Pourquoi il ne faut pas rire du hack d'Ashley Madison

Kevin Poireault, Les Inrockuptibles, 20/08/2015[1].

Si la révélations des données du site de rencontre pour infidèles Ashley Madison a d'abord fait rire beaucoup d'internautes, de plus en plus de gens s'inquiètent aujourd'hui de l'impact que ce piratage pourrait avoir sur l'avenir de la vie privée en ligne.

Mardi 18 août, The Impact Team a tenu parole. Comme aucun des deux sites d'Avid Media Life n'a été fermé, les hacktivistes ont publié les données de près de 35 millions d'utilisateurs d'Ashley Madison (sur 40 millions d'utilisateurs au total, selon le site lui-même). Il y a un mois, ce groupe de hackers a réussi à pirater le site de rencontres adultères AshleyMadison.com et à s'emparer des données de ses utilisateurs. Leur objectif : obliger Avid Media Life (le propriétaire du site), à le fermer ainsi qu'EstablishedMen.com (qui propose aux jeunes filles de trouver un suggar daddy [2]).

En divulguant ces données, les hackers ne revendiquent pas seulement un acte moral - moraliste pour certains - mais visent aussi à dénoncer la fragilité du système de sécurité d'Avid Media Life, qui aurait "menti" à ses utilisateurs en leur affirmant que la confidentialité d'Ashley Madison était assurée. Ce faisant, ces "lanceurs d'alerte" ont compliqué - et parfois même mis en danger - la vie de ces internautes.

En tout, 9,7 gigabytes de données ont été divulgués sur le darknet — un réseau accessible uniquement via des plateformes spéciales, comme le navigateur Tor. On y trouve les coordonnées géographiques et bancaires (ou du moins une partie), les transactions bancaires des sept dernières années ainsi que les identifiants de chaque utilisateur.

[...]

Sur Twitter, les premières réactions amusées ont aujourd'hui laissé place à ces mêmes avertissements, de la part de spécialistes de la vie privée sur Internet mais aussi d'utilisateurs ordinaires. Comme cette twitto, qui publie, à destination de ceux qui "essaient encore de justifier le leak d'Ashley Madison", le témoignage d'un utilisateur saoudien et gay dont les données ont été révélées et qui exprime sa peur d'être condamné à mort dans son pays sur le réseau social Reddit.

Sur le message on peut lire que ce jeune homme a fréquenté le site Ashley Madison lorsqu'il était aux Etats-Unis et que, aujourd'hui rentré en Arabie Saoudite, il craint pour sa vie car ses données ont été divulguées sur la Toile. Il [demande] comment il peut s'y prendre pour acquérir le statut de réfugié.

1. https://www.lesinrocks.com/2015/08/20/actualite/actualite/pourquoi-il-ne-faut-pas-rire-du-hack-dashley-madison/

2. *Suggar daddy :* Homme qui entretient une femme plus jeune que lui en échange d'une relation amoureuse.

Pour le fondateur de Facebook, la protection de la vie privée n'est plus la norme

Le Monde, 11 janvier 2010[1].

"Les gens sont désormais à l'aise avec l'idée de partager plus d'informations différentes, de manière plus ouverte et avec plus d'internautes. (...) La norme sociale a évolué." Le PDG de Facebook, Mark Zuckerberg, est revenu dimanche, à San Francisco, sur la modification des paramètres de vie privée de son réseau social, et estimé que les 350 millions d'utilisateurs du site n'attachent plus autant d'importance à la protection de leurs données personnelles.

Pour le fondateur du plus grand réseau social au monde, cette évolution justifie les modifications des paramètres de vie privée du site, mises en place mi-décembre, et vivement critiquées par les associations de défense de la vie privée. Mark Zuckerberg, qui s'était lui-même fait piéger par le changement de paramètres sur son propre compte personnel, a estimé que cette évolution du site était nécessaire, et reflétait "ce que seraient les normes si nous lancions le site aujourd'hui". [...]

Pour Mark Zuckerberg, ce sont principalement les jeunes générations qui ont une notion différente de ce qu'est la vie privée, et de la manière dont elle doit être protégée.

1. https://www.lemonde.fr/technologies/article/2010/01/11/pour-le-fondateur-de-facebook-la-protection-de-la-vie-privee-n-est-plus-la-norme_1289944_651865.html

The terrifying surveillance case of Brandon Mayfield

Matthew Harwood, Aljazeera America, 8/02/2014[1], traduit par le Framablog : *L'affaire Brandon Mayfield : une surveillance terrifiante, Framablog, le 12/02/2014*[2].

Le 11 mars 2004 à Madrid, des terroristes proches de la mouvance d'Al-Qaïda ont coordonné un attentat à la bombe sur plusieurs trains de banlieue durant l'heure de pointe matinale. 193 personnes furent tuées et environ 1 800 furent blessées. Deux empreintes digitales partielles découvertes sur un sac de détonateurs au cours de l'enquête par la Police Nationale Espagnole (PNE) furent partagées avec le FBI par le biais d'Interpol. Les deux empreintes furent entrées dans la base de données du FBI, qui retourna vingt concordances possibles pour l'une d'entre elles : sur ces vingt concordances, l'une appartenait à Brandon Mayfield. […] Ses empreintes étaient répertoriées dans le système du FBI parce qu'il avait fait son service militaire mais aussi parce qu'il avait été arrêté sur un malentendu vingt ans auparavant. Les charges avaient ensuite été abandonnées.

[…] Certains détails de la vie de l'avocat ont convaincu les agents qu'ils tenaient leur homme. Mayfield s'était converti à l'Islam après avoir rencontré sa femme, une égyptienne. Il avait offert son aide juridique sur une affaire de garde d'enfant à l'un des « Portland Seven », un groupe d'hommes qui avait essayé d'aller en Afghanistan afin de combattre pour Al-Qaïda et les Talibans contre les États-Unis et leurs forces alliées. Il fréquentait aussi la même mosquée que les militants. […]

Des agents du FBI pénétrèrent par effraction dans la maison de Mayfield et dans son cabinet d'avocat. Ils fouillèrent dans des documents protégés par le secret professionnel entre un avocat et son client, ils mirent sur écoute ses téléphones, ils analysèrent sa comptabilité et son historique de navigation Internet, ils fouillèrent même ses poubelles. Ils le suivirent dans tous ses déplacements.

[…]

Pensant que leur couverture avait sauté, les agents du FBI placèrent Mayfield en détention comme témoin matériel dans l'attentat de Madrid, au motif qu'ils craignaient un risque de fuite. […] Il passa deux semaines en prison, terrifié à l'idée que ses codétenus apprennent qu'il était impliqué d'une manière ou d'une autre dans les attentats de Madrid et qu'ils ne l'agressent.

[…]

La seule raison pour laquelle Mayfield est un homme libre aujourd'hui, c'est que la police espagnole a répété à plusieurs reprises au FBI que l'empreinte récupérée sur le sac de détonateurs ne correspondait pas à celles de Mayfield.

1. http://america.aljazeera.com/opinions/2014/2/the-terrifying-surveillancecaseofbr
html
2. https://framablog.org/2014/02/12/le-cas-brandon-mayfield/

Scandale Facebook-Cambridge Analytica

Wikipédia, consultée le 28/02/2020[1]

Le scandale Facebook-Cambridge Analytica […] renvoie aux données personnelles de 87 millions d'utilisateurs Facebook que la société Cambridge Analytica (CA) a commencé à recueillir dès 2014. Ces informations ont servi à influencer les intentions de votes en faveur d'hommes politiques qui ont retenu les services de CA. […]

En juillet 2015, l'implication de CA dans les primaires présidentielles du Parti républicain américain de 2016 est dévoilée. En décembre 2015, le journal The Guardian rapporte que l'homme politique américain Ted Cruz a utilisé les données de CA, les personnes visées ignorant que des sociétés exploitaient ces informations. CA aurait participé en 2016 à la campagne électorale de Donald Trump.

En mars 2018, The New York Times, The Guardian et Channel 4 News rapportent plus de détails sur la fuite de données grâce aux révélations de l'ancien salarié de Cambridge Analytica Christopher Wylie, qui a fourni des éclaircissements sur la taille de la fuite, la nature des données personnelles et les échanges entre Facebook, Cambridge Analytica et des personnalités politiques qui avaient retenu les services de CA dans le but d'influencer les intentions de votes. Selon Christopher Wylie : « Sans Cambridge Analytica, il n'y aurait pas eu de Brexit »

1. https://fr.wikipedia.org/wiki/Scandale_Facebook-Cambridge_Analytica

La Chine commence déjà à mettre en place son système de notation des citoyens prévu pour 2020

Elsa Trujillo, le Figaro, 27/12/2017[1].

Lancé en 2014, le projet vise à récompenser les bons comportements et à punir les mauvais via un système de points. La mise en place a déjà commencé : dès le 1er mai 2018, les Chinois ayant une mauvaise « note sociale » se verront interdire l'achat de billets de train ou d'avion pour une période pouvant aller jusqu'à un an, a fait savoir Pékin vendredi dernier.

Des points en plus pour l'achat de produits chinois, de bonnes performances au travail ou la publication sur un réseau social d'un article vantant les mérites de l'économie nationale. Des points en moins en cas d'opinions politiques dissidentes, de recherches en ligne suspectes ou de passages piétons traversés à la hâte, alors que le feu est rouge. La Chine travaille depuis 2014 sur un système d'évaluation de ses propres citoyens programmé pour être mis en place en 2020. L'empire du Milieu vient même d'accélérer le calendrier : dès le 1er mai prochain, les individus ayant une mauvaise « note sociale » seront inscrits sur une liste noire les empêchant d'acheter des billets de train ou d'avion pour une période pouvant aller jusqu'à un an, selon deux communiqués de la Commission nationale de développement de la réforme en date du deux mars et publiés sur internet vendredi dernier.

[…]

D'après [la chercheuse Katika Kühnreich], un tel système fonctionnera en exploitant les mécanismes du jeu, tels que les scores et la comparaison entre amis, pour devenir un insidieux mais très puissant instrument de contrôle social. […] « Le SCS (pour Social Credit System) utilisera de vrais noms, des données de consommateurs, notamment via Alipay, le système de paiement d'Alibaba, ou des applications de rencontres, dont Baihe », précise Katika Kühnreich. Les enregistrements des tribunaux, de la police, des banques, des impôts et des employeurs, seront eux aussi utilisés.

En résultera une note globale, à la manière de l'indice de « désirabilité » attribué par l'application de rencontres Tinder. De cette même note pourra dépendre l'accès des Chinois aux transports publics, à certains services d'État, logements sociaux et formalités de prêts. Katika Kühnreich note que l'accès des plus méritants à certains emplois ainsi que la limitation de l'accès Internet pour les moins performants sont déjà évoqués. Le gouvernement chinois y voit un moyen de mieux contrôler sa population gigantesque en améliorant l'application des règles sur son territoire.

1. https://www.lefigaro.fr/secteur/high-tech/2017/12/27/32001-20171227ARTFIG00197-la-chine-met-en-place-un-systeme-de-notation-de-ses-citoye php

Google chief : Only miscreants worry about net privacy

Cade Metz, The Register, 7/12/2019[1]*, traduit par Louis Paternault.*

Le patron de Google : Seuls les vauriens s'inquiètent de la vie privée sur internet

Si vous êtes inquiets que Google conserve vos données personnelles, alors vous faites sans doute quelque chose que vous ne devriez pas. Du moins, c'est ce que prétend Eric Schmidt, le directeur général de Google.

« Si vous ne voulez pas que qui que se soit soit au courant de quelque chose, peut-être que vous ne devriez tout simplement pas le faire, » a dit Schmidt […].

Mais la vraie nouvelle est peut-être que Schmidt a en fait reconnu que dans certains cas, le géant de la recherche est obligé de fournir vos données personnelles.

« Si vous avez vraiment besoin de ce genre de vie privée, soyez conscients que les moteurs de recherche — dont Google — conservent les informations un certain temps et qu'il est à noter, par exemple, que nous sommes tous soumis aux États-Unis au Patriot Act et qu'il est donc possible que toutes ces informations soient mises à la disposition des autorités. »

Il y a aussi la possibilité des citations à comparaîtres [des requêtes d'un juge]. Et les piratages informatiques. Mais si ce genre de choses vous dérangent, vous devriez avoir honte de vous, selon Eric Schmidt.

1. https://www.theregister.co.uk/2009/12/07/schmidt_on_privacy

Lettre ouverte à ceux qui n'ont rien à cacher

Jean-Marc Manach, Internetactu.net, 21/05/2010[1].

Il existe de très nombreuses façons d'attenter à la vie privée de quelqu'un, et que même ceux qui n'ont « rien à cacher » peuvent en faire les frais.

Les milliers de Français nés à l'étranger qui, l'an passé, ont connu les pires difficultés pour renouveler leurs papiers, parce que suspectés de fraudes aux titres d'identité par des fonctionnaires tatillons ou suspicieux, devant leur rapporter moult papiers et preuves de filiation et de nationalité, n'avaient rien à cacher.

Ce SDF qui s'est vu refuser le renouvèlement de son RSA, au motif qu'il était trop propre, tout comme cette mère de famille qui a connu pareille mésaventure parce qu'on la soupçonnait de ne plus être célibataire, et qui dut faire le tour de ses voisins pour leur demander de témoigner qu'aucun homme ne vivait chez elle (la contrôleuse de la CAF vint fouiller ses tiroirs en lui demandant à qui appartenait les petites culottes), n'avaient eux non plus rien à se reprocher.

Branly Nsingi, un Congolais de 21 ans résidant en France, parti en vacances en Côte d'Ivoire et qui y est décédé d'une crise cardiaque après que les autorités lui aient refusé de rentrer à Paris parce que son passeport n'était pas biométrique (le même avait pourtant été validé au départ), ou encore ces 32 Marocains placés en rétention, et expulsés, alors qu'ils… rentraient tranquillement chez eux, n'avaient rien fait de mal, ce qui ne les a pas empêchés d'être pris dans la nasse de cette société de surveillance et de son usine à gaz sécuritaire qui renversent la charge de la preuve.

Dans le meilleur des mondes, policiers et gendarmes ne feraient jamais de fautes de frappe au moment de saisir le nom d'un suspect, et de ce dont il a été suspecté, dans leurs fichiers de suspects. Dans les faits, nombreuses sont les victimes qui sont fichées comme suspectes, sans parler des problèmes d'homonymie, d'absences de mises à jour des fichiers, de détournements de ces fichiers… En 2008, la CNIL a ainsi recensé 83 % d'erreurs dans les fichiers policiers qu'elle a été amenés à contrôler.

Dans le meilleur des mondes, ceux qui sont payés pour regarder, toute la journée, les écrans de contrôle des caméras de vidéosurveillance, ne feraient jamais de délit de faciès, et ne se permettraient jamais de zoomer sur les décollettés de ces dames. Dans les faits, « 15 % du temps passé par les opérateurs devant leurs écrans de contrôle relèverait du voyeurisme, 68 % des noirs qui sont surveillés le sont sans raison spéciale, tout comme 86 % des jeunes de moins de 30 ans, et 93 % des hommes ».

1. http://www.internetactu.net/2010/05/21/lettre-ouverte-a-ceux-qui-nont-rien-a-ca

Google : Règles de confidentialité et conditions d'utilisation

Google, consulté le 28 février 2020[1].

Comment Google traite les demandes gouvernementales d'informations sur les utilisateurs

Des autorités administratives du monde entier demandent à Google de divulguer des informations sur les utilisateurs. Nous examinons chaque demande attentivement afin de vérifier sa conformité avec les lois applicables. Si la demande porte sur une trop grande quantité de données, nous essayons de l'affiner. Dans certains cas, nous pouvons refuser de divulguer la moindre information. Pour en savoir plus sur le nombre et le type de demandes reçues, consultez notre site Transparence des informations.

Brice Hortefeux — Déclaration sur le site du ministère de l'intérieur

Brice Hortefeux (alors ministre de l'intérieur), septembre 2009, sur le site du ministère de l'intérieur. Cité par Jean-Marc Manach, Hortefeux fustige la vidéosurveillance dont il a fait l'objet[2].

Je suis naturellement attaché à la préservation des libertés individuelles. Je le dis clairement, et chacun peut le voir, la vidéo, c'est de la protection avant d'être de la surveillance. Les caméras ne sont pas intrusives, elles ne sont pas là pour épier, mais pour protéger.

Vous le savez, les caméras de protection font déjà partie de notre quotidien : lorsque vous faites vos courses au supermarché, lorsque vous retirez de l'argent au guichet de votre banque ou que vous utilisez les transports en commun, vous êtes filmés, vous le savez déjà. Qui cela dérange t-il ?

Si vous n'avez rien à vous reprocher, vous n'avez pas à avoir peur d'être filmés ! Instaurer la vidéo-protection, c'est identifier les fauteurs de troubles, c'est décourager les délinquants ; c'est, surtout, veiller sur les honnêtes gens.

1. https://policies.google.com/terms/information-requests?gl=FR&hl=fr
2. https://www.lemonde.fr/blog/bugbrother/2009/09/15/hortefeux-fustige-la-videosurv

Matin brun

Franck Pavloff, édition Cheyne, 2008. Dans ce roman, le lecteur suit deux amis (le narrateur et Charlie) dans un pays où le gouvernement a interdit tous les chats sauf les bruns. Puis tous les chiens sauf les bruns. Puis la liste des choses interdites (sauf les brunes) s'allonge.

Quelque temps après, c'est moi qui avais appris à Charlie que le Quotidien de la ville ne paraîtrait plus. Il en était resté sur le cul : le journal qu'il ouvrait tous les matins en prenant son café crème ! […]

— Pas un jour sans s'attaquer à cette mesure nationale. Ils allaient jusqu'à remettre en cause les résultats des scientifiques.

— À trop jouer avec le feu…

— Comme tu dis, le journal a fini par se faire interdire.

[…] Après ça avait été au tour des livres de la bibliothèque, une histoire pas très claire, encore. Les maisons d'édition qui faisaient partie du même groupe financier que le Quotidien de la ville, étaient poursuivies en justice et leurs livres interdits de séjour sur les rayons des bibliothèques.

[…]

J'allais chez Charlie. […] Et là, surprise totale : la porte de son appart avait volé en éclats, et deux miliciens plantés sur le palier faisaient circuler les curieux. J'ai fait semblant d'aller dans les étages du dessus et je suis redescendu par l'ascenseur. En bas, les gens parlaient à mi-voix.

— Pourtant son chien était un vrai brun, on l'a bien vu, nous !

— Oui, mais à ce qu'ils disent, c'est que avant, il en avait un noir, pas un brun. Un noir.

— Avant ?

— Oui, avant. Le délit maintenant, c'est aussi d'en avoir eu un qui n'aurait pas été brun. Et ça, c'est pas difficile à savoir, il suffit de demander au voisin.

J'ai pressé le pas. Une coulée de sueur trempait ma chemise. Si en avoir eu un avant était un délit, j'étais bon pour la milice. Tout le monde dans mon immeuble savait qu'avant j'avais eu un chat noir et blanc. Avant ! Ça alors, je n'y aurais jamais pensé ! Ce matin, Radio brune a confirmé la nouvelle. […] « Avoir eu un chien ou un chat non conforme, à quelque époque que ce soit, est un délit. » Le speaker a même ajouté « Injure à l'État national »

Et j'ai bien noté la suite. Même si on n'a pas eu personnellement un chien ou un chat non conforme, mais que quelqu'un de sa famille, un père, un frère, une cousine par exemple, en a possédé un, ne serait ce qu'une fois dans sa vie, on risque soi-même de graves ennuis.

Je ne sais pas où ils ont amené Charlie. Là, ils exagèrent. C'est de la folie. Et moi qui me croyais tranquille pour un bout de temps avec mon chat brun.

Ligue 1 : La reconnaissance faciale arrivera-t-elle demain dans les stades de foot ?

Nicolas Camus, 20 minutes, 24/01/2020[1].

Le club [FC Metz] réfléchit au moyen de contrôler [à l'entrée du stade] les personnes sous le coup d'une interdiction commerciale de stade. [Ces interdictions] peuvent être décidées par un club, de manière unilatérale, au motif de « non-respect des dispositions des conditions générales de vente ou du règlement intérieur du stade relatives à la sécurité des manifestations ».

Mais la personne sanctionnée ne va pas pointer au commissariat, comme pour les deux autres interdictions. C'est au club de la repérer si elle essaie d'entrer. « C'est impossible pour nos stadiers, qui voient défiler des milliers de personnes, reprend Hélène Schrub. Donc on cherche comment faire appliquer ces interdictions. Quand Two-I (la start-up en question, spécialisée dans l'analyse de flux vidéo) est venue nous présenter cette solution, on s'est dit pourquoi pas »

Concrètement, des caméras filmeraient les entrées et seraient reliées à un fichier contenant les photos des personnes concernées. Et « uniquement » elles, insiste la dirigeante. « En aucun cas nous aurons un fichier avec tous nos abonnés, tous nos clients ou pire encore, toutes les personnes qui entrent un jour au stade. Ça, c'est vraiment de la science-fiction, affirme-t-elle. Je comprends la peur et l'angoisse de certaines personnes, qui peuvent se dire que le club saura le détail de leurs déplacements dans le stade. Mais pas du tout. La base de données du logiciel ne sera alimentée que par des gens interdits de stade ».

1. `https://www.20minutes.fr/sport/2702191-20200124-ligue-1-reconnaissance-faciale-`

My reaction to Eric Schmidt

Bruce Schneier, 9/12/2009[1]*,* traduit par Tristan Nicot*, Dérapage d'Eric Schmidt, de Google, 11/12/2009*[2]*.*

La notion de vie privée nous protège de ceux qui ont le pouvoir, même si nous ne faisons rien de mal au moment où nous sommes surveillés. Nous ne faisons rien de mal quand nous faisons l'amour ou allons aux toilettes. Nous ne cachons riens délibérément quand nous cherchons des endroits tranquilles pour réfléchir ou discuter. Nous tenons des journaux intimes, chantons seuls sous la douche, écrivons des lettres à des amoureux secrets pour ensuite les brûler. La vie privée est un besoin humain de base.

[…] Si nous sommes observés en toute occasion, nous sommes en permanence menacés de correction, de jugement, de critique, y compris même le plagiat de nous-même. Nous devenons des enfants, emprisonnés par les yeux qui nous surveillent, craignant en permanence que — maintenant ou plus tard — les traces que nous laissons nous rattraperont, par la faute d'une autorité quelle qu'elle soit qui porte maintenant son attention sur des actes qui étaient à l'époque innocents et privés. Nous perdons notre individualité, parce que tout ce que nous faisons est observable et enregistrable. […]

Voici la perte de liberté que nous risquons quand notre vie privée nous est retirée. C'est la vie dans l'ex-Allemagne de l'Est ou dans l'Irak de Saddam Hussein. Mais c'est aussi notre futur si nous autorisons l'intrusion de ces yeux insistants dans nos vies personnelles et privées.

Trop souvent on voit surgir le débat dans le sens "sécurité contre vie privée". Le choix est en fait liberté contre contrôle. La tyrannie, qu'elle provienne de la menace physique d'une entité extérieure ou de la surveillance constante de l'autorité locale, est toujours la tyrannie. La liberté, c'est la sécurité sans l'intrusion, la sécurité avec en plus la vie privée. La surveillance omniprésente par la police est la définition même d'un état policier. Et c'est pour cela qu'il faut soutenir le respect de la vie privée même quand on n'a rien à cacher.

1. https://www.schneier.com/blog/archives/2009/12/my_reaction_to.html
2. http://standblog.org/blog/post/2009/12/11/Dérapage-d-Eric-Schmidt-de-Google

Données persos : Européens, lisez bien la petite histoire de ce père américain

Xavier de la Porte, L'Obs, 18/11/2016[1]*.*

[Je] vais vous raconter une histoire. Elle s'est déroulée il y a deux ans aux Etats-Unis, dans la banlieue de Minneapolis. Un homme en colère demande à voir le directeur de sa grande surface habituelle, un Target (une chaîne de grands magasins qui, vous allez voir porte merveilleusement son nom). Il est très énervé parce sa fille, qui a 16 ans, qui est encore au lycée, reçoit des publicités provenant de Target lui vantant des habits de bébé et des couches. « Vous voulez la pousser à tomber enceinte ? » demande-t-il au directeur, qui ne sait pas bien quoi répondre, et qui est gêné au point que deux jours plus tard, il appelle l'homme pour s'excuser à nouveau.

Sauf que cette fois-ci, c'est l'homme qui s'excuse : « J'ai parlé avec ma fille. Il se passait chez moi des choses dont je n'étais pas au courant, elle est enceinte. C'est pour août. »

Tout cela a donné lieu à une vaste enquête sur les méthodes de la chaîne Target. Où on s'est aperçu que la chaîne avait un système de publicité ultraciblée, le document papier envoyé au domicile pouvant être personnalisé quasiment à l'unité. Où on s'est aperçu que cette publicité ultraciblée était le fruit d'un travail très précis et très savant de récolte de données et de travail de données, un travail dû à un jeune statisticien du nom de Andrew Pole.

Le principe est simple : en faisant vos courses, vous donnez un nombre incalculable d'informations sur vous-mêmes, en prenant une carte de fidélité vous permettez qu'elles soient associées à un nom, à une adresse. Et le tour est joué. Ensuite, il suffit de faire un gros travail statistique, de construire les algorithmes qui font le lien entre des habitudes d'achat, l'évolution dans ces habitudes et des changements dans la vie (le fait d'avoir un gigantesque corpus permet de faire des liens de corrélation très fins, entre par exemple le changement de type de savon acheté et la grossesse, le fait de ne plus acheter tel type d'aliment et une maladie, etc.). Ainsi, le magasin sait du client ce que ses proches peuvent ignorer.

1. https://www.nouvelobs.com/rue89/rue89-monde/20140311.RUE2598/donnees-persos-europeens-lisez-bien-la-petite-histoire-de-ce-pere-americain.html

Non, je n'ai rien à cacher

Ploum, 21 novembre 2012[1].

Adolescent dans une grande école catholique, je me fais un jour approcher par un condisciple. — Lio, il faut que je montre un truc trop drôle !

Ce camarade me révèle qu'il a trouvé, dans une revue porno, une photo ressemblant fortement à un de nos éducateurs. Intrigué, je demande bien sûr à voir la photo en question. Publiée dans la rubrique « courrier des lecteurs », elle représente un homme nu en érection. Contrairement aux autres photos de cette rubrique, le visage n'est pas flouté. Et la ressemblance est, il est vrai, frappante.

Éclatant de rire, nous avons vite fait de nous adjoindre une petite troupe goguenarde autour de la photo. Je remarque alors une chevalière très particulière et un pendentif en or au cou de notre exhibitionniste.

Ni une ni deux, la petite troupe décide de passer « discrètement » devant le bureau des éducateurs pour vérifier et, stupeur, notre éducateur porte la même chevalière, le même pendentif. Il n'y a donc plus aucun doute.

[…]

De mon côté, intrépide et inconscient, je lui demande de me découper la photo et la fait passer sous le manteau dans l'école. C'est rigolo. Les élèves jasent.

Le lendemain, l'éducateur n'est pas là. Il ne reviendra jamais.

Cet éducateur avait-il quelque chose à se reprocher ? Non, il échangeait une photo où il apparaissait nu avec un public majeur consentant et demandeur. C'était tout à fait légal et on ne peut lui reprocher cela.

Par contre, le magazine est arrivé dans les mains d'un lecteur non-majeur. La personne ayant permis cela est donc coupable car la photo, bien que parfaitement légale, mine l'autorité de l'éducateur. De plus, elle va à l'encontre des valeurs morales affichées par l'employeur. Deux raisons qui font qu'il était impossible de garder l'éducateur en poste.

Il est donc important de souligner un point : le problème n'est pas que l'éducateur aie posé pour des photos pornographiques ni même qu'elles aient été publiées mais bien que les élèves subordonnés à l'éducateur en prirent connaissance. Ce n'est pas le fait ni l'information qui pose problème mais bien que certaines personnes particulières aient accès à cette information.

La phrase « Celui qui n'a rien à se reprocher n'a rien à cacher » est donc fausse car ce n'est pas vous qui choisissez ce que vous vous reprochez. C'est le public qui a tout pouvoir pour décider ce qu'il va décider de vous reprocher. Afin d'illustrer la nécessité de la vie privée, on prend souvent l'exemple du régime totalitaire qui contrôle les citoyens. […]

1. https://ploum.net/rien-a-cacher/

From grainy CCTV to a positive ID : Recognising the benefits of surveillance

Rob Hastings, The Independant, 01/01/2013[1]*, traduit par Louis Paternault.*

Le professeur Mark nikon « a eu quelques échanges tendus » à l'époque avec les groupes de protection des libertés publiques. Expert mondial dans la reconnaissance des personnes par vidéosurveillance en utilisant la biométrie — la bête noire de tous les militants anti-surveillance — il sait très bien ce qu'ils pensent de son travail.

« Ils disent que nous violons leur vie privée », dit-il. « Je ne pense pas que leur liberté soit en danger. » Les techniques qu'il a inventées « ont été utilisées pour attraper des meurtrier — et ça me convient très bien ».

Grâce au travail du professeur Nixon et du docteur John Carter à l'université de Southampton, il est devenu extrèmement facile pour les autorité de tous nous surveiller. Des recherches à la *School of Electronics and Computer Science* (école d'électronique et d'informatique) — financées entre autres par le Pentagone et le ministère de la défense — permettent de trouver et d'identifier de plus en plus précisément des criminels dans des images de vidéosurveillance.

[…]

Cela a permis de résoudre plusieurs crimes en Grande-Bretagne, et a aidé à arrêté l'assasin de l'ancienne ministre Anna Lindh en Suède en 2003.

Le potentiel de tels systèmes de surveillance est énorme. Mais les risques d'atteinte à la vie privée aussi, préviennent les militants.

[…]

Mais le professeur Nixon n'est pas d'accord. « Les inquiétudes par rapport à la vie privée sont très vieilles. Si vous vous intéressez à l'histoire des cartes, vous verrez que les gens ne voulaient pas que des salauds insolents cartographient leurs terres. Les gens ont toujours été méfiants de ce qu'ils ne connaissent pas, mais la plupart diraient que cela ne les dérangerait pas que la police sache plein de choses sur eux si cela permettait d'éliminer des menaces sérieuses. […] »

La demande [en loi encadrant la vidéosurveillance] va probablement ne faire qu'augmenter. Bientôt, l'intelligence artificielle sera capable d'alerter automatiquement les personnels de sécurité sur des comportement suspects avant même que la personne ait fait quoi que ce soit d'illégal.

1. https://www.independent.co.uk/news/uk/home-news/from-grainy-cctv-to-a-positive-html

Victimes du Stic

François Koch, L'Express, 19/01/2009[1].

Tous les cinq ont souffert du Stic, le fichier des "infractions constatées", dont l'utilisation est dénoncée par la Commission nationale informatique et libertés. Témoignages.

[…]

Pierre-Alexis : "Empêché de devenir gendarme"

"Le 13 novembre 2003, je vois ma petite amie frappée par son père, alors que je venais la chercher. Il se jette sur moi. Je réplique. Je porte plainte, car ma voiture est cabossée. Le lieutenant de police chargé de l'enquête, à Vernon (Eure), affirme que j'ai moi-même abîmé ma voiture ! La justice classe l'affaire sans suite. Je rêvais d'entrer dans la gendarmerie. Je réussis alors le concours. Mais quatre jours avant de l'intégrer, à Rouen (Seine-Maritime), une employée me dit que tout est annulé en raison de 'problèmes administratifs'. Je la supplie de m'en dire plus. Elle me précise, sous le sceau du secret, que mon nom est référencé dans le Stic [comme auteur de dénonciation calomnieuse]. Je suis en dépression depuis plusieurs années et toujours au chômage."

Catherine : "Bloquée pour la magistrature"

"Avocate depuis douze années, je pose ma candidature pour devenir magistrate. Je suis alors reçue par un agent de police judiciaire, chargé d'enquêter sur moi : "Avez vous eu des contacts avec la police ?" me demande-t-il. […] "Au milieu des années 1990, j'ai été entendu par un policier de la Brigade financière, pour expliquer le concours du cabinet d'avocats, où je travaillais, au montage d'une opération immobilière." "La mémoire vous revient !", indique le policier refusant toute autre précision. Après avoir reçu une réponse négative à ma candidature à la magistrature, j'écris à la Cnil pour savoir si je suis fichée au Stic. Alors que rien ne m'a jamais été reproché, je découvre avec effroi que je suis inscrite comme "mise en cause pour escroquerie". […]"

1. https://www.lexpress.fr/actualite/societe/victimes-du-stic_732755.html

Rien à cacher (argument)

Wikipédia, page consultée le 28/02/2020[1].

Mauvais usage des données collectées

Le professeur de droit Daniel J. Solove a exprimé son opposition au « rien à cacher » : il affirme qu'un gouvernement, et par extension toute organisation collectant des données, peut diffuser sur une personne des informations susceptibles de lui nuire, ou bien utiliser des informations la concernant pour lui refuser l'accès à certains services, même si cette personne n'a commis en pratique aucune mauvaise action. […] Il n'est pas exclu en effet que des données soient diffusées par mégarde, ou bien que quelqu'un obtienne un accès frauduleux à leur support de stockage.

Mais plus généralement encore se pose la question de la réutilisation des données. Lorsque celles-ci ne sont pas collectées de façon transparente, est-il possible de s'assurer qu'il n'y aura pas de dérives ?

[…]

Un autre argument important, et qui découle du précédent, est la persistance des données collectées dans le temps : rien ne garantit que leur usage sera toujours le même que celui qui aura été annoncé initialement. Par exemple, le cas des Juifs d'Allemagne, qui sont allés se déclarer en 1936, avant que l'ampleur du projet de leur répression ne soit dévoilée. Rien ne garantit qu'un comportement toléré aujourd'hui le soit toujours dans le futur.

Enfin, les données personnelles peuvent également être utilisées et analysées par des sociétés privées pour adapter leur offre en fonction du profil qu'ils auront dressé. C'est d'ailleurs ce que met en avant l'analyste Klara Weiand dans le documentaire Nothing to Hide :

« Une assurance pourrait devenir plus chère pour vous, le prix de marchandises pourrait également varier en fonction de votre revenu estimé et de votre propension à acheter ces produits ».

1. https://fr.wikipedia.org/wiki/Rien_à_cacher_(argument)

On a tous des choses à cacher

Maurits Martijn et Rob Winjnberg, publié le 21 octobre 2013 dans Correspondent, traduit par Courrier International dans le nº 1285 du 18 au 24 juin 2015.

2. Les relations sociales nécessitent que l'on cache certaines choses

Chaque être humain montre une personnalité différente en fonction du contexte, du moment, et des personnes qui l'entourent. […] Dans un contexte social, tout le monde a des choses à cacher. Au travail, il peut s'agir du caractère colérique qui ressort parfois en présence de son conjoint, qui n'a par contre jamais vu le masque de séducteur que l'on revêt devant des inconnus.

3. On cache déjà des choses sans s'en rendre compte

Cacher des choses est devenu tellement naturel qu'on le fait sans réfléchir. Nous cachons notre corps, nos défauts, nos courriels, notre fiche de paie, etc. […]

4. L'interdit dépend du contexte

Dans notre pays [les Pays-Bas] l'adultère n'est pas interdit par la loi, mais en Arabie Saoudite il est passible de la peine de mort. La question de savoir si quelque chose est interdit (et s'il vaut mieux le cacher) dépend donc du contexte. […] Et, quant à votre homosexualité, qui n'intéresse personne [aux Pays-Bas], elle peut vous causer des ennuis devant la douane russe. Bref, on ne peut jamais être sûr de ne pas enfreindre un "interdit".

5. Les interdits évoluent

Dans les années 1970, des voix s'élevaient publiquement pour demander le droit d'avoir des relations sexuelles avec des enfants. Aujourd'hui, ces mêmes personnes seraient inculpées. On peut donc penser ne rien faire d'"interdit" (et donc ne rien avoir à cacher) alors que nos actions pourraient nous causer de gros ennuis ultérieurement.

7. Des faits et gestes mal interprétés

Imaginons que vous êtes journaliste et que vous voulez écrire un article sur les jeunes Néerlandais qui vont faire le djihad en Syrie. Après de nombreuses recherches sur Internet, vous avez trouvé plusieurs numéros de téléphone et adresses mél pour faire des interviews. Un fois l'article terminé, vous voulez aller en vacances à New York et ne prenez qu'un aller simple parce que vous ne savez pas combien de temps vous voudrez y rester. Avant de partir, vous réalisez que vous et votre petite amie venez d'acheter ensemble votre première maison et qu'elle se retrouverait avec des mensualités trop lourdes s'il vous arrivait quelque chose. Vous prenez donc une assurance-vie juste avant votre départ. Vous avez donc les numéros de plusieurs djihadistes dans votre téléphone, vous avez acheté un aller simple pour New York et vous venez de contracter une assurance-vie. La NSA ne risque-t-elle pas de trouver votre voyage suspect ? Qu'est-ce qui garantit que ses algorithmes de recherche ou les personnes qui les interprètent ne tireront pas de mauvaises conclusions vous concernant ?

9. On ne peut pas faire confiance aux pouvoirs publics

Plusieurs fois déjà, les pouvoirs publics néerlandais se sont révélés incapables de bien protéger les données personnelles des citoyens. Quasiment tous les grands projets informatiques de ces dernières années (comme le dossier médical électronique, le vote en ligne ou la carte de transports publics) avaient des failles techniques mettant en danger la sécurité des données. Certes, nous n'avons probablement rien à cacher à l'organisme auquel nous donnes nos informations personnelles, mais cela pose un problème dès lors que d'autres parties ont potentiellement accès à ces données.

10. Les pouvoirs publics font des erreurs

Les exemples ne manquent pas. Prenons l'homme d'affaires néerlandais Ron Kowsoleea. Il a été victime de données mal enregistrées dans les bases de données de différents services de recherche néerlandais pendant plus de quinze ans. Kowsoleea a été arrêté et inculpé plusieurs fois parce que quelqu'un d'autre commettait des délits sous son nom et que les pouvoirs publics néerlandais n'étaient pas capables de corriger les erreurs. Autre exemple : des centaines de travailleurs indépendants ont atterri sur une liste de fraudeurs aux allocations à cause d'un problème informatique. Ils ont été condamnés et ont dû payer de fortes amendes.

11. Quid de nos futurs dirigeants ?

Si certaines données ont déjà été collectées pour une raison x, pourquoi ne pas les utiliser pour une raison y ? Les spécialistes appellent cela le détournement d'usage. Prenons par exemples les empreintes digitales enregistrées sur les passeports de l'Union européenne. À la base, cette mesure de Bruxelles avait pour but de prévenir l'usurpation d'identité, mais aujourd'hui les empreintes digitales sont également utilisées pour des enquêtes judiciaires. Certes, aujourd'hui, les autorités néerlandaises ne s'y intéressent pas, mas il est naïf de croire qu'il pourrait en être autrement dans l'avenir. Nous ne savons pas encore qui seront les futurs dirigeants et quels seront leurs agendas politiques.

Marc L***

Raphaël Meltz, Le Tigre nº 28, novembre-décembre 2008[1].

Bon annniversaire, Marc. Le 5 décembre 2008, tu fêteras tes vingt-neuf ans. Tu permets qu'on se tutoie, Marc ? Tu ne me connais pas, c'est vrai. Mais moi, je te connais très bien. C'est sur toi qu'est tombée la (mal)chance d'être le premier portrait Google du Tigre. Une rubrique toute simple : on prend un anonyme et on raconte sa vie grâce à toutes les traces qu'il a laissées, volontairement ou non sur Internet.

[…]

Alors, Marc. Belle gueule, les cheveux mi-longs, le visage fin et de grands yeux curieux. Je parle de la photo prise au Starbuck's Café de Montréal, lors de ton voyage au Canada, avec Helena et Jose, le 5 août 2008. La soirée avait l'air sympa, comme d'ailleurs tout le week-end que vous avez passé à Vancouver. J'aime particulièrement cette série, parce que Jose a fait des photos, et ça me permet de te voir plus souvent. Vous avez loué un scooter, vous êtes allés au bord de la mer, mais vous ne vous êtes pas baignés, juste traîné sur la plage. En tout, tu as passé un mois au Canada. Au début tu étais seul, à l'hôtel Central, à Montréal (série de photos « autour de mon hôtel »). Tu étais là-bas pour le travail. Le travail ? Tu es assistant au « service d'architecture intérieur », dans un gros cabinet d'architectes, LBA, depuis septembre dernier (Facebook, rubrique Profil). Le cabinet a des succursales dans plusieurs villes, et a priori tu dois travailler dans la succursale de Pessac, dans la banlieue de Bordeaux. Ça, je l'ai trouvé par déduction, vu que tu traînes souvent à l'Utopia (cinéma et café bordelais) ou à Arcachon. Donc à Montréal, tu étais dans un bureau avec Steven, Philipp, Peter, en train de travailler sur des plans d'architectes, devant deux ordinateurs, un fixe et un portable. […] Le 21 août, c'est Steven qui t'a accompagné à l'aéroport. Retour en France, où t'attendait un mariage (Juliette et Dominique), puis, la semaine suivante, le baptême de ta nièce, Lola, la petite sœur de Luc (qui fait des têtes rigolotes avec ses grosses lunettes), à Libourne.

Revenons à toi. Tu es célibataire et hétérosexuel (Facebook). Au printemps 2008, tu as eu une histoire avec Claudia R***, qui travaille au Centre culturel franco-autrichien de Bordeaux (je ne l'ai pas retrouvée tout de suite, à cause du caractère ü qu'il faut écrire ue pour Google). En tout cas, je confirme, elle est charmante, petits seins, cheveux courts, jolies jambes. Tu nous donnes l'adresse de ses parents, boulevard V*** à Bordeaux. Vous avez joué aux boules à Arcachon, et il y avait aussi Lukas T***, qui est le collègue de Claudia au Centre Culturel. Fin mai, il n'y a que quatre photos, anodines, de ton passage dans le petit appartement de Claudia (comme si tu voulais nous cacher quelque chose) et une autre, quelques jours plus tard, plus révélatrice, prise par Claudia elle-même, chez elle : on reconnaît son lit, et c'est toi qui es couché dessus. Habillé, tout de même. Sur une autre, tu te brosses les dents. C'est le 31 mai : deux jours plus tôt, vous étiez chez Lukas « pour fêter les sous de la CAF » (une fête assez sage, mais Lukas s'est mis au piano pour chanter des chansons en allemand, tout le monde a bien ri, vidéo sur Flickr). Ce 31 mai, vous avez une façon de vous enlacer qui ne laisse que peu de doutes. Et le 22 juin, cette fois c'est sûr, vous vous tenez par la main lors d'une petite promenade au Cap-Ferret. C'est la dernière fois que j'ai eu des nouvelles de Claudia. Note bien que j'ai son numéro au travail (offre d'emploi pour un poste d'assistant pédagogique au Centre culturel, elle s'occupe du recrutement), je pourrais l'appeler. Mais pour raconter une séparation, même Internet a des limites. Avant Claudia, tu étais avec Jennifer (ça a duré au moins deux ans), qui s'intéressait à l'art contemporain (vous avez visité ensemble Beaubourg puis tu l'as emmenée au concert de Madonna à Bercy). Elle a habité successivement Angers puis Metz, son chat s'appelle Lula, et, physiquement, elle a un peu le même genre que Claudia. À l'été 2006, vous êtes partis dans un camping à Pornic, dans une Golf blanche. La côte Atlantique, puis la Bretagne intérieure. Tu avais les cheveux courts, à l'époque, ça t'allait moins bien.

On n'a pas parlé de musique. À la fin des années 1990, tu as participé au groupe Punk, à l'époque où tu habitais Mérignac (à quelques kilomètres de Bordeaux). Il reste quelques traces de son existence, sur ton Flicker bien sûr mais aussi dans les archives Google de la presse locale. Tu sais quoi ? C'est là que j'ai trouvé ton numéro de portable : 06 83 36 ** **. Je voulais vérifier si tu avais gardé le même numéro depuis 2002. Je t'ai appelé, tu as dit : « Allô ? », j'ai dit : « Marc ? », tu as dit : « C'est qui ? », j'ai raccroché. Voilà : j'ai ton portable. […]

[…]

Je pense à l'année 1998, il y a dix ans, quand tout le monde fantasmait déjà sur la puissance d'Internet. Le Marc L*** de l'époque, je n'aurais sans doute rien ou presque rien trouvé sur lui. Là, Marc, j'ai trouvé tout ce que je voulais sur toi. J'imagine ton quotidien, ta vie de jeune salarié futur architecte d'intérieur, ton plaisir encore à faire de la musique avec tes potes à Bordeaux, tes voyages à l'autre bout du monde, ta future petite copine (je parie qu'elle aura les cheveux courts). Mais il me manque une chose : ton adresse. Dans ces temps dématérialisés, où mails et téléphones portables tiennent lieu de domiciliation, ça me pose un petit problème : comment je fais pour t'envoyer Le Tigre ? Je sais que tu es avenue F***, mais il me manque le numéro, et tu n'es pas dans les pages jaunes. Cela dit, je peux m'en passer. Il suffit que je ne te l'envoie pas, ton portrait : après tout, tu la connais déjà, ta vie.

1. http://le-tigre.net/marc-L.html

Alicem, la première solution d'identité numérique régalienne sécurisée

Ministère de l'intérieur, 16 décembre 2019[1].

Contexte : Alicem est une application pour mobile proposée par le ministère de l'intérieur permettant de s'authentifier par reconnaissance faciale.

Les données personnelles sont-elles conservées et sécurisées ?

— Les données extraites du titre d'identité sont vérifiées lors de l'inscription mais ces dernières ne sont stockées que sur le smartphone de l'utilisateur sous son contrôle exclusif et protégées par un chiffrement.

— Alicem n'a pas accès aux historiques de transactions grâce à la séparation garantie par la plateforme « FranceConnect », qui anonymise les fournisseurs de service auxquelles sont transmises les données.

— Le décret qui réglemente Alicem contient des dispositions très strictes sur la gestion des données.

— Les données ne font l'objet d'aucune utilisation pour d'autres objectifs que l'authentification électronique et l'accès à des services en ligne par Alicem. Elles ne sont pas transmises à des tiers.

Le fiasco de la reconnaissance faciale testée par la police de Londres

Samuel Khan, Le Figaro, 5 mars 2020[2].

Après plusieurs mois de tests, Scotland Yard [la police Britannique] a procédé aux premières opérations de surveillance fondée sur la reconnaissance faciale. Une camionnette équipée de cette technologie qui permet de scanner et de reconnaître un visage à la volée a été installée à la sortie du métro [d'Oxford Circus, à Londres]. […] Des milliers de personnes ont ainsi eu leur visage filmé sans leur consentement. Mais les résultats sont loin d'être à la hauteur des promesses de la Met Police, pour qui ce système doit permettre de « combattre les crimes, la violence et l'exploitation sexuelle des enfants ».

Sur les 8 600 personnes dont le visage a été filmé dans la journée du 27 février, huit ont été reconnues comme faisant partie d'un fichier de personnes recherchées spécifiquement pour des crimes violents. Problème : sept d'entre elles l'ont été à tort, donnant lieu à plusieurs contrôles non justifiés. Soit un taux d'erreur de près de 90 %, bien loin des 70 % de précision promis par la police au début des tests. […]

1. https://www.interieur.gouv.fr/Actualites/L-actu-du-Ministere/Alicem-la-premiere-solution-d-identite-numerique-regalienne-securisee

2. https://www.lefigaro.fr/secteur/high-tech/le-fiasco-de-la-reconnaissance-facial

Projet de loi sur le renseignement : Conférence de presse de Manuel Valls

Le 19/03/2015[1].

Contexte : Dans cette conférence de presse, pour lutter contre le terrorisme (en particulier les attentats djihadistes), le premier ministre Manuel Valls décrit une loi augmentant les capacités des services de renseignement à surveiller les communications électroniques (internet, téléphone) des citoyens français.

Le second objectif est de garantir la protection des libertés publiques. Aucune mesure de surveillance ne pourra être effectuée sans autorisation préalable et sans contrôle indépendant. Cette loi sera aussi protectrice des citoyens car les limites de ce qu'il est possible de faire dans un état de droit seront gravées dans le marbre : il n'y aura plus de zone grise.

[…]

S'agissant des mesures, le projet de loi codifie les différents types de surveillance et détermine les règles précises qui seront applicables à chacune d'elle : interception de sécurité, accès aux données de connexion, géolocalisation en temps réel […], intrusion informatique pour contourner les effets de cryptage, […]. En résumé, plus les techniques touchent la vie privée, plus les contraintes sont fortes et les durées autorisées limitées.

[…]

Mesdames et messieurs, face à l'accroissement de la menace djihadiste, il faut donc renforcer encore l'efficacité de la surveillance des terroristes.

[…]

Certaines inquiétudes, notamment chez les acteurs du numérique, s'expriment à ce sujet. […] Je vais vous le dire de manière très claire : il ne s'agit en aucun cas de mettre en œuvre des moyens d'exception ou une surveillance généralisée des citoyens. Le projet de loi prévoit expressément que cette surveillance renforcée concernera les communications des seuls terroristes. Cela démontre bien qu'il n'y aura aucune surveillance de masse. Le projet de loi l'interdit.

[…]

Pour identifier les moyens de communication des individus qui cherchent en permanence à dissimuler leurs échanges, les possibilités accordées en la matière aux services de renseignement seront limitées, infiniment plus réduites que dans le cas de la police judiciaire. Seule l'identification et l'aide aux surveillances de terrain seront autorisées. Il n'y aura en aucun cas aspiration massive des données personnelles, comme j'ai pu le lire dans certains journaux au cours des derniers jours.

1. https://www.dailymotion.com/video/x2kjre7

Des policiers britanniques détournent les fichiers à des fins personnelles

Florent Bascoul, Le Monde, 06/07/2016[1].

Big Brother Watch, un groupe britannique de défense des libertés publiques contre la surveillance généralisée, vient de publier un rapport pointant le détournement des fichiers électroniques par des policiers à des fins personnelles. Outre-Manche, près de 800 gardiens de la paix ont accédé à des données confidentielles pour leur propre intérêt au cours de ces 5 dernières années.

[...] [Un rapport de Big Brother Watch] donne quelques exemples de l'utilisation détournée de ces fichiers :

- Un officier qui trouvait le nom d'une victime amusant a pris une photo de son permis de conduire pour l'envoyer à un ami sur Snapchat. L'officier a démissionné pendant la procédure disciplinaire qui l'a visé ;
- Un policier a été licencié après avoir photographié et diffusé des données sensibles contre rémunération ;
- Un agent de police a été renvoyé après avoir transmis des informations confidentielles à un membre de sa famille à propos d'un détenu ;
- Un gardien de la paix a jugé bon d'informer un ancien collègue que l'un de ses voisins avait été condamné pour agression sexuelle. Le rapport ne précise pas si le policier a été puni.

L'association déplore l'impunité des auteurs des détournements données sensibles. Selon les chiffres communiqués, seuls 3 % des policiers ont été poursuivis en justice ou condamnés. Dans la plupart des cas, aucune action disciplinaire n'a été engagée.

1. https://www.lemonde.fr/pixels/article/2016/07/06/des-policiers-britanniques-detc
4965049_4408996.html

Politique d'utilisation des données Instagram

Consulté de 28 février 2002[1].

Comment ces informations sont-elles partagées ?

Annonceurs. Nous fournissons aux annonceurs des rapports sur les types de personnes qui voient leurs publicités et sur les performances de leurs publicités, mais nous ne partageons pas d'informations permettant de vous identifier personnellement (des informations telles que votre nom ou votre adresse e-mail qui peuvent être en elles-mêmes utilisées pour vous contacter ou vous identifier), sauf si vous nous en donnez l'autorisation. Par exemple, nous communiquerons aux annonceurs des informations générales concernant la démographie et les centres d'intérêt (par exemple, une publicité a été vue par une femme entre 25 et 34 ans qui vit à Madrid et qui aime l'ingénierie informatique) pour les aider à mieux comprendre leur audience. Nous vérifions également les publicités Facebook qui vous ont incité(e) à effectuer un achat ou à entreprendre une action auprès d'un annonceur.

1. https://help.instagram.com/519522125107875?helpref=page_content

Géolocalisation des militaires : l'armée française réagit

Guerric Poncet, Le Point, 30/01/2018[1].

L'armée française a réagi après la divulgation de la géolocalisation de nombreux militaires par l'application de fitness Strava. Contacté par Le Point.fr, l'état-major des armées (EMA) explique avoir « effectué un rappel en interne sur la nécessité de respecter les règles élémentaires de sécurité des systèmes d'information », dans lequel « il est en particulier rappelé de désactiver les fonctions de géolocalisation et de GPS ».

[…]

Les Californiens de Strava, une appli pour smartphone qui permet de suivre des activités physiques comme le vélo ou le jogging, publient régulièrement une carte (« heat map ») très détaillée des parcours de ses utilisateurs. La dernière version date de 2017 et affiche plus d'un milliard d'activités dans le monde entier. Même si les données sont anonymisées, la précision des tracés GPS permet de distinguer très clairement les bases militaires, en particulier les installations américaines, britanniques ou françaises sur leur territoire national, mais surtout à l'étranger, là où elles essaient de rester discrètes. Pour la France, par exemple, les bases de l'opération Barkhane (N'Djamena, Madama, Abéché, Faya-Largeau, Niamey, etc.) ou encore la base aérienne projetée de Jordanie apparaissent sur la carte de Strava.

En Afghanistan, en Syrie, au Tchad, au Niger ou encore au Mali, n'importe quel internaute peut voir les trajets habituels des militaires pour leurs footings, leurs patrouilles ou leurs rondes. De quoi monter une embuscade parfaite, ou identifier des bases discrètes, voire secrètes.

[…]

« La divulgation de données personnelles par le site Strava nous rappelle que les objets connectés (montres, téléphones, tablettes, etc.) peuvent également se révéler de véritables espions », nous précise d'ailleurs l'état-major des armées, qui estime que « les armées françaises ont pleinement conscience que les nouvelles technologies et l'utilisation des réseaux sociaux peuvent mettre en péril la sécurité des opérations ». « C'est pourquoi des consignes sont régulièrement passées à nos militaires », assure encore l'EMA.

1. https://www.lepoint.fr/high-tech-internet/geolocalisation-des-militaires-l-armee
47.php

Steps to Protect Your Online Identity from the Taliban : Digital History and Evading Biometrics Abuses

Human Rights First, 17/08/2021[2]*, traduit par Louis Paternault.*

Contexte : En 2021, l'armée américaine se retire d'Afghanistan, qu'elle occupait depuis vingt ans. Très vite, les talibans (fondamentalistes islamiques) reprennent le pouvoir dans le pays grâce à une offensive militaire. L'organisation humanitaire Human Rights First *publie alors un guide (dont des extraits sont reproduits ici) à destination des afghans pour protéger ses données du nouveau pouvoir.*

FAQ : Protection contre les méthodes d'identification numériques des talibans

À quelles données et technologies biométriques les talibans ont-ils accès ?

[…] Nous pensons qu'ils ont — ou auront bientôt — accès à plusieurs bases de données d'informations biométriques, ainsi qu'aux équipements permettant [de les utiliser]. Avant les élections de 2019, une collecte des données biométriques des électeurs de tous le pays a eu lieu à grande échelle. Nous pensons également que les forces militaires étrangères ont enregistré de grandes quantité de données biométriques qui ont été abandonnées sur place. Nous ne sommes pas certains que les talibans puissent accéder à ces bases de données. Néanmoins, nous n'avons aucune raison de penser que ces bases de données ont été détruites.

À quelles données biométriques les talibans ont-ils accès ?

Des enregistrements de visages, iris et empreintes digitales sont présentes dans les bases de données en question.

Quelles autres données et informations peuvent être utilisées contre des personnes dans cette crise ?

Les données des technologies publicitaires (y compris la géolocalisation), toutes les données collectées par les ministères afghans qui sont maintenant contrôlés par les talibans, etc.

2. https://humanrightsfirst.org/library/steps-to-protect-your-online-identity-from