Surveillance

1. Le « crédit social » ou le Big Brother à la sauce chinoise

Source
The Conversation
François Lafargue
20 juin 2018

Depuis plusieurs mois, la presse européenne dénonce le projet de surveillance de la population, le *Plan de planification pour la construction d'un système de crédit social (2014-2020)* que le gouvernement de la Chine populaire met progressivement en place. Parfois de manière ironique, mais souvent sans grand discernement. L'ambition est d'attribuer à partir de 2020, à certaines catégories de citoyens chinois comme aux entreprises, une note de confiance, un « crédit social ». Le chercheur néerlandais Rogier Creemers propose ici une traduction du document de présentation du Conseil des affaires de l'État (l'équivalent du gouvernement en Chine).

Ce projet est officiellement motivé par la volonté de restaurer la confiance dans la vie économique et, plus particulièrement, entre les entreprises et les consommateurs. L'évaluation publique doit permettre une amélioration des comportements. Une nécessité dans un pays où les scandales de corruption sont fréquents, avec parfois des conséquences tragiques comme en 2008 avec la contamination de près de 100 000 enfants (dont plusieurs décédèrent) par du lait contenant de la mélamine (destinée à augmenter sa teneur en protéine).

Des millions de caméras de surveillance

Le site officiel du crédit social affiche déjà les noms et numéros d'identification de personnes interdites de prendre le train ou l'avion. Plusieurs listes d'entreprises accusées de violer la loi pour des motifs divers et donc « indignes de confiance » sont régulièrement publiées.

Mais, à l'heure actuelle, le système reste expérimental et limité à une douzaine de villes comme Shanghai, Nankin, Xiamen et Yiwu. Les barèmes ne sont pas homogènes pour le moment, mais le manque de civisme – comme traverser en dehors des passages piétons ou ne pas respecter les interdictions de fumer – est sanctionné. Les écarts de comportement sont verbalisés grâce aux millions de caméras de surveillance installées dans le pays (près d'une pour deux habitants en 2020).

L'application *Honest Shanghai*, proposée par la municipalité de Shanghai, permet à partir de plusieurs critères d'attribuer une note de comportement social entre « excellent », « bon » ou « médiocre », et de rassurer un employeur ou un créancier potentiel ou encore sa future belle-famille. Toutefois, l'application qui collecte des informations auprès d'une centaine d'agences gouvernementales renseigne également sur la confiance que l'on peut accorder aux commerçants ou le niveau d'hygiène des restaurants. Chacun reste libre de l'utiliser ou non. Une note positive permet, par exemple, aux habitants de bénéficier de tarifs réduits dans les transports en commun.

Avec la collaboration des géants chinois de l'Internet

Le résultat du crédit social est obtenu en compilant des données relatives à sa situation administrative (publications sur les réseaux sociaux, diplômes, antécédents de condamnation et d'amendes), mais aussi grâce aux informations personnelles sur ses préférences de consommation fournies par les géants de l'Internet comme Baidu, Alibaba et Tencent. Pour le moment, rien

n'indique que les données recueillies par ces sociétés soient communiquées systématiquement aux autorités publiques, même si leur collaboration ponctuelle est réelle.

Ces entreprises disposent de leur propre système de crédit, comme le « Sésame credit » développé par une filiale d'Alibaba. Ce score de crédit commercial est calculé en fonction de l'historique d'achat du client sur les sites marchands comme Tmall ou Taobao, et offre aux clients jugés les plus honnêtes et les plus responsables certains avantages (comme ne pas devoir laisser de caution à l'hôtel).

L'établissement de crédit, *China rapid finance* peut obtenir du moteur de recherche Baidu des informations sur l'historique de navigation de ses visiteurs. Et des recherches trop fréquentes sur le cancer ou les jeux de hasard peuvent compromettre la possibilité d'obtenir un prêt à un taux avantageux. Ces systèmes privés sont parfois confondus avec le projet gouvernemental de crédit social, pourtant distinct, même si la frontière reste poreuse.

Le quotidien *Les Échos* sous la plume de Frédéric Schaeffer titrait récemment : « En Chine, 1,4 milliard de suspects sous surveillance » en dénonçant l'usage de l'intelligence artificielle, et des données biométriques pour surveiller, et arrêter les auteurs de crimes ou délits.

Modèle liberticide chinois et régressions occidentales

Les pouvoirs publics justifient ce maillage tentaculaire au nom de la modernité et de la lutte contre la criminalité (dans un pays aussi vaste, où les solidarités familiales et ethniques restent fortes, de nombreux condamnés parviennent à échapper à l'application des décisions de justice). Mais la Chine est-elle la quintessence de la société orwellienne ?

Nos incantations contre ce modèle liberticide ne doivent pas faire oublier, nos propres régressions-évolutions depuis vingt ans dans le domaine des libertés publiques, qui amènent dans les sociétés démocratiques à des comportements de fichage généralisés.

La plus grande base d'empreintes génétiques (ADN) rapportée à la population se situe dans le patrie de l'*habeas corpus*, le Royaume Uni. Constituée à partir de 1995, l'*UK National Criminal Intelligence DNA Database*, contient actuellement près de six millions de profils génétiques, soit un habitant sur six. Et comme l'ADN d'un individu est en partie similaire à celui de ses ascendants et ses descendants, c'est potentiellement, la moitié de la population britannique qui peut ainsi être identifiée.

La France n'est pas en reste avec l'élargissement des cas où les empreintes génétiques sont relevées. Et que dire du *Patriot Act* adopté au lendemain du 11 septembre 2001, et qui oblige les fournisseurs d'accès à Internet à communiquer les informations personnelles de leurs clients aux services de sécurité, et somme les bibliothécaires de dénoncer les usagers suspects ?

Si ces mesures liberticides se justifient face à la menace terroriste, il semble excessif de s'exonérer de reproches pour dépeindre la Chine en antichambre de la société de contrôle. Au Canada comme aux États-Unis, les particuliers sont évalués par les commerçants, leur banque ou leur créancier selon « l'antécédent de crédit ».

Mais il ne suffit pas de payer rubis sur l'ongle ses dettes pour être considéré comme un interlocuteur de confiance, puisque le retard de paiement d'une amende de stationnement ou même à cause d'un livre rendu en retard à la bibliothèque municipale peut vous desservir. Cette cote de crédit peut être consultée par un propriétaire, un loueur de voiture ou un employeur éventuel. Et que dire des Américains qui publient nom, adresse, photographie et description physique des condamnés pour crimes et délis ?

En Inde aussi…

Le contrôle social en Chine partage plusieurs objectifs avec ceux des démocraties occidentales, comme prévenir le risque terroriste, ici lié au séparatisme de la minorité des Ouighours. Mais il diffère sur plusieurs points :

- en Asie, la liberté de l'individu doit s'effacer au profit de l'intérêt collectif. La tranquillité de la société implique de lutter contre les comportements criminels ou plus simplement le manque de civisme.
- le développement économique de la Chine ne s'est pas accompagné d'un système de régulation bancaire efficace. La solvabilité comme le sérieux des entreprises publique ou parapublique est difficile à évaluer (normes comptables différentes, audits complaisants). Or la confiance envers les institutions et les agents économiques est l'un des ingrédients essentiels pour favoriser l'entreprenariat.
- la dénonciation publique des coupables de crimes ou de délits « indignes de confiance » – le

but étant dissuasif, dans une société où la préservation de l'honorabilité du groupe social (la famille, l'entreprise)– est fondamentale.

- une coopération plus régulière entre l'État et les acteurs de l'Internet chinois pour mieux cerner les profils des citoyens en fonction de leurs habitudes de consommation. Mais cette situation n'est pas propre à la Chine, puisque les révélations d'Edward Snowden sur le programme PRISM ont montré la connivence entre la NSA et les sociétés de la Silicon Valley.

La surveillance électronique en Chine n'est pas malheureusement l'apanage des régimes autoritaires, puisque le gouvernement de Narendra Modi en Inde a, lui aussi, entrepris une surveillance massive par le biais de la carte d'identité biométrique, dite carte Aadhar.

En Chine, elle est volontairement plus visible pour être dissuasive et, sous le prétexte d'une lutte louable contre la criminalité, vise à assurer la stabilité du régime et surtout n'offre guère de recours juridiques aux contrevenants.

Source
afp
2 mai 2019

2. HRW dénonce la surveillance quotidienne au Xinjiang grâce à une application

Les autorités chinoises utilisent une application de téléphonie mobile pour surveiller les musulmans du Xinjiang et taxent de suspectes des conduites quotidiennes « totalement légales », assure un rapport de l'ONG Human Rights Watch.

Pékin s'est attiré de vives critiques dans le monde avec sa politique de fermeté au Xinjiang (nord-ouest) où les Ouïghours, ethnie musulmane apparentée aux Turcs, sont majoritaires. Une politique mise en place au nom de la lutte contre le terrorisme islamique et le séparatisme dans cette région de plus de 20 millions d'habitants endeuillée ces dernières années par des attentats et des violences ethniques.

Pékin est accusé d'avoir interné jusqu'à un million de Ouïghours dans des camps de rééducation politique. Le régime communiste dément ce chiffre et parle de « centres de formation professionnelle » destinés à lutter contre la radicalisation islamiste.

Human Rights Watch a déjà fait état par le passé de l'utilisation par les autorités au Xinjiang d'un système de surveillance intitulé Integrated Joint Operations Platform (IJOP) pour rassembler des informations provenant de diverses sources allant de caméras de reconnaissance faciale aux analyseurs de wifi en passant par les barrages policiers, les données bancaires et les perquisitions à domicile.

Mais dans son nouveau rapport, intitulé « Les algorithmes de répression de la Chine », HRW étudie l'utilisation d'une application connectée à l'IJOP pour surveiller des conduites spécifiques.

Selon le rapport, les autorités du Xinjiang surveillent ainsi étroitement 36 catégories de conduites, par exemple le fait de ne pas sympathiser avec ses voisins, d'éviter d'utiliser la porte principale ou un smartphone, de faire des dons à des mosquées « avec enthousiasme » ou d'utiliser des quantités « anormales » d'électricité.

Surveillance élargie

L'application conseille aussi de surveiller quiconque est lié à une personne ayant un nouveau numéro de téléphone ou ayant quitté le pays depuis plus de trente jours.

« Nos recherches montrent, pour la première fois, que les policiers du Xinjiang utilisent des informations collectées de manière illégale à propos de conduites parfaitement légales et les utilisent » contre les personnes concernées, a déclaré Maya Wang, spécialiste de la Chine pour HRW.

L'ONG a obtenu une copie de l'application et a demandé à la société berlinoise de cybersécurité Cure53 de l'étudier. Outre la collecte de données personnelles, l'application incite les autorités à faire des rapports sur les personnes, véhicules ou événements qu'elles jugent suspects et envoie des « missions d'enquête » à la police pour un suivi.

Les policiers se voient également demander de vérifier l'utilisation de l'un des 51 outils internet estimés suspects, parmi lesquels des plateformes étrangères comme WhatsApp, LINE ou Telegram.

Plusieurs personnes ont indiqué qu'elles-mêmes ou des membres de leur famille avaient été arrêtés pour avoir WhatsApp ou un Virtual Private Network (VPN) installé sur leur téléphone, selon le rapport.

Le rapport estime que le système IJOP semble suivre les données de chacun au Xinjiang par le

biais de la localisation des téléphones et des véhicules ainsi que l'utilisation d'électricité et de gaz.

Selon HRW, l'application a été développée par Hebei Far East Communication System Engineering Company (HBFEC) alors contrôlée par le groupe public China Electronics Technology Group Corporation (CETC). CETC n'a pu être contacté et HBFEC n'a pas répondu aux demandes de commentaires.

Washington avait imposé l'an dernier des contrôles sur les exportations de compagnies chinoises dont HBFEC et d'autres entités contrôlées par CETC en invoquant des risques pour la sécurité nationale.

Selon Greg Walton, un expert indépendant sur la cybersécurité qui a conseillé les auteurs du rapport, le système constitue «un outil brutal qui peut directement contribuer au nombre massif de gens dans des camps d'internement».

Mais en outre, les données recueillies, si elles sont stockées, pourraient servir à de nouveaux algorithmes : « les données collectées aujourd'hui par l'application pourraient être analysées dans quelques années avec une logique bien plus sophistiquée ».

Source
lebigdata.fr
Bastien L
23 septembre 2019

3. La caméra 500 MP créée par la Chine met fin au concept de vie privée

Les scientifiques chinois ont créé une caméra de définition 500 MP, capable de filmer des milliers de personnes simultanément et d'identifier n'importe quel individu instantanément. Un véritable désastre pour la confidentialité des citoyens chinois...

C'est une véritable prouesse technologique, mais aussi un couperet pour la confidentialité. Les scientifiques chinois de la Fudan University de Shanghai et du Changchun Institute of Optics, Fine Mecanics and Physics of Chinese Academy of Sciences de Changchun ont créé une caméra de 500 mégapixels reposant sur l'intelligence artificielle.

Cette définition d'image est cinq fois plus élevée que celle de l'oeil humain, qui atteint 120 millions de pixels. Ainsi, ce système est capable de capturer les milliers de visages de spectateurs d'un stade dans les moindres détails.

Grâce à l'IA et à la reconnaissance faciale, toutes les personnes photographiées sont immédiatement identifiées et leurs données sont transmises vers le Cloud. Si une personne précise est recherchée, la caméra est capable de la localiser instantanément…

La caméra 500 MP identifie n'importe qui en un instant grâce à l'IA

Selon Zeng Xiaoyang, l'un des scientifiques à l'origine du projet, des utilisateurs du monde entier pourront se connecter au système pour obtenir des données. Par exemple, la police pourra installer la caméra dans les grandes villes afin de surveiller la foule et empêcher toute activité criminelle.

Cette innovation peut aussi être appliquée au secteur militaire. La caméra pourra par exemple surveiller les bases militaires ou les bases de lancement satellite, ainsi que les frontières nationales.

Cependant, plusieurs experts s'inquiètent à juste titre des conséquences négatives que pourrait avoir ce système sur la confidentialité des citoyens. Selon Wang Peiji, doctorant à l'école d'aéronautique de l'Harbin Institute of Technolog, cette caméra pourrait être utilisée au détriment de la confidentialité personnelle.

Si les individus peuvent être surveillés et identifiés en permanence par une telle caméra, ils peuvent renoncer à la notion de vie privée. Selon Wang, les systèmes de surveillance déjà en place sont largement suffisants et celui-ci représente donc en plus un coût superflu...

Source
Siècle Digital
Geneviève Fournier
5 novembre 2019

4. Le déclin de la liberté sur internet

L'ONG Freedom House publie son rapport annuel ce mardi 5 novembre 2019, en pointant du doigt la manipulation et la surveillance des réseaux sociaux.

Étude pour le moins alarmante de la part de Freedom House, organisation non-gouvernementale (mais financée en partie par le gouvernement américain), qui déclare *constater* une « chute de l'indice de liberté sur le Web » dans 33 pays. Sur les 65 pays passés en revue – regroupant 87 % des utilisateurs dans le monde – pas moins de 40 d'entre eux utiliseraient des « programmes avancés de

surveillance des réseaux sociaux ». Autre « record » annoncé : 38 États emploient des individus pour interférer sur les informations en ligne.

Les réseaux sociaux, outils de propagande

L'interférence sur internet est devenue, selon le rapport, une stratégie commune à beaucoup de pays dont les dirigeants sont prompts à disloquer les démocraties. La désinformation et la propagande sont les principaux outils utilisés dans cette interférence. Les États nationaux, et les acteurs partisans utilisent les réseaux en ligne pour répandre leurs conspirations, théories du complot, et plus généralement de fausses informations. Ce faisant, des gouvernements amis, personnalités médiatisées ou du secteur des affaires, favorables à ces acteurs locaux ou États, sont souvent associés à ces stratagèmes : « Beaucoup de gouvernements trouvent que l'utilisation des réseaux sociaux pour diffuser leur propagande est beaucoup plus efficace que la censure » déclare Mike Abramowitz, président de l'organisation Freedom House.

« Les autoritaristes et populistes du globe exploitent la nature humaine et l'associe à la magie des algorithmes numériques pour contrer les scrutins, et passer outre les règles établies pour garantir des élections libres, et justes. », est-il ajouté. Et si les entreprises technologiques tentent de mettre en place des techniques de défense, et des systèmes de vérification pour combattre ce type de désinformation, certains de ces acteurs ne cessent de faire évoluer leurs tactiques. Le rapport prend l'exemple des candidats aux Philippines, n'hésitant pas à solliciter directement les acteurs influenceurs sur les réseaux sociaux tels que Facebook, Twitter, ou encore Instagram pour qu'ils déploient de fausses informations, en échange d'une jolie somme d'argent.

L'affaire est d'autant plus juteuse pour ces États qu'hormis ces quelques pot-de-vins, elle ne leur coûte que très peu d'argent. Les réseaux sociaux permettent d'atteindre un maximum d'utilisateurs en très peu de temps. De quoi pervertir ce qui, il y a une bonne dizaine d'années, pouvait être considéré comme un outil fantastique de communication, favorisant les liens sociaux.

Cette dérive est d'autant plus inquiétante, qu'en plus de devenir un outil de propagande venant ternir le système électoral démocratique, les réseaux sociaux se transforment peu à peu en outil de surveillance pour ces acteurs peu scrupuleux. Aussi, en plus d'interférer dans les campagnes politiques comme ce fut le cas lors des élections présidentielles américaines en 2016, ou des élections de mi-mandat en 2018, et d'offrir à des pays comme la Russie, la Chine, l'Iran, et l'Arabie Saoudite, les moyens d'influencer les élections démocratiques étrangères, dixit l'ONG américaine, l'utilisation de ces plate-formes permet la collecte et l'analyse de nombreuses données.

Les réseaux sociaux, outils de surveillance

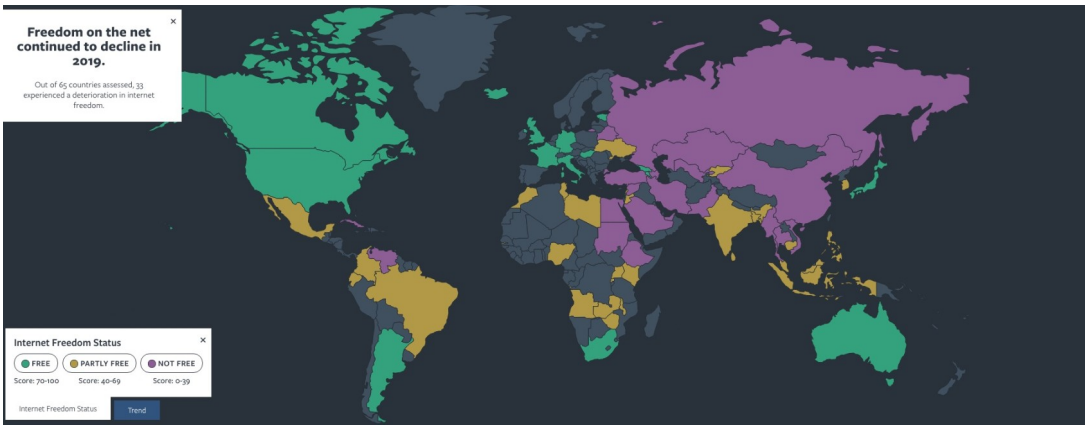
L'ONG américaine déclare avoir trouvé des preuves de l'existence de « programmes avancés de surveillance des réseaux sociaux » dans 40 des 65 pays passés en revue, regroupant 87 % des utilisateurs d'Internet dans le monde. Ce qui à une époque semblait réservé aux agences internationales de renseignement, devient quasi un lieu commun pour un ensemble d'acteurs nouveaux, bien décidés à profiter de ce nouveau terrain de jeu, à en croire l'étude publiée. De « nouveaux objectifs » sont évoqués, sans pour autant être clairement établis. À l'évidence, ils confèrent tous à prendre, ou maintenir le pouvoir de certains acteurs politiques, avec *in fine* des actions plus ou moins lucratives : rien de neuf à l'horizon.

L'embêtant, et le rapport ne manque pas de le préciser, réside davantage dans les moyens utilisés, directement reliés au quotidien des utilisateurs, et par conséquent aux libertés individuelles : « Le résultat est un redoutable accroissement global des abus sur les libertés civiles tandis que l'espace en ligne pour les actions civiques rétrécit » est-il expliqué. Parmi les 65 pays étudiés, 47 d'entre eux ont procédé à des arrestations de personnes tenant des discours d'ordre politique, social ou religieux, précisent les auteurs du document.

Cette étude aura sollicité la contribution de 70 analystes, utilisant une méthodologie de recherche regroupant des thèmes abordant les problèmes d'accès à Internet, de liberté d'expression et de respect de vie privée. Établi entre juin 2018 et mai 2019, l'objectif d'un tel rapport, expliquent les membres de l'ONG, est d'évaluer l'impact des technologies de l'information et de communication sur la démocratie. Les données spécifiques aux pays qui sous-tendent les « tendances de cette année » sont disponibles en ligne, peut-on lire sur le site de Freedom House.

Des natures méfiantes pourraient éventuellement avancer que parmi les États pointés du doigt, nombreux sont reconnus comme des pays qui s'opposent de manière générale au modèle américain, que ce soit d'un point de vue social, politique ou économique. Libre à chacun de vérifier les données établies. Plus difficile toutefois de contester les atteintes aux valeurs démocratiques qu'impliquent les

actions des pays cités. Aussi lorsque la décision de supprimer l'accès des citoyens à Internet ou à certaines plate-formes du Web est prise en Chine, au Soudan, au Bangladesh, au Brésil, ou au Zimbabwe, difficile de ne pas considérer cela comme de la censure, ni plus, ni moins.



Représentation cartographique de la liberté sur Internet, établie par Freedom House
Crédit : ONG Freedom House

Les États-Unis ne sont pas épargnés par l'ONG, qui rapporte les actes des forces de l'ordre américaines : « Les forces de l'ordre et les autorités qui s'occupent de l'immigration ont étendu leur surveillance, en contournant les mécanismes de transparence, de contrôle et de responsabilité qui auraient pu restreindre leurs actions ». Et d'ajouter que « les agents ont espionné, sans mandat, les appareils électroniques de voyageurs pour récolter des informations sur des activités protégées par la Constitution, comme les manifestations pacifiques ». Ceci avant de conclure sur la nécessité de « corriger les réseaux sociaux » et le rôle de l'État qui se doit de promouvoir « la transparence et la responsabilisation à l'ère numérique ». Vaste sujet. Si pour les responsables de Freedom House, c'est « le seul moyen d'empêcher internet de devenir un cheval de Troie pour la tyrannie et l'oppression », la transparence et la responsabilisation peuvent tout aussi bien être utilisées pour répondre aux besoins des services de sécurité nationale.

Comment trouver un équilibre entre la liberté d'expression, le respect des libertés individuelles, de la vie privée, et les détournements évoqués dans ce rapport ? S'il convient de respecter ces libertés indissociables des valeurs démocratiques, nombreux sont les cas, où au nom de les protéger, contre le terrorisme notamment, celles-là même sont bafouées, au profit d'un espionnage numérique. Il en va de même pour la lutte contre la désinformation, en particulier lors des campagnes politiques, jusqu'où l'État doit-il, et peut-il, se porter garant d'une transparence, et donc d'un contrôle ?

Ces questions n'ont, semble-t-il, pas fini d'ombrager le paysage de l'ère numérique dans laquelle la société évolue désormais.

5. Trois milliards d'internautes sont espionnés par les gouvernements

Source
VICE
David Gilbert
20 novembre 2019

Un nouveau rapport révèle l'utilisation du numérique par les gouvernements pour réprimer la dissidence, faire de la désinformation et saboter les élections, même dans les démocraties.

Des dizaines de gouvernements autour du monde utilisent les réseaux sociaux pour saboter les élections démocratiques et espionner leurs propres citoyens, comme le révèle un nouveau rapport. Chaque année, la *Freedom House*, une ONG financée par le gouvernement des États-Unis pour étudier et défendre la démocratie, publie un rapport d'analyse de la liberté sur Internet dans le monde. La dernière édition du rapport annuel « *Freedom on the Net* » montre que, plutôt que d'agir comme vecteur pour plus de transparence et d'élections ouvertes, Internet est utilisé pour saper le processus démocratique.

Lundi dernier, Mike Abramowitz, président de *Freedom House*, a livré son analyse à des journalistes : « Les gouvernements et les mouvements populistes utilisent les médias pour manipuler les élections à grande échelle et les gouvernements utilisent la technologie pour surveiller leurs

propres citoyens comme jamais auparavant. » C'est la deuxième année que la liberté sur Internet décline, selon les données collectées par la *Freedom House*. Il y a deux raisons principales qui peuvent expliquer cette tendance, qui sont dues, en partie, au pouvoir sans cesse croissant des réseaux sociaux : le piratage croissant des élections en ligne et la surveillance gouvernementale renforcée.

Aujourd'hui, presque trois milliards de personnes dans le monde sont sous surveillance des gouvernements et de la police – sachant qu'il y a 38 millions d'utilisateurs de réseaux sociaux en France – en partie parce que la surveillance numérique est de plus en plus abordable, selon les rapports. « Les gouvernements utilisent les médias sociaux pour rassembler et analyser des dossiers de données personnelles sur des populations entières, dit Mike Abramowitz. Beaucoup utilisent l'intelligence artificielle pour identifier de potentielles menaces et pour faire taire l'opposition. Alors que la cyber-surveillance devient de moins en moins chère, un nombre croissant de services de police utilisent la surveillance de masse avec peu de supervision et de comptes à rendre. »

Le rapport étudie la liberté Internet dans 65 pays du monde, couvrant 87 % des internautes au total. Pour la quatrième année consécutive, la Chine est le pays où la liberté d'expression est la plus limitée et l'Islande le pays où elle est le plus protégée. Aux États-Unis, la liberté Internet a décliné pour la troisième année de suite grâce à la croissance de la surveillance sur les réseaux sociaux par les services de police, les autorités d'immigration contrôlant les gens qui veulent traverser la frontière méridionale.

Des documents publiés plus tôt dans l'année ont révélé qu'en été 2018, le service d'immigration des États-Unis avait surveillé l'usage des réseaux sociaux des participants lors d'une manifestations anti-Trump à New York. « Des agents du département de la Sécurité intérieure des États-Unis ont utilisé les outils de surveillance des réseaux sociaux pour suivre de près les activités des Américains encadrées par la constitution. Ils observent non seulement le passage de la frontière du Mexique mais aussi des manifestations pacifiques sur l'immigration et d'autres sujets », a révélé Adrian Shahbaz, un des auteurs du rapport.

Le rapport a révélé une autre évolution perturbante : l'utilisation croissante de la désinformation dans les démocraties. Les campagnes de désinformation en ligne existent depuis des années, mais le rapport montre qu'elles ne sont plus le simple privilège des dictatures. « Le plus alarmant c'est que non seulement les leaders populistes et d'extrême droite sont devenus des partisans de la désinformation massive mais ils exploitent aussi les réseaux qui les diffusent », commente Mike Abramowitz.

Adrian Shahbaz a pris comme exemple l'élection présidentielle du Brésil de 2018, où le leader autoritaire Jair Bolsonaro a réussi à exploiter le pouvoir des plateformes numériques pour s'assurer la présidence. « Tout comme des experts ont volé aux États-Unis des données de Facebook pour développer des profils psychologiques de millions d'Américains, il y a trois ans, les autorités politiques au Brésil ont extorqué des numéros de téléphone via les réseaux sociaux et ajouté automatiquement des électeurs à des groupes WhatsApp spécialement créés, selon le lieu, le genre et le niveau de revenus, a révélé Shabaz. Ces groupes sont devenus le laboratoire parfait pour ce nouveau système de campagne électorale sans scrupules. » Il y a eu des cas similaires en Inde et aux Philippines. Au Myanmar Facebook a été accusé d'aider l'armée à mener un génocide.

Mais Mike Abramowitz indique que malgré le déclin général, il y a eu quelques victoires. « Il y a eu quelques exemples frappants de la technologie nourrissant un changement positif pour les démocraties », a lancé Mike Abramowitz en pointant du doigt le Liban, l'Algérie et Hong Kong, où les activistes utilisent Internet et les smartphones pour tenir « les politiciens incompétents et corrompus » responsables auprès du peuple.

Le rapport recommande plusieurs façons de réagir aux campagnes de désinformation et à la surveillance des réseaux sociaux. Ils suggèrent notamment « d'assurer que les publicités politiques soient transparentes et que leurs contenus adhèrent à des standards stricts. » Alors que Twitter a interdit les publicités politiques, Facebook affirme qu'il ne va pas vérifier le contenu des publicités politiques sur sa plateforme.

Mais le rapport met en garde en expliquant que sans collaboration du gouvernement et des compagnies privées pour régler le problème, la situation n'allait qu'empirer, en particulier avec l'avancée de la technologie comme la 5G, les données biométriques et l'intelligence artificielle qui nous attendent au coin de la rue. « De fortes protections des libertés démocratiques sont nécessaires pour assurer qu'Internet ne devienne pas un cheval de Troyes de la tyrannie et de l'oppression », juge le rapport. « Le futur de la vie privée, de la liberté d'expression et de la gouvernance démocratique repose sur les décisions que nous faisons aujourd'hui. »

Source
letemps.ch
Anouch Seydtaghia
26 juillet 2021

6. Derrière le scandale Pegasus, la face oubliée de la surveillance de masse

La mise en lumière de l'espionnage effectué grâce au logiciel Pegasus de la société NSO ne doit pas faire oublier la surveillance de masse effectuée par les géants de la tech. Attention, aussi, aux mesures prises pour lutter contre la pandémie.

Le 18 juillet fera date dans l'histoire de la surveillance de masse. Les révélations autour de l'utilisation du logiciel espion Pegasus, vendu par la société israélienne NSO, ont créé un choc mondial : plus de 50 000 numéros ciblés, des dizaines de téléphones infectés analysés, des personnalités visées telles Emmanuel Macron et le dalaï-lama… L'affaire rappelle celle déclenchée par les révélations dues à Edward Snowden, dès le 6 juin 2013, sur les écoutes de masse effectuées par la NSA, l'Agence nationale de sécurité américaine. Un détonateur planétaire, puis des soubresauts, avant un quasi-basculement dans l'oubli.

Ces coups de projecteur violents sur ces activités d'espionnage ont choqué. Certains espèrent qu'ils apporteront des changements de pratique. Mais rien n'est moins sûr. Les États-Unis poursuivent certainement leurs activités d'écoute massive. Et rien n'indique que les États qui emploient les logiciels de NSO cesseront d'acheter leurs licences – que ce soit pour des cibles à l'interne ou à l'étranger.

Système global

Mais ces éclats ne doivent pas faire oublier une tendance plus massive. Et d'une échelle sans commune mesure avec celle des deux affaires précitées: la surveillance de masse effectuée par les géants de la tech. On ne parle plus ici du ciblage de personnalités publiques, ou de citoyens d'un pays. On parle d'un système global de récolte massive de données, dans un but purement commercial. Un phénomène sans limite, que ne doivent pas occulter les récentes affaires d'espionnage.

Cette aspiration de données n'est bien sûr pas nouvelle. Mais de manière silencieuse et quasi indétectable, elle s'intensifie. La pandémie dope Google, Facebook ou Amazon – on le verra encore cette semaine après la publication de leurs résultats – et les rend plus indispensables. Des exemples ? Google qui analyse les recherches liées au virus et crée des centres de dépistage, Amazon qui s'implique dans la vaccination, Facebook qui participe au débat sur les vaccins, Uber qui détient des données sur les trajets offerts vers les lieux de vaccination... « Les défis auxquels nous faisons face demandent une alliance sans précédent entre le secteur privé et le gouvernement », esquissait en avril 2020 Satya Nadella, directeur de Microsoft.

Privatisation des données

En parallèle, détenteurs de données sanitaires précieuses, plusieurs de ces géants veulent entrer sur le marché de la santé, notamment au moyen d'apps sophistiquées. Pour le bien de tous? Non, dans un but purement privé, comme le mettait récemment en lumière Nina Burleigh, autrice du livre *Virus: Vaccinations, the CDC, and the Hijacking of America's Response to the Pandemic* : « Les données collectées par ces applications ne sont pas transmises aux cabinets médicaux, ni versées dans une base de données de santé publique locale ou nationale. Elles sont vendues pour aider les commerçants à vendre des produits aux utilisateurs des applications, et non pour aider les responsables de la santé publique. Et d'autres technologies qui traquent les données et auraient pu également aider les responsables de la santé publique – les technologies de capteurs portables, la technologie de la maison intelligente et d'autres intelligences artificielles de surveillance de la santé en cours de développement – sont toutes conçues de la même manière au seul service d'intérêts commerciaux. »

Pour Nina Burleigh, la situation est paradoxale: de nombreux citoyens affichent de la défiance face aux autorités. Et en parallèle, ils laissent les géants de la tech aspirer une masse de plus en plus importante de leurs données. De manière indifférente, voire pour leur bien, pensent-ils. Mais cette surveillance de masse profite avant tout aux multinationales du numérique. « De jeunes entrepreneurs, sans aucun mandat démocratique, se sont emparés d'une manne d'informations et d'un pouvoir sans limites et sans comptes à rendre », écrivait récemment la sociologue et professeure à Harvard Shoshana Zuboff dans une tribune parue dans le *New York Times,* que *Le Temps* a traduite.

Un exemple ? Qui s'offusque encore, comme le rappelait récemment *Wired,* qu'Instagram récolte des données sur notre localisation, notre lieu d'habitation, les endroits que nous visitons et des détails sur les gens et les commerces que nous fréquentons ?

Les idées d'Israël et de Singapour

En parallèle à cette surveillance de masse effectuée de manière privée, la tentation est forte, pour certains Etats, de glisser vers un contrôle accru de leurs citoyens. Pour des motifs de santé publique, des mesures jugées liberticides par certains commencent à apparaître. Ce dimanche, le gouvernement israélien a ainsi décidé de surveiller les voyageurs de retour de l'étranger. Une application devra être installée sur leur téléphone pour connaître en tout temps leur localisation. En parallèle, confronté lui aussi à une augmentation des infections au virus, Singapour a étendu l'utilisation de son système d'enregistrement. Il faut s'enregistrer lorsqu'on pénètre dans des supermarchés, des restaurants ou des centres commerciaux.

En Suisse, rien de tel pour l'heure : le certificat covid n'est pas un moyen de s'enregistrer lorsqu'on pénètre dans un lieu (tel un festival), et aucune base de données centrale n'est créée. Tout comme pour SwissCovid, l'app du certificat n'utilise jamais la localisation.

Pointe de l'iceberg

Il faudra continuer à observer de près les nouveaux moyens de lutte numérique contre le virus à l'étranger. Mais aussi garder à l'esprit l'immense appétit des géants de la tech pour nos données. Et, enfin, ne pas oublier que l'affaire NSO, même si elle est importante, n'est que la pointe de l'iceberg d'une surveillance de masse à laquelle nous nous sommes sans doute déjà habitués.

Source
Courrier International
7 août 2021

7. Les nouveaux outils d'Apple pour lutter contre la pédophilie font peur aux défenseurs des libertés

Innovantes ou toxiques ? Les nouvelles mesures annoncées par le géant informatique pour repérer des images d'abus sexuel sur des enfants sur les appareils de ses utilisateurs et ses serveurs de stockage divisent, rapporte Wired.

Apple, en annonçant de nouvelles mesures pour repérer les images à caractère sexuel impliquant des enfants sur ses téléphones, tablettes et ordinateurs, s'expose à la critique des défenseurs des libertés publiques.

"Depuis des années, les entreprises de la tech sont tiraillées entre deux nécessités : celle de crypter les données de leurs utilisateurs pour protéger leur vie privée et celle de détecter les pratiques les plus répréhensibles de leurs utilisateurs", explique **Wired.** Voulant lier les deux, Apple a dévoilé jeudi 5 août de nouveaux outils, recourant à l'intelligence artificielle, pour "*détecter la nudité dans les photos envoyées via iMessage",* qui permettront également "*d'empêcher l'envoi et la réception de ces images, d'afficher des messages d'avertissement et, dans certains cas, de prévenir les parents que leur enfant a consulté ou reçu ce type de contenus"*.

Et les avis sont très partagés, entre ceux qui y voient une "*nouvelle solution innovante"* pour lutter contre la pédophilie en ligne et les autres, qui pointent une "*dangereuse capitulation face à la surveillance gouvernementale".*

La "fonctionnalité la plus innovante sur le plan technique – et la plus controversée", poursuit *Wired,* c'est un nouveau système comparant les images téléchargées sur le serveur iCloud d'Apple aux États-Unis avec les images d'abus sexuels sur des enfants identifiées. Cette technologie repose sur un processus de cryptage sur l'appareil et les serveurs d'Apple qui, à l'aide d'une intelligence artificielle reconstituant certaines couches d'images, les signalerait au Centre national pour enfants disparus et exploités (NCMEC), puis aux forces de l'ordre.

Apple soutient qu'aucune de ces nouvelles fonctionnalités "*ne met en danger la vie privée des utilisateurs",* le système "*permettant d'identifier des collections d'images d'abus sexuels sur des enfants sans jamais voir les autres images que les utilisateurs téléchargent sur iCloud".*

Une nouvelle forme troublante de surveillance

Si nombre d'associations de défense des mineurs "*ont immédiatement applaudi les mesures prises",* note le magazine, les défenseurs de la vie privée "*affirment qu'Apple a fait un pas vers une nouvelle forme troublante de surveillance et affaiblit sa position historiquement forte sur la vie*

privée face à la pression des forces de l'ordre".

Ce que résume pour *Wired* Nadim Kobeissi, spécialiste en cryptologie et fondateur de la société de logiciels de cryptographie Symbolic Software, basée à Paris :

"*Je ne défends pas la pédophilie. Mais le fait que nos appareils personnels soient constamment en train de nous analyser et de surveiller ce que nous faisons, en quête de contenus répréhensibles, et qu'ils transmettent un signalement aux autorités dans certains cas entraîne Apple sur une pente très, très glissante."*

Apple a toujours refusé de recourir à un système de chiffrement fort des données sur iCloud, son espace de stockage dématérialisé, malgré les demandes des défenseurs de la vie privée, rappelle *Wired*. On a pu le soupçonne d'ainsi "*céder à la pression"* des forces de l'ordre, comme le FBI, qui sans cela seraient privées d'un "*outil d'enquête précieux"*.

Avec ce nouveau système de détection des images pédophiles, pour l'instant limité au territoire américain, Apple met un doigt dans l'engrenage, *"prélude au cryptage définitif d'iCloud".* Matt Green, spécialiste en cryptographie à l'université Johns Hopkins, y voit une *"victoire mitigée sur le plan de la protection de la vie privée",* qui *"pourrait ouvrir la porte à d'autres demandes de la part de gouvernements du monde entier".* Et que fera Apple s'il était sollicité par la Chine pour chercher des contenus qui ne soient pas de la pédopornographie, mais *"des images politiques ou d'autres types d'informations sensibles"* ?

Source
letemps.ch
Anouch Seydtaghia
27 mai 2022

8. Respect de la vie privée ou lutte contre le crime, une tension impossible

En Suisse et dans l'Union européenne, des projets législatifs visant à affaiblir la sécurité des communications font débat. Même si leur but semble tout à fait louable .

Ces prochaines heures, ou peut-être ces prochaines minutes, vous allez sans doute utiliser, sur votre smartphone, les services de WhatsApp, Signal, Facebook Messenger ou Threema. Des services de messagerie fiables, pratiques et qui possèdent surtout une énorme qualité : la sécurisation des conversations. Les communications sont chiffrées, ce qui signifie que, hors circonstances exceptionnelles, personne ne peut accéder à vos messages. Comme protection de sa sphère privée, difficile de faire mieux. Et ce bouclier autour de nos communications a d'autant plus de valeur, aujourd'hui, que nos données personnelles sont sans cesse pillées, achetées et revendues par une myriade d'acteurs du numérique.

Mais cette protection est en danger. Car qui dit chiffrement des milliards de messages envoyés chaque jour, dit impossibilité pour les autorités d'y avoir accès. En Suisse, le législateur est tenté d'affaiblir ce chiffrement via la révision de plusieurs ordonnances. La manœuvre est pour l'heure étrange et confuse : les autorités semblent prendre prétexte de l'adaptation du cadre légal autour de la 5G pour y glisser des mesures visant à empêcher le chiffrement des données.

Des intentions louables

Au niveau européen, la volonté est beaucoup plus franche : un projet de loi vise à obliger les plateformes numériques à scanner en permanence les messages, avec le but clair de lutter notamment contre la diffusion de contenu pédopornographique.

Que ce soit en Suisse ou au niveau du continent, les intentions du législateur semblent louables. Mais elles comportent des risques énormes. Car affaiblir le chiffrement des communications, c'est tuer le chiffrement. Autoriser des états à accéder aux messages via des portes virtuelles uniquement accessibles à eux est totalement illusoire: des criminels auront vite fait de repérer ces accès et de les utiliser eux aussi.

Demander aux géants de la tech de scanner en permanence tout le contenu mis en ligne est tout aussi problématique. Il s'agirait alors d'une analyse totale de nos messages commise par le secteur privé, ce qui n'a rien de rassurant. On se souvient que l'année passée, Apple avait évoqué un système de détection par défaut, pour tous ses utilisateurs, d'images liées à de la pédopornographie. Mais face aux risques énormes de dérive – que faire en cas de faux positif, par exemple ? –, Apple avait gelé ce projet.

Affaiblir le chiffrement n'est jamais une bonne idée, car c'est la porte ouverte à une surveillance de masse. Cette tension entre les états d'un côté, les géants du numérique de l'autre, dure depuis des années. Aux premiers de réfléchir aux conséquences de leurs projets de loi. Aux seconds de proposer

d'autres solutions techniques. Il y va de la défense de nos libertés individuelles à tous.

Source
letemps.ch
Anouch
Seydtaghia
27 juin 2022

9. La surveillance de masse, une menace pour les Américaines qui songent à avorter

Aux États-Unis, les données récoltées par Google, Apple et une myriade d'autres sociétés tech pourraient aider à poursuivre des femmes souhaitant avorter. Les appels se multiplient pour que les géants de la tech récoltent moins de données.

Il y eut le premier choc, avec le feu vert, vendredi dernier, donné par la Cour suprême des États-Unis de criminaliser l'avortement. Puis, très vite, le deuxième choc. De nombreux Américains ont découvert l'incroyable système de surveillance mis en place par les géants de la technologie. Une surveillance permanente, sans limite, ultra-invasive, qui rend extraordinairement vulnérables les femmes qui songent à avorter. Les appels se multiplient pour que Google, Apple et d'autres firmes récoltant des données protègent les femmes. Mais pour l'heure, les géants du numérique se taisent.

Deux exemples très concrets montrent comment, avant même la décision de vendredi, des informations numériques étaient utilisées contre les femmes. En 2015, une femme habitant dans l'Indiana, ayant donné naissance à un enfant mort-né avait été condamnée à 20 ans de prison. L'accusation avait utilisé comme preuves à charge des SMS envoyés entre cette femme et une amie, portant sur l'achat de pilule abortive. En 2018, dans le Mississippi, un jury avait accusé de meurtre une femme ayant, elle aussi, mis au monde un enfant mort-né. L'accusation avait là aussi utilisé, à charge, ses recherches sur internet pour des pilules provoquant une fausse couche.

Sources précieuses

Dans les deux cas, l'accusation avait finalement abandonné, rendant la liberté à ces femmes. Mais l'annulation de l'arrêt Roe v. Wade, vendredi, change tout, car il crée une base légale qui devrait permettre à la moitié des États américains de criminaliser l'avortement en utilisant des sources précieuses d'information : recherches en ligne, localisation des téléphones, échanges de messages, applications de fertilité…

Vendredi, plusieurs sénateurs ont déposé une requête auprès de la *Federal Trade Commission* (FTC), afin qu'elle fasse pression auprès de Google et d'Apple pour qu'ils permettent une récolte de données massive de leurs clients. « Les courtiers en données revendent et partagent déjà les informations de localisation des personnes qui se rendent dans des cliniques pratiquant des avortements à toute personne possédant une carte de crédit », ont écrit les politiciens. Selon eux, partout où l'avortement sera illégal, les procureurs pourront exiger des informations de localisation sur toute personne ayant visité un fournisseur d'avortement.

Milliers de requêtes

Ce n'est pas un délire de politiciens. De plus en plus, les autorités exigent des géants de la tech des informations sensibles sur leurs utilisateurs. Prenons Google : 43 683 demandes de la justice américaine en 2018, 61 609 demandes en 2019, 78 591 demandes en 2020 et 2021 – pour laquelle les chiffres ne sont pas définitifs – devrait dépasser les 100 000 requêtes. En moyenne, Google obtempère dans 80 % des cas.

Ce n'est pas tout. Des politiciens exigent que les géants cessent d'obéir à des *geofence warrants*, soit des demandes de la justice souhaitant savoir qui se trouvait dans un endroit précis – comme une clinique pratiquant des avortements – à un certain moment. Les démocrates demandent ainsi que Google anonymise les données de localisation, sur le modèle d'Apple qui a déjà fait des efforts à ce sujet. « Les Américains qui peuvent s'offrir un iPhone bénéficient d'une plus grande protection contre la surveillance de leurs mouvements par le gouvernement que les dizaines de millions d'Américains qui utilisent des appareils Android », écrivent les signataires.

Conseils pratiques

Eva Galperin, directrice de la cybersécurité de l'ONG Electronic Frontier *Foundation* (EFF), a résumé ainsi la situation sur Twitter : « La différence entre aujourd'hui et la dernière fois que l'avortement était illégal aux États-Unis, c'est que nous vivons dans une ère de surveillance en ligne sans précédent. » EFF a ainsi publié un guide pratique pour tenter de protéger sa vie privée sur internet.

L'ONG recommande d'utiliser certains navigateurs, tels Brave, Firefox et DuckDuckGo, pour effectuer des recherches sensibles. L'ONG insiste sur l'utilisation de messageries chiffrées, telle la solution suisse Proton. L'emploi d'un VPN pour chiffrer toute sa connexion à internet est vivement recommandé. Il faut aussi désactiver les services de localisation de son téléphone « si vous vous rendez ou revenez d'un endroit plus susceptible d'être soumis à une surveillance accrue, ou si vous êtes particulièrement inquiet de savoir qui pourrait savoir que vous êtes là », écrit EFF.

Apps dangereuses

Les femmes américaines doivent aussi se méfier de certaines apps. En 2021, les autorités avaient épinglé l'app Flo, spécialisée dans le suivi des cycles menstruels, car elle partageait, sans le dire, des données avec Google et Facebook. Cette app est utilisée par plus de 100 millions de femmes.

À noter que ni Google ni Apple n'ont réagi face aux demandes de récolter moins d'informations. Ces sociétés ont promis de payer les déplacements de leurs employées pour qu'elles puissent se faire avorter si elles se trouvent dans des États où cela est désormais interdit. Google permet aussi à ses employés de déménager dans un autre État.

Source
letemps.ch
Agathe Seppey
27 juin 2022

9.1. Aux États-Unis, « Big Brother is watching » les utérus

Dans les États où l'avortement est ou sera illégal, les données en ligne des femmes pourraient être le butin d'une « chasse aux sorcières ». Sociologue du numérique, Sami Coll y voit une prise de contrôle des corps.

Un message à une amie, une recherche d'informations sur internet, un trajet géolocalisé vers une clinique d'IVG, une app de suivi du cycle menstruel. Les portables des Américaines qui pensent à avorter pourraient être utilisés comme des mines de « preuves à charge » dans les États où l'interruption de grossesse est, ou sera, criminalisée. La révocation de l'arrêt Roe v. Wade et ses conséquences matérialisent l'architecture et les mécanismes puissants de la surveillance de masse. Alors que les appels envers les géants de la tech retentissent pour que la récolte des données des femmes soit repensée, le sociologue du numérique genevois Sami Coll commente une situation vertigineuse.

L'abrogation de Roe v. Wade fait passer la surveillance des données, souvent abstraite, à une réalité très concrète pour des femmes des États conservateurs qui voudraient avorter malgré une interdiction. Laquelle ?

Sami Coll: Partons des bases. En ayant accès aux données d'une personne – une sorte de journal intime numérique – il est possible de reconstruire largement sa vie. À condition qu'il y ait une volonté politique et de l'argent, les possibilités technologiques sont pratiquement infinies. Dans ce cadre, on peut imaginer les pires des scénarios pour les Américaines qui souhaitent avorter. Géolocalisation, e-mails, messages, réseaux sociaux, systèmes de paiement, applications de traçage du cycle menstruel : tous les outils pourraient être utilisés pour les traquer et les punir.

Comment ?

Il y a d'abord la suspicion : la police pourrait fouiller dans les données d'une femme suspectée d'avoir avorté. Mais ça ne s'arrête pas là. Une criminalisation *a priori* et ciblée de celles qui pourraient potentiellement recourir à l'IVG pourrait être mise en place : on identifierait celles qui sont allées à un premier contrôle gynécologique, on traquerait ensuite leur géolocalisation pour voir si elles passent une frontière pour se rendre dans un autre État. Enfin, il ne faut pas penser que la justice et la police seraient les seules intéressées. Des associations extrémistes pro-vie peuvent se substituer aux autorités, s'approprier des outils numériques en créant de faux sites d'information sur l'IVG, engager des hackers, acheter des données et créer d'immenses listes de dénonciation. Le recoupement ouvre des mines d'informations.

Tout cela prédit une catastrophe, une chasse aux sorcières, et même si des lois viendront, je l'espère, encadrer tout cela, il y a de quoi s'inquiéter. D'ailleurs, le rapport « Pregnancy Panopticon» de l'organisation STOP (The Surveillance Technology Oversight Project) montre comment les femmes enceintes sont déjà traquées par les outils numériques, et comment cela pourrait s'aggraver.

Est-ce la première fois à l'échelle occidentale que Big Brother entrerait à ce point dans nos intimités ?

Je dirais que nous sommes déjà dans une société de surveillance généralisée mais hétérogène: les bases de données existent partout, mais grâce à des lois et à nos démocraties, elles ne peuvent pas forcément être croisées ou devenir centralisées. On parle plutôt de « Little Brothers ». Or, ce que le monde d'après Roe v. Wade appelle à l'esprit, c'est une avancée dans la prise de pouvoir et de contrôle sur les corps, théorisée en 1976 déjà par Michel Foucault dans *Histoire de la sexualité*. ici, on pourrait appeler ça un « biopouvoir hybride », tant exercé par l'État que par des privés.

En 2017, une femme du Mississippi a accouché d'un bébé mort-né. Dans son historique internet, il apparaissait qu'elle avait cherché des pilules provoquant une fausse couche et cela a été utilisé comme preuve pour l'accuser de meurtre. Cette situation pourrait arriver à n'importe quelle femme dans l'Amérique d'après Roe v. Wade ?

Ce cas est doublement, et extrêmement, parlant. Autant par la violence de ce jugement (une peine de prison, qui avait ensuite été abandonnée), que par son côté anodin (de simples recherches sur internet comme supposées preuves). Cet exemple montre aussi à quel point la punition peut nous rattraper bien après que l'on eut semé des informations en ligne. Il ne faut pas non plus oublier que des données dormantes, a priori peu sensibles à un moment X, peuvent être utilisées contre nous suite à un changement de régime politique, par exemple. L'Amérique post-Roe est une excellente illustration du faux sentiment de sécurité qui se retourne contre les gens qui pensent n'avoir « rien à cacher ».

C'est-à-dire ?

Dans nos démocraties libérales et progressistes, on a tendance à ne pas trop s'inquiéter. Or, il suffit d'un durcissement de régime pour que le cauchemar de la surveillance se révèle. La présence de l'extrême droite au pouvoir peut faire pencher la balance.

La seule solution pour les Américaines concernées par l'IVG qui veulent protéger leurs données et leur liberté, c'est donc de vivre cachées ?

À peu de chose près. Il ne faut rien publier d'explicite sur les réseaux, garder son téléphone éteint et communiquer depuis une cabine téléphonique, s'il en reste, durant le voyage vers l'État où elles se feront avorter. Cela montre à quel point la criminalisation est forte.

Des discriminations pourraient émerger entre les personnes qui ont plus de moyens de protéger leurs données et les autres ?

Oui. Les riches et les classes sociales plus éduquées auront par exemple plus facilement accès à des services médicaux complaisants, coûteux, qui pourraient agir discrètement, peut-être avec le service d'avocats qui feront en sorte de ne pas laisser de traces. On dit que la vie privée est un privilège de riches. Le droit à l'avortement devient de facto lui aussi un privilège de riches. Les inégalités sociales seront assurément encore davantage creusées.

Source
letemps.ch
Anouch Seydtaghia
24 février 2023

10. Au final, les CFF veulent contrôler les citoyens à un niveau jamais atteint en Suisse

Même sans utiliser la reconnaissance faciale, le projet de l'ex-régie fédérale sera le plus poussé du pays, devançant largement les services de mesure de Swisscom. Explications.

« Surveillance ». Rarement, sans doute, ce mot a été employé aussi souvent que cette semaine en Suisse. Mis en lumière par le magazine alémanique K-Tipp, le projet des CFF de pister les voyageurs dans les gares a suscité l'émoi. Riposte en deux temps de la compagnie, réactions de politiciens et d'experts, lettre ouverte d'AlgorithmWatch CH et de la Société numérique… Le dossier est

ultrasensible, pour plusieurs raisons : il concerne des millions de voyageurs, il touche une entreprise à 100% en mains publiques et a trait à des informations sensibles sur notre comportement. Maintenant que la poussière semble retombée, il est utile de placer cette affaire dans un contexte plus global.

D'abord, le terme de surveillance est-il juste ? Si l'on parle de contrôles et de mesures effectués de manière collective, la réponse est oui, sans ambiguïté. Si l'on pense à un pistage individuel, la réponse est non. Dans un premier temps, épluchant un appel d'offres effectué par les CFF, K-Tipp avait évoqué la reconnaissance faciale. Les CFF allaient installer des caméras permettant d'identifier les voyageurs un à un, avait-on lu. Il n'en sera rien, assurent désormais les CFF : « Nous ne voulons en aucun cas identifier les personnes. Nous n'avons donc pas besoin de reconnaissance faciale », assurait ainsi mardi Alexis Leuthold, responsable du département Immobilier.

« Nous ferons mieux »

Promis, affirmait le dirigeant, « il ne s'agit pas d'identifier des individus ». Alors, pourquoi un tel quiproquo ? « L'appel d'offres était formulé de manière très technique, avec des passages équivoques. Nous devrons faire mieux la prochaine fois », admettait Alexis Leuthold. Sur ce point essentiel, il faut croire les CFF, placés désormais sous surveillance par le préposé fédéral à la protection des données, ainsi que plusieurs collectifs de la société civile. En parallèle, il faut garder en mémoire que l'utilisation de la reconnaissance faciale, elle, se développe en Suisse : malgré ses approximations techniques, malgré ses biais, quatre polices cantonales, dont celles de Neuchâtel et Vaud, emploient cette technologie. Elle n'est toutefois pas utilisée de manière proactive et en temps réel, mais a posteriori, pour tenter d'identifier des individus sur la base de photos.

Une fois ce point éclairci, la question suivante est celle des moyens qui vont être employés dans 57 gares, avec une mise en service dès septembre prochain. Les capteurs – dont la nature reste à déterminer – permettront de savoir beaucoup de choses, admettent les CFF eux-mêmes : le nombre de poussettes sur un quai, la présence de voyageurs avec des skis ou des vélos. Bien sûr, ces capteurs seront aussi capables de mesurer le nombre de personnes à un endroit et leurs vitesse et sens de déplacement. Mais ce n'est pas tout: les CFF pourront connaître le genre, l'âge ou la taille. Comment l'ex-régie obtiendra-t-elle ces informations ? Avec quel degré de fiabilité ? Et ces données risquent-elles d'être croisées avec d'autres informations ? Pour l'heure, les CFF n'apportent aucune réponse à ces questions fondamentales.

À des fins commerciales

Un autre problème se pose : pourquoi récolter de telles données ? L'entreprise met en avant l'argument de la sécurité, sans le développer. Et admet à demi-mot que ces informations pourront être utilisées à des fins commerciales, pour louer au mieux des surfaces dans les gares. Même anonymisées, ces données, utilisées par une entreprise en mains de l'État à des fins commerciales, suscitent des questions légitimes.

En parallèle, il ne faut pas sous-estimer la puissance des outils technologiques. Nous l'évoquions en novembre 2021 : une firme suisse, Analysis Simulation Engineering, qui travaille d'ailleurs pour les CFF, est capable, via ses capteurs, de différencier les employés des clients en se basant sur leurs mouvements, d'analyser dans quelle direction regardent ces personnes et de détecter si elles portent ou non un masque.

L'exemple de Crans-Montana

Autre question : ce phénomène est-il nouveau ? Réponse : non, mais ce type de contrôle ou de mesure de masse atteint une précision sans précédent, grâce à l'évolution de la technologie. Depuis une dizaine d'années déjà, en utilisant les signaux Bluetooth des téléphones, des magasins, y compris en Suisse, étudient les déplacements des clients.

De plus, Swisscom continue à développer son offre appelée Mobility Insights en se basant sur l'analyse, anonymisée, des déplacements de ses clients en téléphonie mobile. L'opérateur, qui se targue d'analyser 20 milliards d'interactions sur son réseau chaque jour, peut ainsi fournir des données précises. Il donne ainsi l'exemple de la station de Crans-Montana : il a réussi à déterminer facilement que durant les fêtes de fin d'année 78,54 % des visiteurs venaient de Suisse, 6,31 % d'Italie ou encore 3,58 % des Pays-Bas. De plus, 15 % de ces visiteurs effectuaient juste avant un arrêt à Sion ou Sierre – sans doute pour des achats, selon Swisscom. Autre exemple: lors du Montreux Jazz Festival de 2019, toujours selon Swisscom, 22 % des visiteurs avaient moins de 20 ans et 27 % avaient entre 21 et 40 ans.

Sans que l'on s'en rende vraiment compte, nos données de déplacement sont scrutées de plus en plus précisément. Mais jamais un projet aussi avancé que celui des CFF n'a été lancé en Suisse…