INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES LYON

Projet Personnel en Humanités

Votre vie privée dans le monde d'aujourd'hui

ZOUGGARI *Yassine*

Supervisé par :
François Lesueur

Jury :
François Lesueur
Romaric Pujol

25 janvier 2019

Table des matières

Introduction

A l'ère du numérique, notre droit à la vie privée est de plus en plus difficile à protéger. Le monde est de plus en plus connecté, nous fournissons de plus en plus de données contre des services, et nos informations privées sont souvent stockées loin de notre contrôle.

Beaucoup sont sensibles à cela, et sentent que leurs informations leur échappent. A travers leurs propres activités, sur les réseaux sociaux, ou à travers leur téléphone, smart TV, assistant connecté. Mais aussi à travers leurs amis, pas toujours conscients des informations qu'ils partagent, des droits qu'ils octroient à des applications tierces, qui peuvent utiliser leurs données comme elles l'entendent.

Du progrès, pourtant, il y en a, notamment sur le point légal : le RGPD, Règlement Général à la Protection des Données, est la première initiative d'envergure à l'échelle européenne pour s'attaquer au problème. Toutefois, sans un vrai changement des mentalités, les progrès seront difficiles. Or beaucoup sont ceux qui considèrent n'avoir « rien à cacher », et qui ne prêtent aucune attention à l'utilisation de leur données.

Le présent document essaye de faire l'état des lieux de la situation aujourd'hui, et d'extrapoler sur l'évolution à laquelle nous pouvons nous attendre. Son but premier est de convaincre un lecteur sceptique de l'importance qu'il faut accorder à la protection de sa vie privée, et de fournir de premiers éléments de réponse pour se protéger.

Pour ce faire, nous commencerons par mieux cadrer le sujet. Parce que votre vie privée, qu'est ce que c'est exactement, pour vous ? Une première question qui mérite réflexion et dont la réponse n'est pas évidente, car très influencée par votre culture, vos opinions. Une fois les termes bien fixés, nous parlerons ensuite des dangers de la perte de cette vie privée, tels qu'abordés dans la littérature scientifique.

Mais une chose est claire, c'est bien de la vie privée de vos informations dont il est principalement question ici. Notre prochain objectif sera de fixer exactement les acteurs qui s'y intéressent aujourd'hui, qu'ils soient étatiques ou privés, et comment.

Enfin, nous analyserons la situation dans un pays comme la Chine, état de surveillance depuis longtemps, et plus récemment en plein dans le numérique. Les travers de cette surveillance nous pousserons ensuite à s'interroger sur la trajectoire sur lesquels notre société et le monde sont. Nous terminerons par quelques possibilités d'évolution de la situation, tels que décrites dans la fiction.

Bonne lecture !

Comment définir vie privée ?

Pour essayer de définir le terme de vie privée, commençons par chercher dans le dictionnaire. Le Larousse définit « privé » comme quelque chose concernant « quelqu'un dans sa personne même », « dans sa vie personnelle », mais le définit également par opposition à « public » (« ne concerne pas le public », « se fait sans témoins », « en dehors d'un cadre officiel »)[25].

C'est en gros la définition que nous appliquons au jour le jour : quand quelque chose est privé, il nous concerne directement (exclusivement, ou pas) et on ne souhaite pas qu'il soit accessible à quiconque sans notre consentement.

La dualité public/privé dans la définition ci-dessus nous rapproche de celles des courants philosophiques et sociologiques. Ainsi, des théories s'intéressent à la « sphère privée », la considèrent comme une grande catégorie que l'on ne distingue pas plus, et qui s'oppose à la « sphère publique ». Les travaux de recherche sur le sujet s'intéressent particulièrement à la frontière entre vie privée et publique, aux changements sociétaux qui la modifient [40].

Une barrière bien difficile à placer, en effet. Où s'arrête la vie privée d'un individu, où commence-t-elle ? Des questions comme l'orientation sexuelle par exemple, restent encore aujourd'hui en France un sujet considéré par beaucoup comme une affaire publique, à l'image de la virulence des débats dont on se rappelle au vote de la loi 2013-404 du 17 mai 2013, dite du « mariage pour tous ». Une loi qui aujourd'hui encore est discutée, 5 ans après sa signature, Libération indiquant que « le même paradigme conservateur hostile au pacs et au mariage pour tous réapparaît sur la scène publique » [7]. Des discussions similaires ont lieu dans d'autres pays concernant la religion, par exemple, mais aujourd'hui ces concepts sont en général vus comme privés. Une apparente modification de la barrière entre sphère privée et publique, donc, mais qui en fonction des sujets peut être assez floue, ou pas encore suffisamment ancrée dans la société.

En sociologie, les orientations principales se concentrent sur la vie privée en elle-même, plus particulièrement son lien avec la famille, et les évolutions de celle-ci, la famille étant considérée comme le pilier traditionnel de la vie privée d'un individu. La vie en famille, a survécu dans ses composantes principales de l'antiquité à nos jours, et la notion de vie privée est souvent fortement attachée à celle-ci : ce qui concerne votre cercle familial exclusivement est au centre de votre vie privée [40].

Un critique de la notion de vie privée comme vue aujourd'hui et à travers les âges est, peut-être assez étonnamment à première vue, le mouvement de pensée féministe. Celui-ci réfléchit au caractère ambivalent de la chose : il s'intéresse ainsi au bannissement au domaine de la vie privée de certaines personnes ou de certaines discussions et thèmes, et le condamne comme une différenciation régressive, un système social injuste et un concept duquel il faut s'émanciper [44]. Un point de vue intéressant, invitant à réfléchir à la place de la femme dans la société, longtemps vue comme « ménagère » et vivant intégralement dans la sphère privée, tandis que l'homme est supposé habiter la sphère publique [44].

En somme, la vie privée reste un concept très influencé par l'environnement : en fonction des moeurs, certaines choses sont considérées comme privées, d'autres ne le sont pas. Et comme notre société évolue, la barrière privé / public est également en perpétuelle adaptation.

Il n'est pas ici question d'essayer de dresser cette barrière. Toutefois, une distinction très importante est à réaliser : la vie privée telle que discutée ci-dessus, et celle particulièrement mise à mal dans le monde numérique d'aujourd'hui. Cette vie privée là, c'est votre vie privée informationnelle : le fait que vous étiez en visite à Paris le week-end dernier, ou que vous préférez faire l'amour le matin [10].

Les théories résumées ci-dessus précèdent le temps de l'information. Aujourd'hui, c'est un nouveau discours qui se développe, concerné particulièrement par vos données, leur privauté, et les effets néfastes possibles si elles sont exploitées par n'importe qui, sans régulation. Beaucoup redoutent l'évolution de notre société vers une société panoptique, concept que nous verrons plus en détail par la suite. Mais une chose est sûre : les théories sur la vie privée informationnelle sont traitées parallèlement et indépendamment aux autres théories énoncées ici, et bien sûr, toutes ces théories convergent sur beaucoup de points

[40].

Vie privée selon la loi

Définition légale

Au niveau légal, là encore, la définition est intentionnellement large, pour éviter que seuls les cas précisés par la loi ne soient couverts. D'après le Dictionnaire du Droit Privé, « La vie privée [...] fait partie des droits civils. Les composantes de la vie privée n'ont pas fait l'objet d'une définition ou d'une énumération limitative afin d'éviter de limiter la protection aux seules prévisions légales. Les tribunaux ont appliqué le principe de cette protection, au droit à la vie sentimentale et à la vie familiale, au secret relatif à la santé, au secret de la résidence et du domicile, et au droit à l'image » [8].

Quand on s'intéresse à la protection de la vie privée informationnelle plus précisément, l'Europe est longtemps restée une grande absente du débat, sans lois claires, et donc une grande victime selon Olivier Iteanu. En effet, les sociétés américaines de la Silicon Valley, à savoir beaucoup des grands géants de l'informatique, sont tous soumis au droit californien et ont essentiellement pour doctrine la « liberté », à rapprocher à la liberté des marchés, et en somme à une dé-régularisation. [23].

Le Règlement Général sur la Protection des Données (RGPD)

Depuis mai 2018, toutefois, le RGPD (Réglement Général sur la Protection des Données, ou GDPR en anglais) est actif au sein de l'Union Européenne (voté en avril 2016, après de longues négociations). Présentée comme « la loi de vie privée et de sécurité la plus dure au monde », elle impose des obligations aux entreprises du monde entier si celles-ci traquent ou collectent des informations sur un résident européen [38].

Ces obligations sont globalement d'ordre technique : il faut que le design d'un produit soit construit autour de la protection de la vie privée de l'utilisateur, et par vie privée on entend toutes les informations dont le service dispose sur cet utilisateur. Le service se doit ainsi de récupérer seulement les données dont il a besoin, de ne pas les garder plus longtemps que nécessaire, de protéger leur intégrité et confidentialité (notamment en les chiffrant), par exemple [38].

Si un service traite vos données, il doit être capable de justifier pourquoi, avoir des procédures en place pour la protection de ces données, et toujours vous donner accès à vos droits (d'information, de rectification, de suppression notamment). Dans le cas de données recueillies qui ne sont pas cruciales au fonctionnement du service (ou dans d'autres cas précisés), l'autorisation de l'utilisateur est indispensable.

Le « bundling » est de plus explicitement interdit, à savoir obliger l'utilisateur à donner son accord contre l'accès au service, d'après l'article 7[4] du règlement [38]. Il doit avoir le droit de refuser la collecte d'informations.

De plus, si ce service détecte une vulnérabilité ayant exposé des informations privées, il se doit de le déclarer aux autorités sous 72 heures, pour éviter que ces failles ne soient négligées, comme c'était arrivé à Yahoo notamment : « [...] Yahoo, en 2014 : une enquête interne sur une brèche de sécurité avait été laissée de côté, avant de finalement découvrir en 2016 que celle-ci avait permis à des cybercriminels de mettre la main sur les données personnelles de 500 millions dutilisateurs » [2].

Sur Internet et depuis que le règlement est en vigueur, vous avez peut-être remarqué que les sites web (en tout cas, ceux conformes) vous demandent maintenant si vous acceptez d'être traqué, et vous avez le droit de définir quelles informations sont collectées : oui aux cookies pour le fonctionnement du site, non à ceux pour le tracking, par exemple.

Et pour obliger les entreprises à fléchir, un pouvoir sans précédent est conféré aux autorités de protection de données de chaque pays. Les entreprises se doivent d'être capables de démontrer qu'ils sont conformes RGPD. Si elles n'y arrivent pas ou que l'autorité en question peut prouver que le règlement a été enfreint (suite à un audit typiquement), elles s'exposent à des amendes faramineuses : jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires mondial annuel de l'entreprise, le montant le plus gros étant celui appliqué [38].

Ce pouvoir réside avec la CNIL (Comission Nationale de l'Informatique et des Libertés) en France, et (au hasard) la Data Protection Commission en Irlande. Au hasard, pas vraiment en fait : législation fiscale avantageuse oblige, beaucoup de multinationales s'implémentent à Dublin, et sont donc sous l'autorité de cette agence. Quelques noms pour vous donner une idée : il y a Facebook, Google, Apple, Microsoft, Twitter, Amazon, IBM... si une action devait être entreprise contre les gros du secteur de l'information, donc, cette agence sera forcément mêlée. Il s'agit du système de « guichet unique » prévu par le règlement,

une organisation européenne doit avoir pour seule interlocutrice l'agence du pays où elle est implantée, si celle-ci est compétente en la matière (sinon, d'autres peuvent s'en charger).

Il est bien sûr possible à vous et moi de saisir directement les autorités compétentes. C'est ce qu'a fait NOYB (« None Of Your Business », ou « C'est pas tes oignons » en français) , une structure à but non lucratif, quelques heures à peine après le 25 mai 2018 à minuit, conjointement avec la Quadrature du Net, association de défense des droits et libertés sur Internet. Ce sont Facebook, Google (Android), Instagram et WhatsApp qui sont attaqués, la CNIL, la DPA (Belgique), la DPA (Autriche) et la HmbBfDI (Allemagne) ont été saisies [32]. C'est l'accord « forcé » de l'utilisateur qu'obtiennent ces compagnies qui est avancé comme raison principale. Au total, ce sont 7 milliards d'euros (3,7 milliards pour Google, 3,9 milliards pour Facebook) en éventuels frais. Une action qui aura au moins le mérite de nous montrer à quel point le règlement sera réellement appliqué.

Et, alors que je peaufine la fin de ce document, le procès en question vient de porter ses fruits (en partie) : la CNIL impose à Google une amende de 50 millions d'euros, pour « manque de transparence, information insatisfaisante et absence de consentement valable pour la personnalisation de la publicité » [11]. En cause, principalement, le fameux « bundling » expliqué plus haut (il faut accepter en bloc les politiques de Google pour pouvoir créer un compte), et le pré-cochage de l'option pour afficher des publicités ciblées, cachée derrière un « Plus d'options » lors de la création du compte [11].

D'autres amendes ont déjà été prononcées, notamment pour Optical Center en France à hauteur de 250 000, deux semaines après la mise en application de la RGPD. Une amende qui aurait pu s'élever à 20 millions d'euros si les fuites avaient eu lieu après la mise en application effective de la RGPD [16].

Les failles logicielles qui affectent les produits de ces entreprises mettent en danger les informations privées qu'ils stockent, récemment par exemple avec Facebook et une fuite d'informations pour 50 millions d'utilisateurs, dont 5 millions européens [45]. En théorie, cela pourrait également donner lieu à une action contre eux. Toutefois, notamment parce qu'il faudrait que l'agence prouve qu'ils ont été négligents, certains n'y croient pas encore [2].

Le Privacy Shield

D'après Iteanu, tout cela n'est pas encore parfait. Une nouvelle loi qu'il pointe du doigt notamment, votée quelques semaines après le RGPD : l'accord UE - Etats-Unis nommé Privacy Shield. Son objectif, mieux cadrer la transition vers le RGPD pour les entreprises américaines. Une possibilité, d'après Iteanu, pour celles-ci de « s'affranchir du RGPD et de ses contraintes » [23]. En effet, le Privacy Shield n'est en lui-même pas conforme au RGPD, mais ses règles s'en rapprochent. Les entreprises américaines peuvent l'utiliser comme « outil » pour s'adapter, mais doivent malgré tout appliquer le RGPD. Toutefois, si une entreprise choisit de s'auto-déclarer conforme au Privacy Shield, les règles de celui-ci s'imposent légalement [27]. Cela ne la protège pas pour autant du risque d'amende conformément au RGPD, en théorie [39].

Le Data Protection Working Party, organe consultatif indépendant européen, a publié un rapport sur la question. Les conclusions tirées sont que le Pricay Shield améliore en effet certains points par rapport à Safe Harbor, l'accord précédent négocié entre l'UE et les Etats-Unis en 2000, qu'il vient remplacer. Ces points sont en particulier une clause de révision annuelle, laissant une porte pour l'amélioration du dispositif, ou encore la déclassification des décisions de la cour de surveillance FISA (le Foreign Intelligence Surveillance Act américain) [34].

Mais ces quelques points positifs sont contre-carrés par beaucoup d'autres, moins reluisants. Le Working Party déplore notamment « un nombre important de problèmes non résolus », appelle à un « renforcement de la surveillance de la conformité des entreprises avec les principes du Privacy Shield » pour le côté commercial. Côté surveillance pour des raisons de sécurité nationale, sur laquelle nous reviendrons plus en détail dans le chapitre suivant, il appelle à « plus de preuves » sur l'utilisation de données collectés, et des mesures « contraignantes juridiquement » [34].

En conclusion, la législation autour de la question est bien compliquée, comme souvent au niveau européen, et le fonctionnement exact reste aujourd'hui encore assez obscur. Ce premier chapitre nous permet d'être bien au point sur ce que l'on entend par « vie privée » et les protections mises en place. Toutefois, pour vraiment protéger sa vie privée, un utilisateur d'aujourd'hui doit bien comprendre sa valeur : nous nous efforçons ci-après de détailler cette importance de vos informations, et pourquoi leur collecte le touche personnellement.

La valeur à accorder à votre vie privée

Pour ceux qui revendiquent n'avoir rien à cacher

« Si l'on a rien à cacher, pas besoin de se préoccuper de sa vie privée ».

Cet argument revient très souvent : il est utilisé par ceux ne se préoccupant pas particulièrement de la protection de leur vie privée, en ligne ou ailleurs, et par ceux souhaitant que l'on puisse scruter les données de tout le monde, pour débusquer plus facilement les « méchants ».

Et à première vue, il est facile de le considérer comme fondé. Si je ne mène aucune activité illicite, pourquoi devrais-je essayer de cacher mes communications ? Pourquoi ne pas laisser le gouvernement savoir quelles pages web je visite ?

Comme nous le verrons, plusieurs raisons laissent toutefois penser que le droit à la vie privée reste très important.

On sait par exemple que le simple fait d'être surveillé, et de le savoir, change le comportement que l'on aurait eu autrement. Glenn Greenwald, l'un des journalistes ayant publié les révélations d'Edward Snowden, cite de nombreux exemples [20] : en plus d'études psychologiques montrant un changement de comportement quand on se sait observé, il parle notamment du panoptique : il s'agit d'un type d'architecture carcéral plongeant les détenus dans un état de surveillance constante. Pour ce faire, une tour centrale est construite et voit dans toutes les cellules : un même gardien peut surveiller tout le monde. Mais surtout, les prisonniers ne savent pas quand ils sont observés.

Résultat, les détenus se sentent observés en permanence, et même plus besoin d'avoir un gardien dans la tour centrale. Dans « Surveiller et punir », Michel Foucault avance que les idées derrière le panoptique s'appliquent plus largement aux écoles, usines, lieux de travail, et y voit un « diagramme de la société disciplinaire ». Dans ce livre, le philosophe traite du système carcéral en particulier, et analyse le changement qu'il a subi. On passe d'un « supplice » public, instrument du pouvoir pour s'imposer par la force. Il détaille par exemple le cas de Robert-François Damiens, le dernier homme à avoir subi l'écartèlement en France (tentative d'assassinat sur Louis XV en 1757), ou encore les supplices en eux-même et leur symbolique (on perce la langue des blasphémateurs...) [15].

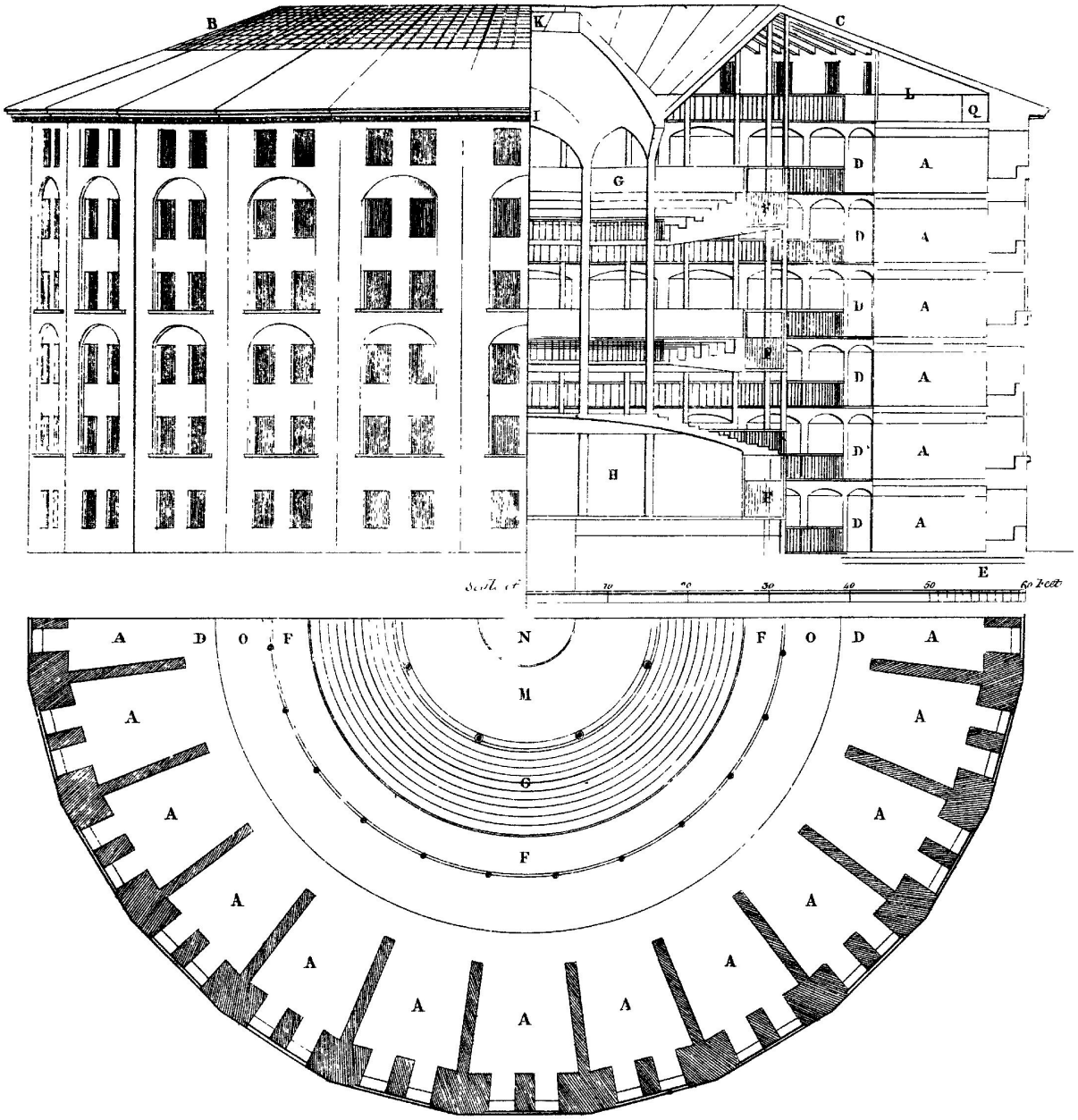
Avec le nouveau système carcéral, la dynamique est différente : « Le châtiment est passé dun art des sensations insupportables à une économie des droits suspendus ». Le pouvoir n'essaye plus de montrer sa force, mais au contraire de faciliter le contrôle du plus grand nombre par une élite, à l'image du panoptique. Foucault développe le rôle de la police, le quadrillage des populations et sa surveillance dans le contexte de la peste [15].

Cette théorisation du système carcéral par Foucault donnera lieu quelques années plus tard à un courant de pensée désigné sous le nom de « société de contrôle », qui voit son fondement le plus extensif en 2000, avec la publication de l'essai Empire. Cette nouvelle organisation de la société contrôle les citoyens « non plus par enfermement, mais par contrôle continu et communication instantanée » et où « les mécanismes de maîtrise se font [...] toujours plus immanents au champ social, diffusés dans le cerveau et le corps de citoyens » [30].

L'essai théorise le passage de notre société à ce qu'il appelle un « phénomène moderne d'impérialisme » : l'ennemi d'une nation n'est plus un autre pays comme c'est le cas classiquement. L'Empire dont l'essai tire son nom considère l'« ennemi » comme « une sorte de criminel », qui est un danger « non plus pour le système politique ou national mais pour la loi ». Cet ennemi est non seulement « banalisé (réduit à une répression policière routinière) », mais également « absolutisé (l'Ennemi est une menace absolue à l'ordre éthique) » [30].

Déjà à l'époque, le changement des outils d'un régime pour contrôler la population est noté : « Les

FIGURE 1 – Schéma d'une prison panoptique. Jeremy Bentham The works of Jeremy Bentham vol. IV, 172-3 (domaine public)



vieilles sociétés de souveraineté maniaient des machines simples, leviers, poulies, horloges ; mais les sociétés disciplinaires récentes avaient pour équipement des machines énergétiques ». Ainsi, « les sociétés de contrôle opèrent par machines de troisième espèce, machines informatiques et ordinateurs » [30].

Une autre thèse avancée est que le simple fait de se savoir surveillé change notre comportement durablement. Et, dans une démocratie où le citoyen doit être informé sur la politique intérieure et extérieure de son pays, pour pouvoir prendre ses décisions et voter en connaissance de cause, un tel effet est indésirable.

De nouveaux éléments sont venus étayer cette thèse, notamment une étude empirique menée par Jonathon Penney, candidat PhD. à Oxford. L'une des premières preuves concrètes de l'effet de la surveillance sur la population, elle montre une baisse de 20% de consultation d'articles Wikipédia relatifs au terrorisme avant et après juin 2013, date à laquelle Snowden divulgue ses informations. L'étude montre de plus que ces révélations ont eu des effets immédiats, mais également sur le long-terme [35].

Nous nous sommes concentrés ci-dessus à l'importance de notre vie privée dans le cadre d'une surveillance gouvernementale, mais une toute autre facette du problème concerne plus largement la société d'aujourd'hui. Spécifiquement, ce que l'on partage aujourd'hui de notre plein gré, avec des sociétés à but lucratif (Google, Facebook, ...) mais aussi avec nos amis via ces services.

Ainsi, J-M Manach s'est même demandé si la vie privée n'est pas un problème de « vieux cons ». Il compare l'absence de pudeur des natifs du numérique, qui partagent allègrement leurs faits et gestes sur Internet, à la libération sexuelle des années 60-70. Pour certains, il s'agit là d'un changement de société profond qu'il faut non seulement constater, mais pousser plus loin ; il s'agirait de l'utiliser pour changer nos conceptions dépassées de ce qui est privé et de ce qui ne l'est pas [28].

Mark Zuckerberg, le fondateur et CEO de Facebook, dresse un constat similaire : pour lui, la vie privée n'est plus une « norme sociale ». « Tout le monde est devenu très enclin à partager plus d'informations [...], plus ouvertement et avec plus de monde. Cette norme sociale a simplement évoluée » [24].

Dans son article (devenu livre par la suite), Manach conclut toutefois que le droit à la vie privée est « la première des libertés », sans laquelle « la liberté dopinion (de pensée plus dexpression), la liberté de circulation, et de réunion, les libertés politiques, syndicales et de culte, ne peuvent être exercées » [28].

Au delà des conséquences de la surveillance de tous les citoyens, exposées ci-dessus, il convient aussi de réfléchir à ce que l'on entend par « méchants », ceux que la surveillance se dit cibler en particulier. Quand on pense à quelque chose de répréhensible, les exemples qui nous viennent à l'esprit sont les actes de terreur, les meurtres et autres crimes graves. Il est naturel de vouloir se défendre contre de telles actions, et si la surveillance permet de s'en protéger, on est enclin à vouloir l'appliquer.

Toutefois, les « mauvaises » actions, aux yeux du gouvernement et des agences qui opèrent cette surveillance, englobent beaucoup plus que les actes criminels cités plus haut. Alors, qui sont exactement les gens qui se revendiquent avoir quelque chose à cacher, et qui souhaitent que leur vie privée soit protégée ?

Pour ceux ayant des choses légitimes à cacher

La surveillance globale montre que défendre sa vie privée, si on y tient, est important. C'est doublement vrai si l'on a des choses à cacher, même si on le fait légitimement.

Un exemple de profession à risque : les journalistes. Un exemple américain : Laura Poitras, journaliste et réalisatrice de CitizenFour, Oscar du meilleur documentaire 2016 dépictant Snowden et ses révélations [37]. Son travail avec le dissident lui a permis de nous en apprendre long sur la surveillance mondiale américain, sur laquelle nous reviendrons plus en détail au prochain chapitre. En théorie, une investigation sur le gouvernement américain ne devrait pas la placer dans une position dangereuse, et un journaliste n'a pas de compte à rendre à l'état. Pour que la presse puisse rester le contre-pouvoir qu'elle se doit d'être, il est évident que le droit à la vie privée des journalistes est primordial.

Dans une interview avec Bill Maher, toutefois, elle explique s'être retrouvée sur le radar des autorités américaines bien avant CitizenFour pour d'autres documentaires comme « My Country, My Country » (2006), traitant de la guerre en Irak : « après ce film j'ai été mise sous surveillance, je me faisais arrêter à chaque fois que je revenais aux Etats-Unis après un vol international, plus de 40 fois sur plusieurs années. Les agents de la douane attendaient directement à la sortie de l'avion, pour effectuer le contrôle des passeports, et ils m'emmenaient pour m'interroger sur ce que j'ai fait ».

Pour les journalistes comme Poitras, cette surveillance peut les empêcher d'effectuer leur travail correctement. Mais en Europe et aux Etats-Unis, les conséquences restent toutefois mesurées. Dans un pays comme la Chine, la manque de vie privée des habitants peut très vite se transformer en véritable enfer pour les journalistes.

Liu Hu est un vrai journaliste d'investigation dans ce pays qui en a cruellement besoin. Il a exposé plusieurs officiels chinois dans des affaires de corruption, résolu des enquêtes criminelles laissées sur le côté par les autorités, dont une affaire de meurtre. Si son travail est acclamé à l'international, le pouvoir en place ne le voit pas d'un très bon oeil. Hiu a accusé un haut placé d'extorsion en 2015, et a perdu le procès pour diffamation qui s'en est suivi : il a dû payer une première amende, de laquelle il s'est acquitté, mais a refusé d'en payer une deuxième qui lui était imposée. Résultat : il est effectivement assigné à résidence à partir de 2017, sous le nouveau système de crédit social chinois (que nous détaillons en dernière partie) [1].

En plus de l'empêcher de se déplacer en dehors de sa ville, ses comptes Weibo ont tous été bloqués (une plateforme de microblogging très populaire en Chine). Son compte principal avant son arrestation comptait près de 2 millions d'abonnés. Il a beau en recréer de nouveaux, ils sont tous supprimés par les autorités dès leur découverte. « Le gouvernement me voit comme un ennemi. Les média mainstream sont une machine de propagande pour le parti. Leur fonction principale est d'endoctriner les gens et les empêcher de connaître les faits » [1].

Liu Hu n'en est de plus pas à ses premiers problèmes avec les autorités. En 2013, il est détenu sans procès pour avoir lié des hauts placés du parti communiste à la prostitution illégale. Il est interrogé plus de 70 fois en un an, menacé, avant d'être finalement relâché. Depuis cette date, il y a 5 ans, il dit que le paysage médiatique du pays a beaucoup changé. « Beaucoup de journalistes ont quitté l'industrie, surtout ceux faisant du travail d'investigation. Mais j'aime toujours mon travail » [1]. Un travail qu'il ne peut pas exercer sans être inquiété.

Durant un « Ask Me Anything » sur Reddit (questions posées par les internautes), Edward Snowden résume excellemment bien la question concernant la protection de la vie privée, surtout dans le cas de la presse : « Argumenter que vous ne vous préoccupez pas de votre droit à la vie privée parce que vous n'avez rien à cacher est équivalent à dire que vous ne vous préoccupez pas de votre liberté d'expression parce que vous n'avez rien à dire. Une presse libre est bénéfique à bien plus de monde que simplement ceux qui écrivent les articles » [42].

Un documentaire sur la question de la valeur de la vie privée est disponible librement sur Internet, sous licence Creative Commons : « Nothing To Hide » [29]. Il aborde le problème de la surveillance tant du point de vue du citoyen lambda que de celles d'activistes du monde entier. Le fil directeur du film est une expérience menée sur « Mister X » (Max Thommes), un comédien berlinois, qui accepte de donner accès à son cellulaire, à ses comptes de réseaux sociaux pour se rendre compte de toutes les informations que l'on peut en tirer.

Un exemple français y est présenté, le cas de Joel Domenjoud, un militant écologiste, notamment assigné à résidence durant la COP21 et constamment surveillé par les autorités. Pour lui et sa famille, cela a été une prise de conscience « violente » des dangers de la surveillance, de ce qu'elle peut entraîner. « La plupart des gens se pensent à l'abri de ça. Mais il suffit que la police se trompe de porte, lors d'une perquisition administrative sous état d'urgence, qu'un voisin ou collège dise [...] "lui, il est louche" [...], et on peut très vite tomber dans cette case de personne surveillée » [29].

Une phrase de Joel Domenjoud conclut très bien ces deux premières parties, autant pour un citoyen lambda que pour un journaliste, activiste, ou personne ayant des choses légitimes à cacher : « Avoir le sentiment qu'on est à l'abri de [la surveillance] parce qu'on a rien à se reprocher, c'est là ou s'articule [sa force] : elle isole [...] le bon individu du mauvais individu » [29].

Pour ceux ayant des choses illégales à cacher

Nous avons donc traité du cas des citoyens normaux et de ceux qui cachent des choses légitimement. Mais qu'en est-il des criminels, des pédophiles, des terroristes ? Comment lutter contre les abus de ceux-là ?

Car c'est bien l'un des points phares de la rhétorique pro-surveillance : « si vous n'avez rien à cacher vous n'avez rien à craindre », phrase célèbre du parlementaire anglais Richard Graham, de l'ancien premier secrétaire d'Etat et secrétaire des affaires étrangères britannique William Hague, mais surtout de Joseph Goebbels qui l'utilise en premier [43].

La police est en effet dépassée par le volume, la demande pour ces services qui s'est développée en ligne, et le fait que si une plateforme d'échanges illégaux tombe, une autre réapparait, tout simplement. Un vrai jeu du chat et de la souris, par exemple dans le cas du trafic de faune et de flore [6], un trafic particulièrement destructeur.

Cette phrase sous-entend qu'attraper les criminels justifie une intrusion dans la vie privée de l'ensemble des citoyens, d'un pays particulier ou même du monde entier. Toutefois Thomas Blake, ancien

analyste pour l'armée américaine devenu tireur d'alarme, tire un portrait moins reluisant de la « vraie » surveillance, qu'il a lui-même opéré : « Vous comprenez pourquoi l'Etat veut faire des exemples : ils n'ont pas à stigmatiser des portions entières de la population, ils ont juste à les surveiller. Et ceux qui s'expriment un peu plus, qui demandent des comptes aux autorités, c'est ceux-là qu'on va surveiller avec attention. Surtout s'ils s'organisent, montent une association » [29].

La première motivation d'une telle surveillance n'est pas vraiment d'attraper les criminels, mais plutôt de contrôler la population. Un avis partagé par Bruce Schneier, expert en cybersécurité américain et auteur de nombreux livres sur le sujet, qui cite notamment cette phrase attribuée au cardinal Richelieu : « Quon me donne six lignes écrites de la main du plus honnête homme, jy trouverai de quoi le faire pendre ». D'après lui, « beaucoup caractérisent le débat comme "vie privée contre sécurité". Mais le vrai choix est entre "vie privée et contrôle" » [41].

Je n'ai pas de réponse claire à apporter à ce qu'il faut faire pour empêcher ces gens-là de procéder à leurs activités. C'est un problème épineux, que beaucoup ont déjà essayer de traiter, et pas seulement en ligne. Une chose est sûre, il est possible de se protéger convenablement, si on en fait l'effort. Par exemple, des dizaines de guides existent en ligne comment se protéger efficacement, notamment pour les journalistes [12]. Même si le gouvernement instaure une surveillance draconienne, il sera toujours possible pour un acteur motivé d'y échapper.

Par contre, pour toutes les raisons exposées ci-dessus, il m'apparaît clair que la vie privée d'un individu est trop importante pour que l'on enlève ce droit à tout le monde, sous couvert d'essayer d'arrêter les comportements illicites. Surtout que malgré les dispositifs en place aujourd'hui, des dispositifs déjà assez vieux (13 ans dans le cas de PRISM par exemple, détaillé ci-dessous), le trafic en ligne est toujours un problème : la vente de drogues sur le Darknet représente 18 millions d'euros par mois en 2016, selon un rapport du RAND pour le gouvernement néerlandais [13].

En somme, arrêter le trafic de substances illégales en ligne et autres actes illégaux est louable. Mais une surveillance constante sur l'ensemble de la population ne permettra, premièrement, pas de se débarrasser de ces abus. Ceux qui souhaitent trafiquer trouveront toujours un moyen de le faire. Elle se ferait de plus au mépris de ce droit, et entraînerait tout un tas de problèmes, exposés plus haut, pour un gain somme toute très relatif.

Votre vie privée informationnelle, sous assaut

Aujourd'hui, tout le monde se sait surveillé et traqué sur Internet, comme nous l'avons montré plus haut. Mais, à la manière du panoptique, on se sait pas quand, ni exactement comment, ce qui nous pousse à nous censurer en permanence. Cette partie a pour but d'expliquer exactement comment un citoyen lambda est surveillé sur Internet, quelles sont les données qui lui sont associées, qui y a accès et comment.

Surveillance étatique

Les révélations d'Edward Snowden [46] depuis l'été 2013 ont permis à des journalistes du *Guardian* et du *Washington Post* notamment, de détailler plusieurs programmes de surveillance globale américains (PRISM, XKeyscore, ...) et britanniques (Tempora, Muscular, ...). Et à l'appui, l'ancien contracteur de la NSA a divulgué aux journalistes un nombre très important de documents décrivant les opérations de la NSA principalement, mais également d'autres agences gouvernementales (1,7 millions étant l'estimation la plus récente de l'ampleur des fuites).

Aujourd'hui, Edward Snowden jouit d'un droit de résidence en Russie et est toujours poursuivi aux Etats-Unis pour espionnage et vol de propriété gouvernementale. Les équipes du *Guardian* et du *Washington Post* ont quant à elles été récompensées du prix Pulitzer, pour leurs « révélations sur la surveillance secrète globale menée par la NSA, ayant aidé grâce à leurs articles agressifs à initier un débat sur des problèmes concernant vie privée et sécurité » [36].

Nous ne reviendrons pas ici sur tous les programmes dévoilés, car il y en a beaucoup trop. Nous essayerons toutefois de détailler certains d'entre eux, considérés ici comme les plus « intéressants ». Et pour commencer, la collecte massive d'informations sur les utilisateurs de Verizon, un grand opérateur américain : le pouvoir a été conféré à la NSA par FISA, et Verizon se devait de fournir à la NSA et au FBI toutes les informations dont elle dispose. Ces informations sont les numéros de ceux qui appellent, la durée de la conversation, leur localisation respective, notamment, et ceux pour les appels des Etats-Unis vers l'étranger mais aussi au sein du territoire [18].

Autre dispositif, cette fois affectant le monde entier : PRISM, un programme lancé en 2007 qui autorise la NSA, cette fois encore via une décision de FISA (toutes classées confidentielles, rappelons-le), à demander les informations collectées par Google, Facebook, Apple et autres géants du secteur technologique. Tous les documents liés à des recherches spécifiques, prédéfinies par FISA, doivent être mis à disposition. Il peut s'agir d'emails, de vos chats Facebook, de votre historique de recherche, etc [19].

Pour finir, nous allons détailler XKeyScore, encore un autre programme de surveillance qui lui recueille « presque tout ce qu'un utilisateur fait sur Internet ». Cet outil permet aux analystes de la NSA de « rechercher dans une vaste base de données, remplie d'emails, conversations en ligne et historique de millions d'individus, sans avoir besoin d'autorisation préalable ». Une phrase assez controversée de Snowden est expliquée par ce programme : « Assis à mon bureau, tout de suite, je peux espionner (« wiretap », ndt) n'importe qui, vous, votre comptable, un juge fédéral ou même le président, sous réserve d'avoir son email personnel » [21].

En somme, la surveillance est extensive, et nous n'avons ici détaillé qu'une toute petite partie des moyens en place. Ces agences gouvernementales, américaines mais mondiales, utilisent toutes les possibilités que le numérique offre, et n'hésitent pas à recourir aux données stockées par des entreprises tierces. Un constat assez alarmant sur leur pouvoir, surtout qu'aujourd'hui, six ans après ces fuites, ils continuent selon toute vraisemblance à être utilisés.

Intérêts privés

Aujourd'hui, Internet a un rôle très important dans notre vie. Nous sommes beaucoup à en avoir besoin tous les jours. La gratuité du contenu sur Internet a longtemps été principalement portée par la publicité, et continue aujourd'hui à faire vivre beaucoup de sites. En 2017, les revenus publicitaires totaux sur le web sont d'environ 88 milliards de dollars. Google tire de sa place prédominante dans le marché une part importante de ses revenus, via Google AdWords : près de 35 milliards de dollars. Pour Facebook (ou plutôt, pour les « réseaux sociaux » en général), les revenus sont en constante progression, ayant doublé entre 2015 et 2017, pour un total de 22,2 milliards de dollars. En 2017 ce sont 63% des dépenses publicitaires totales sur Internet qui reviennent à ces deux entreprises [4].

Vos données sont importantes pour les entreprises du numérique, c'est un fait. Il faut donc commencer par remettre ces grandes entreprises en place. Avant d'être des acteurs majeurs du monde technologique, Facebook et Google sont avant tout des publicitaires, et vos données sont leur ressource la plus précieuse.

Ces même données sont souvent utilisées sans que vous en ayiez vraiment conscience. Google Maps, par exemple, fournit un service de géolocalisation payant aux entreprises, basé sur les bornes d'accès WiFi environnantes. En gros, il suffit de scanner les points WiFi détectés, la puissance du signal, et remonter toutes ces infos à Google, qui vous répond par une localisation approximative. Comment Google a-t-il construit ce service ? La réponse est simple, c'est les téléphones Android du monde entier qui lui envoient ces données, et lui permettent de garder une base de données à jour et complète. Ainsi, pour peu que vous utilisiez le service de localisation de Google Maps sur votre téléphone, les réseaux WiFi que vous scannez couplés à votre géolocalisation sont remontés [47].

Et c'est loin d'être la seule information que Google récolte. Une étude menée par le journal Quartz, avec des téléphones Android neufs, a mis en évidence l'ampleur des fuites : le mouvement que votre téléphone pense que vous faîtes (avec des pourcentages, de type « Marche : 51%, Sur un vélo : 4%, Dans le métro : 3% »), la pression atmosphérique, l'adresse MAC de votre point d'accès WiFi (identifiant unique), l'adresse MAC, puissance et fréquence de tous les autres points d'accès à proximité, les mêmes infos pour les points d'accès Bluetooth, le niveau de charge de votre batterie, son voltage, vos coordonnées GPS et la précision associée, votre altitude GPS et la précision associée [47]. De quoi donner le tournis !

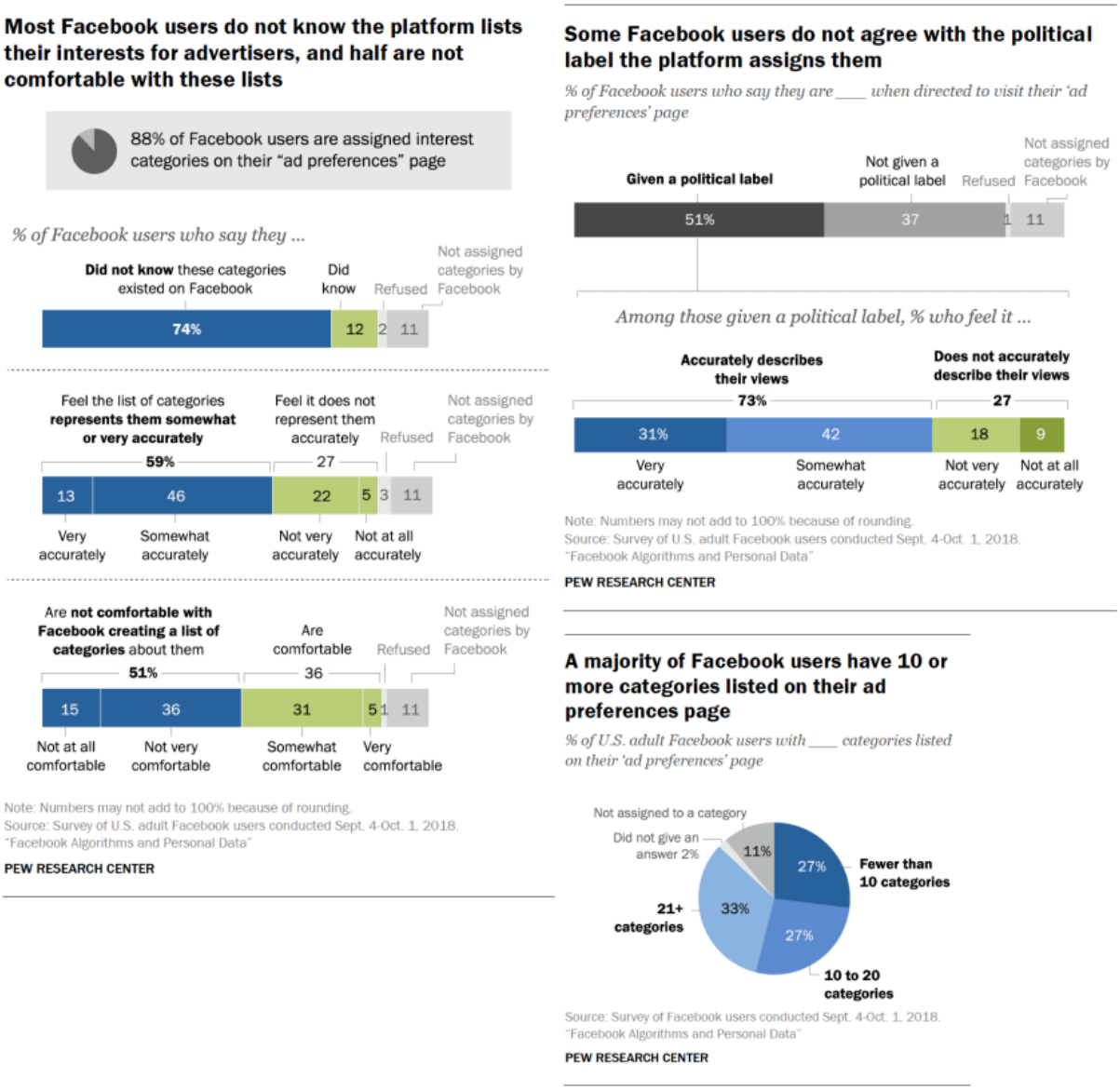
Facebook, bien sûr, n'est pas en reste, mais le travail est bien plus facile pour lui. Pas besoin de recueillir la moindre information, nous la fournissons nous-même : nous indiquons participer à tel ou tel évènement, suivons les pages de nos artistes préférés, « likons » les vidéos qui suivent notre ligne de pensée, politique, environnementale, ou en matière de football. C'est un véritable portrait psychologique qui pourrait être dressé, et Facebook a bel et bien sauté le pas. Dans des documents confidentiels récupérés par The Australian, rédigé par les hauts-placés Facebook en Australie et à destination d'une grande banque du pays, le réseau social indique savoir quand un adolescent se sent « angoissé », « stressé », « nerveux », « inutile » ou même « un échec ». Facebook qui d'ailleurs sait très bien qui utilise son service en Australie, « 1,9 millions de lycéens, 1,5 millions d'étudiants dans le supérieur et 3 millions de jeunes actifs », et met à disposition de l'annonceur leur « localisation, statut amoureux, et la date de dernière visite sur la plateforme, en ligne et sur mobile » [26]. Le document en question n'a pas été publié, mais Facebook a plus tard réagit en affirmant qu'il s'agit d'un « un papier de recherche partagé avec un annonceur », pour lui permettre de « mieux comprendre comment les gens s'expriment » sur le réseau social.

Ce n'est pas la première fois que Facebook se cache derrière « la recherche » pour justifier ses actions. En 2014, l'entreprise avait déjà essuyé beaucoup de critiques pour avoir manipulé les émotions de 689 000 utilisateurs (ou plutôt, rats de laboratoire ?). Après les avoir divisé en deux groupes, elle a supprimé du fil d'actualité du premier la moitié des posts « positifs », du deuxième la moitié de ceux « négatifs », pendant une semaine en janvier 2012. Les conclusions de la recherche sont somme toute assez intéressantes, les émotions ont prouvées être « contagieuses ». Si vous voyez plus de posts déprimants, votre moral en prendra un coup, et le contraire est vrai [22].

Une conclusion intéressante, donc, mais à quel prix ? Pourtant, Facebook nous avait bien prévenu : il est écrit noir sur blanc dans sa politique d'utilisation des données qu'elle se réserve le droit de l'utiliser pour « faire de la recherche et innover pour le bien-être social ». La recherche inclut donc visiblement l'éventuelle manipulation des utilisateurs et de leurs émotions [14].

L'un des problèmes majeurs à mon sens est très simple : si chacun avait conscience de l'énorme quantité de données offerte à ces entreprises, des comportements plus responsables auraient sûrement lieu, les réseaux sociaux décentralisés comme Mastodon ou Diaspora auraient beaucoup plus de succès par exemple. Mais dans les faits, beaucoup d'utilisateurs Facebook ne se savent pas du tout traqués. Une étude du Pew Research Center a été menée sur le sujet, et sur les quelques 1000 personnes représentatives

FIGURE 2 – "Facebook Algorithms and Personal Data", graphiques, Pew Research Center



interrogées, ils sont 74% à ignorer que leurs intérêts sont catégorisés et disponibles aux annonceurs. 59% d'entre eux pensent que ces catégories les représentent assez bien, et 51% n'aiment pas l'idée que Facebook crée ces catégories [9].

La gestion de ces informations, très personnelles, n'est de plus pas toujours irréprochable. Bien sûr, chaque acteur agit selon ses propres conditions d'utilisation, au moins sur le papier. Mais même si vous avez confiance en Facebook, par exemple, le fait qu'il ait accès à ces données les ouvrent potentiellement à d'autres, en plus des risques de cybersécurité déjà mentionnés plus haut.

Ainsi, la perspective de ces données utilisées pour influencer le vote pour le prochain président de la république, par exemple, ne doit pas vous mettre très à l'aise. C'est pourtant la spécialité de Cambridge Analytica, une firme britannique combinant analyse de données et data mining pour « changer le comportement grâce aux données ». En 2016, elle est utilisée par Donald Trump pour gagner plus d'informations sur son électorat [5].

Mais là où le bât blesse, c'est que ces données, si cruciales à l'offre de Cambridge Analytica, n'ont pas été recueillies dans les règles : elles l'ont été à travers un quiz présenté comme exclusivement « académique », ne faisant aucune mention d'une quelconque information remontée à qui que ce soit. Or celui-ci récupère non seulement les informations de la personne qui participe mais également celles de tous ses amis. Le fondateur de l'entreprise, Alexander Nix, filmé en caméra cachée, indique de plus que les pratiques de la société « s'étendent à la diffusion volontaire de fausses informations, à l'espionnage

d'adversaires politiques, au recours à des prostituées et à la corruption pour manipuler l'opinion publique à l'étranger » [5].

Le constat dressé jusqu'à présent est donc assez alarmant. Nos données sont exploitées de toute part, et pourraient bien facilement être retournées contre notre société. Certains affirment que c'est déjà le cas, et que Cambridge Analytica et les « trolls russes » ont décuplé la popularité de Donald Trump, et lui ont permis de se faire élire [17]. Cela nous pousse à nous interroger sur le futur, quel avenir pour notre vie sur Internet, et plus largement notre société ?

Vers une société sans vie privée ?

Ce constat nous pousse à nous intéresser à la Chine. Si un régime totalitaire venait à être instauré en Europe, il est totalement possible que la situation évolue, au moins partiellement, en ce sens. Pour finir, nous nous demanderons vers quoi notre société pourrait évoluer, et reviendrons pour ce faire sur deux oeuvres de fiction, Black Mirror et 1984.

Le cas chinois

Pourquoi s'intéresser aux chinois ? C'est un pays autoritaire qui a mis en place des moyens de surveillance pour ouvertement surveiller la population, et qui le revendique comme la politique phare du parti communiste. Voilà qui n'arriverait jamais dans un pays occidental...

Pourtant, Thomas Blake cité auparavant affirme que si quelqu'un de mal intentionné est élu, les Etats-Unis, l'Allemagne et d'autres sociétés occidentales ne sont qu'à un pas du régime totalitaire : « les démocraties occidentales comme l'Allemagne d'aujourd'hui ne sont pas des états policiers. Mais les mécanismes nécessaires pour l'instauration d'un tel état sont déjà en place. La seule vraie différence, c'est ceux au pouvoir » [29]. Et personne ne peut garantir que cela ne se produira pas.

La surveillance en Chine regroupe les outils à disposition du pouvoir et les utilise conjointement pour contrôler finement la population : par exemple des caméras dans les rues, à reconnaissance facile, ou des points de contrôle à l'entrée du métro. Mais aussi un système de crédit social instauré il y a quelques mois, qui deviendra obligatoire pour tous les chinois à partir de 2020 [1].

Son fonctionnement est simple : les autorités surveillent vos comportements, et utilisent ces informations pour vous donner une note sur 800. Le crédit est calculé à partir de ce que vous achetez au supermarché, les sites web que vous visitez, si vous sortez vos poubelles fréquemment, etc. Mais il prend également en compte vos idées politiques : il est une mauvaise idée d'exprimer son désaccord avec le parti communiste, ou de discuter de démocratie, libertés fondamentales, et autres sujets jugés par le régime comme tabou.

Pour ceux qui se « comportent bien », de nombreux avantages sont à la clé, parce qu'ils sont considérés « dignes de confiance ». Des avantages comme le droit de réserver une chambre d'hôtel ou une voiture sans avancer les frais [1].

Par contre, si votre crédit social est bas, vous êtes considéré « malhonnête ». Liu Hu, le journaliste chinois décrit ci-dessus, en a particulièrement ressenti les effets pour ses problèmes avec les autorités. Son score est très bas, et il est donc effectivement assigné à résidence dans sa ville natale de Chongqing. Pas question pour lui de songer à acheter un vol vers l'international : de simples tickets de train vers les villes avoisinantes lui sont maintenant refusés [1].

« Beaucoup de gens en Chine sont sur la liste noire sans bonne raison, et ils n'arrivent pas à en sortir », indique-t-il.

Point de vue intéressant, celui des youtubers d'ADVChina : un anglais et un américain vivant en Chine. Ils relèvent les mêmes éléments que ceux que nous exposons ci-dessus, mais les nuancent avec leur expérience sur place : « quand tu fais quelque chose de "mauvais", les gens dans nos pays (Etats-Unis et Grande Bretagne en l'occurence, ndlr) n'hésitent pas à te confronter. En Chine, les gens t'ignorent, tout simplement, et donc beaucoup de monde ne suit pas les règles ». « De vrais règles sociales sont maintenant respectées avec ce nouveau système ». « Le comportement des jeunes est certes bien meilleur que celui des plus vieux, mais il y a des dizaines de millions de personnes sans aucun tact ou bienséance sociale » [3]. Si, de notre point de vue occidental, il est difficile de défendre un tel système, on comprend que les locaux, eux, puissent le voir d'un bon oeil.

Hu est également conscient de l'avis général de la population, et le voit comme un clair endoctrinement : « Leurs yeux sont bandés, leurs oreilles sont bloquées. Ils en savent peu sur le monde et vivent dans l'illusion » [1].

Le futur dans l'imaginaire

En me documentant sur la surveillance en Chine, j'ai été choqué par les similarités avec un épisode de Black Mirror, « Chute libre » [31]. Celui-ci montre la vie en société sous un système de réputation, influencé par le vote de tout le monde. Si vous conduisez mal ou faites quelque chose qui est mal perçu, vous vous exposez à recevoir des basses notes de tous les témoins. Si par contre vous publiez une photo sur les réseaux sociaux et qu'elle est bien reçue, vous gagnez des points.

Dans l'épisode, l'héroïne doit avoir une note de 4,5/5 ou plus, pour pouvoir acheter un appartement à crédit, une mesure qui irait à merveille avec les autres implémentées pour le crédit social chinois. A 4,2 pour le moment, elle redouble d'efforts pour être bien vue, au point de pratiquer son sourire le matin en face d'un miroir, d'acheter un café qu'elle ne boira pas simplement pour en prendre une photo. Tout le monde se doit d'être gentil constamment, les relations sociales s'en voient complètement faussées.

Même un mariage devient une façon de gagner des points. Au lieu d'avoir sa meilleure amie comme demoiselle d'honneur, c'est l'héroïne qui est choisie pour le rôle car sa note, celle d'un « bas 4 », couplée à une histoire fabriquée de toutes pièces, est considérée « optimale » pour gagner des points, selon plusieurs simulations.

Bien sûr, il nous est impossible de terminer ce document sans faire allusion à 1984, la célèbre dystopie de George Orwell [33], écrite en 1948. En 1984 et après une guerre nucléaire vers les années 1950, elle montre la vie sous un régime totalitaire mené par « Big Brother », une personnification de l'état policier. Le roman révèle de plus en plus comme une anticipation de la société d'aujourd'hui, et celle vers laquelle on va. Pour rappel, nous y suivons l'histoire de William Smith, qui se révèle être un « criminel de la pensée ». Mais William Smith n'est qu'un prétexte pour nous montrer la vie sous la surveillance de Big Brother, la « Police de la Pensée », la modification de la langue pour rendre toute doctrine non conforme difficile à formuler [33].

Aujourd'hui, la célèbre phrase « Big Brother is watching you » (Big Brother vous regarde), est communément utilisée pour désigner l'ensemble des activités de surveillance gouvernementales que nous avons décrit.

Conclusion

Nous avons abordé dans le présent document beaucoup de concepts bien différents, tant philosophiques et sociologiques que pratiques, en rapport avec la vie privée d'un individu aujourd'hui. Entre le début de l'écriture de ce document, en 2016, et aujourd'hui, beaucoup de choses ont déjà évolué dans le bon sens. A l'époque, les discussions pour la mise en place du RGPD apparaissaient au point mort, le cadre légal était beaucoup moins défini, et nos données étaient plus que jamais exploitées par les grandes entreprises américaines, en plus d'une surveillance mondiale qui était déjà apparente.

Aujourd'hui, je suis content de pouvoir dire qu'au moins au niveau légal, les choses ont évolué dans le bon sens, et les droits des citoyens (européens) ne sont plus autant pris à la légère. Evidemment, beaucoup reste à améliorer, notamment en ce qui concerne la surveillance étatique, sur laquelle nous n'avons vu aucune évolution (mis à part entre les Etats-Unis et l'Europe avec la déclassification des décisions du tribunal FISA dans le cadre du Privacy Shield, un gain relativement minime mais déjà non négligeable).

Ma conclusion est toutefois que même si des pas sont faits dans le bon sens, notre droit à la vie privée n'a jamais été aussi important. L'élection de Donald Trump, Jair Bolsonaro récemment laisse présager que l'apparition d'un leader totalitaire en Europe n'est en fait pas si improbable que cela. Et si cela arrive, de fortes protections sur ce droit sont nécessaires à l'exercice de tous les autres.

Remerciements

Je souhaite remercier en particulier M. Lesueur, pour son aide apportée tout au long de l'écriture du document. Nombreuses de mes sources m'ont été suggérées par lui et ce document ne serait pas le même sans ses précieux conseils et ses relectures avisées.

J'aimerai également remercier la Bibliothèque Marie Curie de l'INSA Lyon, qui a commandé à ma demande le livre d'Iteanu m'ayant beaucoup aidé à cadrer mes recherches, en plus des autres ouvrages disponibles auxquels j'ai pu avoir accès.

Enfin, je terminerai par remercier Edward Snowden, sans qui nous en saurions, aujourd'hui encore, beaucoup moins sur la surveillance mondiale. Ses révélations ont contribué à un fort débat de société sur la vie privée et l'ont catalysé. Sans lui, des lois comme le RGPD n'auraient peut-être pas eu la médiatisation nécessaire à être adoptées.

Bibliographie

[1] ABC News (Australia). *Exposing China's Digital Dystopian Dictatorship | Foreign Correspondent*. Sept. 2018. URL : https://www.youtube.com/watch?v=eViswN602_k.

[2] Louis Adam. *Faille Facebook : lourde amende à cause du RGPD ? Pas si sûr...* Oct. 2018. URL : https://www.zdnet.fr/actualites/faille-facebook-lourde-amende-a-cause-du-rgpd-pas-si-sur-39874457.htm.

[3] ADVChina. *China's Dystopian Social Credit system*. Oct. 2018. URL : https://www.schneier.com/essays/archives/2006/05/the_eternal_value_of.html.

[4] Pierrick Aubert. *Facebook et Google : les rois de la pub !* Fév. 2018. URL : https://www.zdnet.fr/blogs/watch-it/facebook-et-google-les-rois-de-la-pub-39863764.htm.

[5] William Audureau. *Ce quil faut savoir sur Cambridge Analytica, la société au cur du scandale Facebook*. Mar. 2018. URL : https://www.lemonde.fr/pixels/article/2018/03/22/ce-qu-il-faut-savoir-sur-cambridge-analytica-la-societe-au-c-ur-du-scandale-facebook_5274804_4408996.html.

[6] Rachael Bale. *Google, Facebook, and Other Tech Giants Unite to Fight Wildlife Crime Online*. Mar. 2018. URL : https://news.nationalgeographic.com/2018/03/wildlife-watch-tech-companies-online-wildlife-crime-coalition/.

[7] Daniel Borrillo. *Le mariage pour tous et ses ennemis*. Avr. 2018. URL : https://www.liberation.fr/debats/2018/04/23/le-mariage-pour-tous-et-ses-ennemis_1645281.

[8] Serge Braudo. *Définition de Vie privée*. URL : https://www.dictionnaire-juridique.com/definition/vie-privee.php.

[9] Pew Research Center. *Facebook Algorithms and Personal Data*. Jan. 2019. URL : http://www.pewinternet.org/2019/01/16/facebook-algorithms-and-personal-data/.

[10] Guillaume Champeau. *Qui d'Apple ou Google saura quand vous faites l'amour ?* Jan. 2015. URL : https://www.numerama.com/magazine/31782-qui-d-apple-ou-google-saura-quand-vous-faites-l-amour.html.

[11] CNIL. *La formation restreinte de la CNIL prononce une sanction de 50 millions deuros à lencontre de la société GOOGLE LLC*. Jan. 2019. URL : https://www.cnil.fr/fr/la-formation-restreinte-de-la-cnil-prononce-une-sanction-de-50-millions-deuros-lencontre-de-la.

[12] Michael Dagan. *Online Privacy Guide for Journalists*. Jan. 2019. URL : https://www.vpnmentor.com/blog/online-privacy-journalists/.

[13] RAND Europe. *Taking Stock of the Online Drugs Trade*. Août 2016. URL : https://www.rand.org/randeurope/research/projects/online-drugs-trade-trafficking.html.

[14] Facebook. *Politique dutilisation des données*. Jan. 2019. URL : https://fr-fr.facebook.com/privacy/explanation.

[15] Michel Foucault. *Surveiller et punir*. Gallimard, fév. 1975.

[16] Generation-NT. *RGPD : une première condamnation à 250 000 d'amende pour Optical Center*. Juin 2018. URL : https://www.generation-nt.com/rgpd-premiere-condamnation-250-000-amende-optical-center-actualite-1954919.html.

[17] Michelle Goldberg. *Yes, Russian Trolls Helped Elect Trump*. Déc. 2018. URL : https://www.nytimes.com/2018/12/17/opinion/russia-2016-election-influence-trump.html.

[18] Glenn Greenwald. *NSA collecting phone records of millions of Verizon customers daily*. Juin 2013. URL : https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

[19] Glenn Greenwald. *NSA Prism program taps in to user data of Apple, Google and others*. Juin 2013. URL : https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

[20] Glenn Greenwald. *Why privacy matters*. Oct. 2014. URL : https://www.ted.com/talks/glenn_greenwald_why_privacy_matters.

[21] Glenn Greenwald. *XKeyscore : NSA tool collects 'nearly everything a user does on the internet'*. Juil. 2013. URL : https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data.

[22] Kashmir Hill. *Facebook Manipulated 689,003 Users' Emotions For Science*. Juin 2014. URL : https://www.forbes.com/sites/kashmirhill/2014/06/28/facebook-manipulated-689003-users-emotions-for-science/.

[23] Olivier Iteanu. *Quand le digital défie l'état de droit*. Eyrolles, oct. 2016.

[24] Robbie Johnson. *Privacy no longer a social norm, says Facebook founder*. Jan. 2010. URL : https://www.theguardian.com/technology/2010/jan/11/facebook-privacy.

[25] Dictionnaire Larousse. *Définition de privé.e*. URL : https://www.larousse.fr/dictionnaires/francais/priv%C3%A9_priv%C3%A9e/64013.

[26] Sam Levin. *Facebook told advertisers it can identify teens feeling 'insecure' and 'worthless'*. Mai 2017. URL : https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens.

[27] CNIL (Comission Nationale de l'Informatique et des Libertés). *Le Privacy Shield*. Mai 2017. URL : https://www.cnil.fr/fr/le-privacy-shield.

[28] Jean-Marc Manach. *La vie privée, un problème de vieux cons ?* Mar. 2009. URL : http://www.internetactu.net/2009/03/12/la-vie-privee-un-probleme-de-vieux-cons/.

[29] Mihaela Gladovic Marc Meillassoux. *Nothing to Hide*. Oct. 2017. URL : https://vimeo.com/189016018.

[30] Antonio Negri Michael Hardt. *Empire*. Harvard University Press, 2000.

[31] Charlie Brooker - Netflix. *Black Mirror - saison 3, épisode 1 - "Chute libre"*. Oct. 2016.

[32] NOYB.eu. *GDPR : noyb.eu filed four complaints over "forced consent" against Google, Instagram, WhatsApp and Facebook*. Mai 2018. URL : https://noyb.eu/wp-content/uploads/2018/05/pa_forcedconsent_en.pdf.

[33] George Orwell. *1984*. Secker et Warburg, juin 1949.

[34] Article 29 Data Protection Working Party. *EU U.S. Privacy Shield - First annual Joint Review*. Nov. 2017. URL : https://iapp.org/media/pdf/resource_center/Privacy_Shield_Report-WP29pdf.pdf.

[35] Jon Penney. « Chilling Effects : Online Surveillance and Wikipedia Use ». In : *Berkeley Technology Law Journal, Vol. 31, No. 1, p. 117* (avr. 2016).

[36] Ed Pilkington. *Guardian and Washington Post win Pulitzer prize for NSA revelations*. Avr. 2014. URL : https://www.theguardian.com/media/2014/apr/14/guardian-washington-post-pulitzer-nsa-revelations.

[37] Laura POITRAS. *Citizenfour - film*. Oct. 2014.

[38] Proton Technologies Programme Horizon 2020 (UE). *GDPR overview, compliance*. Jan. 2019. URL : https://gdpr.eu/.

[39] David Roe. *Why the Privacy Shield Won't Make You GDPR-Compliant*. Mai 2018. URL : https://www.cmswire.com/information-management/why-the-privacy-shield-wont-make-you-gdpr-compliant/.

[40] Beate Rossler. *The Value of Privacy*. John Wiley & Sons, mar. 2018.

[41] Bruce Schneier. *The Eternal Value of Privacy*. Mai 2006. URL : https://www.schneier.com/essays/archives/2006/05/the_eternal_value_of.html.

[42] Edward Snowden. *Just days left to kill mass surveillance under Section 215 of the Patriot Act. We are Edward Snowden and the ACLUs Jameel Jaffer. AUA - Reddit.* Mai 2015. URL : https://www.reddit.com/r/IAmA/comments/36ru89/just_days_left_to_kill_mass_surveillance_under/crglgh2.

[43] Edward Snowden. *Tory MP Richard Graham accused of quoting Joseph Goebbels in defence of new surveillance bill.* Nov. 2015. URL : https://www.indy100.com/article/tory-mp-richard-graham-accused-of-quoting-joseph-goebbels-in-defence-of-new-surveillance-bill--bklSCE9n0g.

[44] Mary Ann Tétreault. « Frontier Politics : Sex, Gender, and the Deconstruction of the Public Sphere ». In : *Alternatives : Global, Local, Political* (2001).

[45] Martin Untersinger. *Cinquante millions de comptes Facebook affectés par une faille de sécurité.* Sept. 2018. URL : https://www.lemonde.fr/pixels/article/2018/09/28/facebook-une-faille-de-securite-concernant-des-dizaines-de-millions-de-comptes-decouverte_5361846_4408996.html.

[46] Wikipédia. *Révélations d'Edward Snowden - chronologie de tous les articles.* URL : https://fr.wikipedia.org/wiki/R%C3%A9v%C3%A9lations_d'Edward_Snowden.

[47] David Yanofsky. *If youre using an Android phone, Google may be tracking every move you make.* Jan. 2018. URL : https://qz.com/1183559/if-youre-using-an-android-phone-google-may-be-tracking-every-move-you-make/.