazaro, Washington post, *How Trump won the presidency with razor-thin margins in swing states*, nov 2016 : <https://www.washingtonpost.com/graphics/politics/2016-election/swing-state-margins/>

Reich Robert, « Obama’s Transition Economic Advisory Board : The Full List », US News & World Report, November 7, 2008. - <https://www.nytimes.com/2008/11/08/us/politics/08advisors.html>

Szadkowski Michaël, « « Infox » au Brésil : comment les fausses informations ont inondé WhatsApp », *Le Monde.fr*, 25/10/2018. : https://www.lemonde.fr/pixels/article/2018/10/25/infox-au-bresil-comment-les-fausses-informations-ont-inonde-whatsapp_5374637_4408996.html

Vogel Kenneth, « Cruz partners with donor's 'psychographic' firm », Politico, 7 juillet 2015 : <https://www.politico.com/story/2015/07/ted-cruz-donor-for-data-119813>

Sitographie :

Isabel Kusche, The conversation, 7 mai 2019 : <https://theconversation.com/pourquoi-le-micro-ciblage-politique-pourrait-saper-la-democratie-116319>

Terrogeance, « Biometric Database Enhancement », en ligne sur <https://www.terrogeance.com/capabilities/biometric-database-enhancement/>>

Monde. Le fil « Pour toi » de TikTok risque de pousser des enfants et des jeunes vers du contenu dangereux en lien avec la santé mentale, [<https://www.amnesty.org/fr/latest/news/2023/11/tiktok-risks-pushing-children-towards-harmful-content/>].

Choice, « How Long Does It Take to Read Amazon Kindle’s Terms and Conditions? », YouTube, 17 mars 2017 : <https://www.youtube.com/watch?v=sxygkyskucA>

<https://fr.statista.com/statistiques/1368090/publicite-digitale-part-revenus-entreprises/>

<https://campaignforaccountability.org/>

<https://fr.ejo.ch/deontologie-qualite/cinquante-nuances-desinformation-fakenews-trouble-information-claire-wardle-manipulation>

<https://www.la-croix.com/Monde/Scandale-Cambridge-Analytica-68-pays-victimes-propagande-electorale-2020-01-08-1201070529>

<https://www.techtransparencyproject.org/articles/civis-analytics>

<https://www.techtransparencyproject.org/articles/googles-revolving-door-us>

Ressources juridiques :

Convention européenne des droits de l'homme Telle qu'amendée par les protocoles n° 11 et 14, complétée par le protocole additionnel et les protocoles n° 4, 6, 7, 12 et 13 :
https://www.cncdh.fr/sites/default/files/2022-02/cedh_0_1.pdf

RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) : <https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679>

RÈGLEMENT (UE) 2022/2065 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques) : <https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32022R2065>

INTRODUCTION	9
I. LES DONNEES AUX FONDEMENTS DU MICROCIBLAGE ET DES MANIPULATIONS ELECTORALES ...	21
A. L’AFFAIRE CAMBRIDGE ANALYTICA REVELATRICE DES PRATIQUES DE COLLECTE DES DONNEES NUMERIQUES	23
1. <i>De la genèse de Cambridge Analytica au scandale</i>	23
a) La genèse de Cambridge Analytica : l’influence de Google et des Républicains.....	23
b) Les révélations des pratiques de Cambridge Analytica	26
2. <i>Au-delà de Cambridge Analytica</i>	29
a) Les pratiques similaires des plateformes.....	29
b) L’usage des cookies à travers le web.....	31
B. LES MECANISMES AU SERVICE DES MANIPULATIONS ELECTORALES NUMERIQUES.....	33
1. <i>Typologie des troubles informationnels</i>	34
a) Définition.....	34
b) Typologie	36
2. <i>Les mécanismes de propagation et d’amplification des troubles informationnels</i>	39
a) Les usines à trolls et les bots.....	40
b) Les algorithmes : chambres d’écho et bulles de filtre	41
II. L’EFFICACITE DES MANIPULATIONS ELECTORALES NUMERIQUES QUESTIONNEE	45
A. LE DEBAT REITERATIF DE L’EFFICACITE DE LA PROPAGANDE ELECTORALE.....	47
1. <i>Le choix des électeurs entre poids des structures sociales et poids de la campagne</i>	47
a) Courant déterministe : le poids des structures sociales sur le vote	48
b) Le courant cognitiviste : le poids de la campagne sur le vote	49
2. <i>Le marketing politique</i>	50
a) Interrelation entre publicité et propagande.....	50
b) L’électeur comme consommateur politique	53
B. LE MICROCIBLAGE POLITIQUE COMME FACTEUR D’EFFICACITE DES MANIPULATIONS NUMERIQUES	55
1. <i>Les techniques et implications du microciblage politique pour la vie privée</i>	55
a) Analyse du microciblage politique.....	55
b) Les implications du consentement non-éclairé de l’utilisateur au microciblage	57
2. <i>Les effets du microciblage sur les médias sociaux</i>	59
a) Les critiques quant à l’efficacité du microciblage	59
b) Les preuves indirectes de l’efficacité du microciblage	61
III. LES GRANDS GAGNANTS DU MICROCIBLAGE COMME CHEVAL DE TROIE : LES GAFAM ET LE CAPITALISME DE SURVEILLANCE ET D’INFLUENCE	65
A. LE MICROCIBLAGE POLITIQUE OU LE CHEVAL DE TROIE DU CAPITALISME DE SURVEILLANCE ET D’INFLUENCE	67
1. <i>Le surplus comportemental au cœur du capitalisme de surveillance</i>	67

a)	Le surplus-comportemental comme source principale de revenu-des GAFAM	68
b)	Le fonctionnement du marché publicitaire	70
2.	<i>La convergence entre champ politique et champ commercial</i>	71
a)	Les interconnexions entre les acteurs des GAFAM et les acteurs politiques.....	72
b)	Le marché électoral comme porte d'entrée au marché commercial	74
B.	LES GAFAM : DES ACTEURS INCONTOURNABLES DEVENUS INDISPENSABLES	77
1.	<i>La dépendance des acteurs politiques aux données</i>	77
a)	La standardisation des campagnes électorales en ligne	77
b)	La collecte de données multiples par les différents data brokers	79
2.	<i>L'institutionnalisation du capitalisme de surveillance</i>	81
a)	Une politique du laisser faire	82
b)	L'influence des GAFAM sur la création et l'évolution du cadre juridique relatif aux données	84
CONCLUSION		91
ANNEXE :		95
1.	<i>Brittany Kaiser</i>	95
2.	<i>La communication de Cambridge Analytica</i>	96
3.	<i>Publicité sous forme d'article de presse</i>	97
4.	<i>Publicité sous forme de sites internet référencés par Google</i>	98
5.	<i>Vidéo authentique mais sans contexte</i>	98
6.	<i>Campagne négative à l'encontre d'H. Clinton</i>	101
7.	<i>Les pays où Cambridge Analytica est intervenu</i>	102
8.	<i>Harcèlement organisé par Cambridge Analytica à l'encontre d'H. Clinton</i>	103
9.	<i>Graphique 2 : Le chiffre d'affaires publicitaire de Google de 2001 à 2023</i>	104
10.	<i>Graphique 3 : Répartition des dépenses publicitaires par type de média en France de 2018 à 2022(en milliards d'euros), publié par Maxime Gautier, le 15 déc. 2023 sur Statista</i>	105
11.	<i>Expérience à partir de mes données Instagram</i>	106
BIBLIOGRAPHIE		111