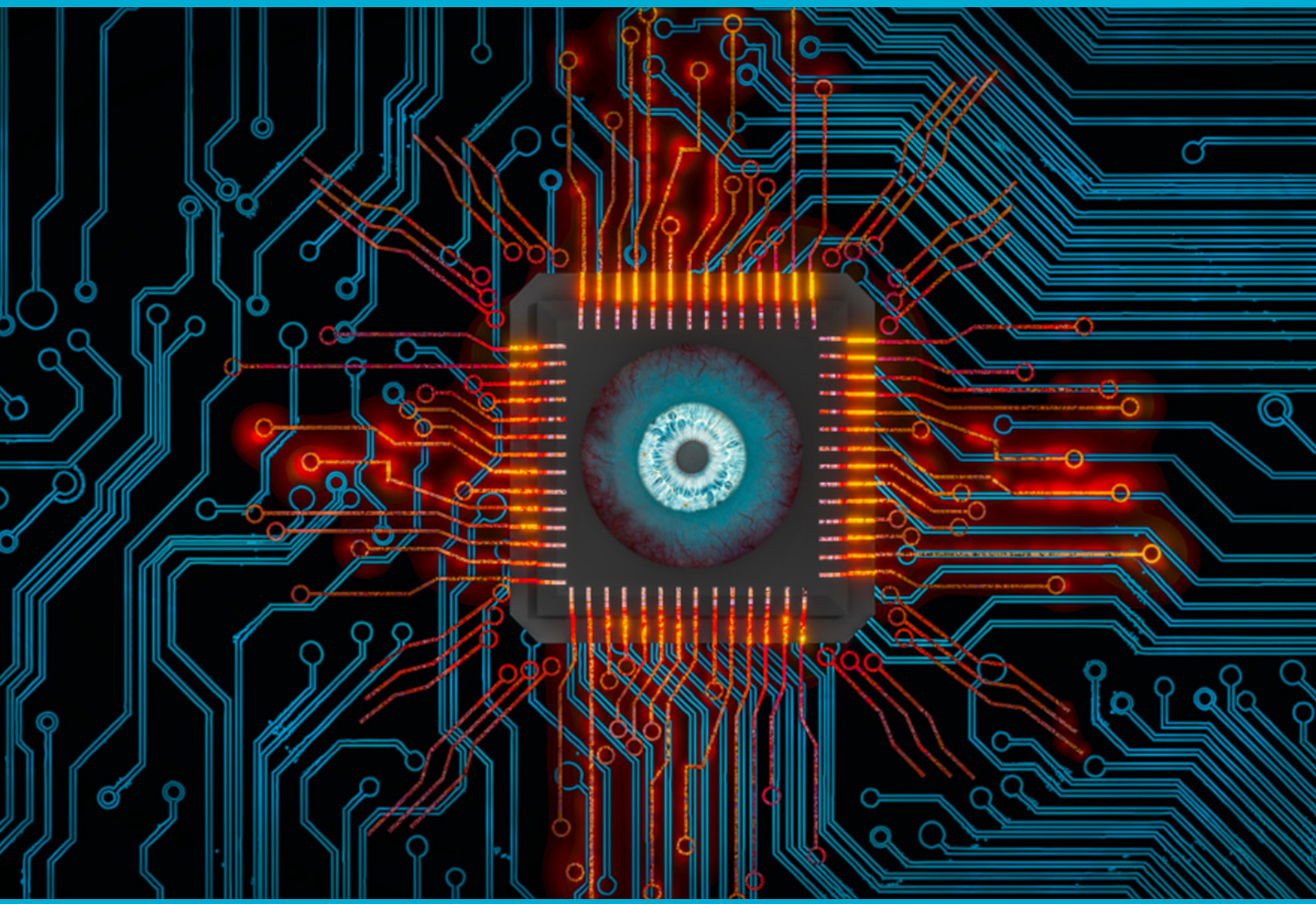
RSC SRC

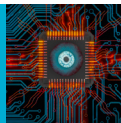
INFOVEILLANCE



GROUPE DE TRAVAIL DE LA SRC
2020

Table des matières

English version available.



Introduction

Infoveillance : Données, confidentialité, égalité et surveillance

David Lyon, Benoît Dupont, Anatoliy Gruzd, et Jane Bailey, en collaboration avec Stephen Wyatt et Monica Heller

Les visions utopiques et dystopiques des technologies numériques font débat depuis longtemps. Cette publication aborde un aspect spécifique des conséquences parfois perverses ou inattendues de l'entrée de ces technologies dans notre vie quotidienne : ce que nous appelons l'*infoveillance* - l'intégration des technologies de l'information et de la surveillance.

Les téléphones intelligents, la reconnaissance faciale, les moteurs de recherche Internet, les médias sociaux et les algorithmes d'auto-apprentissage offrent tous de nouvelles possibilités de générer des données à propos de nos activités quotidiennes individuelles, des données qui sont ensuite utilisées pour déterminer notre profil et nous suivre. Ce phénomène est devenu de plus en plus visible depuis la pandémie de COVID-19. Cinq millions de Canadiens ont déjà téléchargé *Alerte COVID*, l'application de suivi et de notification lancée par le gouvernement fédéral, créant une tension accrue quant à la question de savoir si la vie privée doit être échangée contre la sécurité.

L'infoveillance fait l'objet de discussions de plus en plus nombreuses au sein de groupes aussi divers que les universitaires, les professionnels de la santé, les représentants des communautés militant pour l'égalité, les décideurs politiques, les urbanistes et les défenseurs de la vie privée et des droits de la personne. Cette publication vise à explorer la signification de ce changement transformateur, en évitant l'optimisme sans limite des uns et le pessimisme profond des autres, afin d'envisager une voie médiane à suivre pour la société canadienne.

Alors que nous remplacions déjà de plus en plus les interactions physiques par des moyens virtuels en ligne, que ce soit pour le travail, les discussions quotidiennes, les réunions familiales, les verres entre amis, les divertissements ou les achats, la pandémie a intensifié et accéléré ce changement transformateur. Cette situation a créé une montagne de données sur nos intérêts, nos préférences et nos habitudes, ainsi que sur ceux de tous nos contacts. Lorsque les algorithmes analysent ces données, ils déterminent d'autres sujets ou produits qui pourraient nous intéresser, nous poussant ainsi vers certains comportements (tel que décrit dans le film *Derrière nos écrans de fumée*[1]).

Cet amas de données a clairement une valeur commerciale énorme et nous ne devrions pas être surpris que de nouvelles techniques soient développées pour monétiser ces informations en modifiant notre comportement, que ce soit pour faire des achats, manger, voter ou faire du tourisme. Shoshana Zuboff utilise le terme « *capitalisme de surveillance*[2] » pour souligner le fait que les données constituent un nouveau mode d'accumulation économique. Les algorithmes utilisent ces précieuses données accumulées pour nous classer en profils à des fins de marketing et pour alimenter les décisions des entreprises et des gouvernements qui ont une incidence directe sur tout, qu'il s'agisse des demandes de renseignements en ligne, de l'accès aux soins de santé, des possibilités d'emploi ou du système judiciaire. Comme Safiya Noble l'indique clairement dans *Algorithms of Oppression*[3], Les groupes qui revendiquent l'égalité sont particulièrement vulnérables à ce profilage qui reflète, perpétue et renforce la discrimination systémique inhérente à la société.

Devrions-nous donc être rassurés par l'engagement du gouvernement fédéral à renforcer la protection de notre vie privée ? Les défis soulevés par l'infoveillance vont bien au-delà de la simple protection de nos données personnelles, mais comprennent la manière dont les données, même anonymes, sont utilisées

1 *Derrière nos écrans de fumée* (2020) réalisé par Jeff Orlowski et sorti sur Netflix
2 *L'âge du capitalisme de surveillance* (2019) de Shoshana Zuboff et publié par Public Affairs
3 *Algorithms of Oppression* (2018) de Safiya Noble et publié par NYU Press

et par qui. Les nouveaux cadres de gouvernance doivent porter sur les futures pratiques probables en matière de collecte, d'analyse et d'utilisation des informations, et non pas seulement sur les pratiques passées et actuelles. L'élaboration de ces cadres exigera de la créativité dans la collaboration avec toutes les parties prenantes, ainsi que de la souplesse et de la responsabilité pour apaiser les inquiétudes des Canadiennes. Il faudra également opérer un changement conceptuel pour que la vie privée soit considérée comme un droit de la personne, intimement liée à d'autres droits tels que l'égalité.

Cet ensemble multidisciplinaire d'articles réunit quatre experts dans divers domaines, qui ont constitué le groupe de travail de la SRC sur l'infoveillance (2019-2020), sous les auspices du Comité de la SRC sur l'engagement public (CEP), et avec le soutien de deux des membres du CEP, Stephen Wyatt et Monica Heller. Ces articles constituent une série récente sur l'infoveillance dans *La Conversation*, publiée à différents moments en 2020. Ensemble, ils tentent d'atténuer l'optimisme et le pessimisme, de fournir des réponses aux questions et de poser les questions nécessaires à mesure de l'intégration de l'infoveillance en tant que nouvelle norme au Canada.

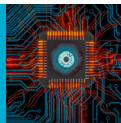
David Lyon, sociologue, directeur du Centre d'études de la surveillance à la *Queen's University*, a développé le concept de surveillance en tant que « tri social » et dirige un projet international sur la « surveillance des mégadonnées ».

Benoît Dupont, criminologue, titulaire d'une Chaire de recherche en cybersécurité à l'Université de Montréal, s'intéresse aux conséquences de la prolifération des technologies de surveillance sur notre société.

Anatoliy Gruzd, technologue de l'information, est titulaire d'une Chaire de recherche sur les médias sociaux à la *Ryerson University* et étudie les impacts des réseaux sur la société moderne.

Jane Bailey, professeure de droit à l'Université d'Ottawa, codirige le projet eQuality et étudie l'impact des technologies évolutives sur l'égalité, la vie privée et les droits, en particulier pour les membres des communautés en quête d'égalité.

David et Monica sont membres de la Société royale du Canada. Anatoliy, Benoît, Jane et Stephen sont membres du Collège de nouveaux chercheurs et créateurs en art et en science.



La surveillance au-delà de la vie privée

David Lyon | 17 juin 2020

La pandémie de la COVID-19 a déclenché une tempête au sujet de la surveillance, par rapport à la fois aux efforts de recherche déployés et aux questions liées à l'utilisation des données personnelles et à la confiance publique qui ont été soulevées. Les chercheurs ont amorcé une course folle pour mettre au point de nouvelles formes de surveillance et de suivi des données de santé publique, mais la transmission des données personnelles aux entreprises privées et aux gouvernements entraîne des risques en matière de droits personnels et collectifs. La COVID-19 ouvre un débat qui s'imposait depuis un bon moment.

Par exemple, Google et Apple ont offert des données de géolocalisation aux autorités de la santé pour la recherche de contacts. Et ce type de stratagème, comme certains autres, fait l'objet d'un vaste débat. La ruée vers des « solutions » de gestion des données est, espérons-le, bien intentionnée, mais qu'elles fonctionnent ou non, elles engendrent des risques qui dépassent le domaine de la « vie privée », au sens étroit du terme.

Un vaste ensemble de données est recueilli sur chacun et chacune d'entre nous – sur notre santé, notre éducation, nos emplois, nos contacts avec la police, notre comportement de consommateur – en fait sur toute notre vie. Ces données sont continuellement croisées selon des manières qui évoluent constamment et nous ne pouvons qu'espérer que ceux qui les manipulent respecteront notre « vie privée ». Mais ces données ont une influence souvent déterminante sur nos chances dans la vie et les choix qui nous sont offerts.

L'imposant ouvrage de Shoshana Zuboff, The Age of Surveillance Capitalism, a fait les manchettes pour son analyse des procédés utilisés par Google pour effectuer sa surveillance, des motifs de l'entreprise et des conséquences de cette surveillance. La thèse qu'elle défend est qu'un tout nouveau mode d'accumulation économique a rapidement commencé à se développer le jour où les plateformes Internet — avec Google en tête — ont découvert comment monétiser ce que certains appellent « l'échappement de données » généré par les communications en ligne quotidiennes; les recherches, les messages, les tweets, les textes. Les conséquences — la perte de la vie privée, la modification des comportements et la destruction de la démocratie — sont désastreuses.

Quoiqu'on puisse penser de tel ou tel détail de l'ouvrage de Mme Zuboff — il suscite tout un débat! — on ne peut manquer de remarquer son cri du cœur et sa dénonciation cinglante de « l'indifférence radicale » des plateformes telles qu'elles sont actuellement constituées, et de leurs « doctrines de l'inévitable ». Mais que faudra-t-il pour nous persuader que la surveillance est désormais devenue une dimension fondamentale de nos sociétés et qu'elle menace plus que notre simple « vie privée »? Le problème est indéniablement complexe, obscur et apparemment hors de contrôle, mais cela n'est pas une excuse pour nous laisser aller à la passivité. Cela doit plutôt nous encourager à creuser certaines des dimensions essentielles de la surveillance, à forcer l'ouverture des boîtes noires et à réaffirmer notre pouvoir humain.

Quatre électrochocs

Commençons par secouer certaines idées très répandues : que la surveillance est une affaire de caméras vidéo, de renseignements d'État et d'activités policières, qu'elle permet d'identifier des suspects et qu'elle porte atteinte à la vie privée. Google fait assurément de la « surveillance », communément

définie comme « toute attention ciblée, régulière et systématique portée à des détails personnels en vue d'exercer un contrôle ou une influence, ou à des fins de gestion.

Il n'y a pas que les caméras de vidéosurveillance – la surveillance est numérique, basée sur les données.

Pendant trop longtemps, le symbole suprême de la surveillance fut l'omniprésente caméra de surveillance, ce qui est tout à fait normal. La racine du mot surveillance en français signifie littéralement veiller sur, et c'est précisément ce que font les caméras. Elles deviennent de plus en plus intelligentes, surtout lorsqu'elles sont améliorées par une technologie de reconnaissance faciale. Clearview AI, par exemple, racle des milliards d'images sur des plateformes comme Facebook ou Google et vend ses services de jumelage à d'importants services policiers aux États-Unis et, jusqu'à récemment, à Toronto.

Mais aujourd'hui, c'est le téléphone intelligent qui mérite ce titre de symbole de la surveillance. Ce dispositif, plus que toute autre chose, nous relie aux entreprises, qui non seulement recueillent, mais analysent, trient, catégorisent et utilisent aussi les données que nous émettons constamment. Et cela se fait sans notre consentement, dans le but de nous influencer, de nous contrôler ou de nous gouverner. L'analyse des données est utilisée pour prédire, puis pour inciter des groupes précis de personnes à acheter, à se comporter ou à voter de la manière souhaitée. Le flux de données que transmettent nos dispositifs personnels alimente aujourd'hui la surveillance.

Il n'y a pas que l'État, il y a le marché – la surveillance sert à nous influencer, à des fins pécuniaires

Bien que l'État et ses organismes étendent effectivement trop souvent leurs tentacules au-delà des limites acceptables pour mettre en œuvre des stratégies de renseignement et de surveillance policière sans doute bien intentionnées, c'est le marché, et non l'État, qui détient les cartes d'accès du jeu de la surveillance. La surveillance étatique menace encore la démocratie et les libertés à différents degrés dans le monde. Certains aspects de la surveillance liée à la COVID-19, par exemple, peuvent également franchir cette limite. Mais l'État n'est plus le seul acteur qui inquiète.

Peu de gens ont remarqué, au début du 20e siècle, que de grands magasins, comme Syndicat St-Henri à Montréal, conservaient des dossiers détaillés sur leurs clients et qu'ils accordaient ou refusaient leur crédit en fonction du statut qu'ils leur avaient accordé. Aujourd'hui, nos profils indiquent notre « valeur individuelle » aux entreprises, mais ils servent aussi à nous propulser des publicités, qui influencent subtilement nos comportements et nos habitudes, et ces pratiques ne sont à peu près pas réglementées.

Le 11 septembre 2001 fut une date charnière, à partir de laquelle les entreprises technologiques, avides de clients après l'éclatement de la bulle Internet, ont commencé à offrir leurs services aux gouvernements. Ces partenariats de type « public-privé » sont monnaie courante aujourd'hui.

Maintenant, nos profils massivement gonflés de données indiquent notre « valeur individuelle » aux entreprises. Et ces données peuvent aussi être utiles à d'autres, par exemple les « consultants électoraux » – pensons seulement à Aggregate IQ et à Cambridge Analytica.

Il n'a pas que les suspects, c'est pour nous tous – la surveillance sert à nous classer en fonction de notre réputation

La surveillance visait autrefois principalement les suspects — ceux qui étaient soupçonnés de commettre des crimes étaient observés. Ce qui préoccupait en 1954 le sociologue français Jacques Ellul est devenu une réalité : l'appétit de plus en plus grand de la police pour des renseignements a fait de nous tous des suspects. Mais Ellul n'aurait pas pu deviner que tout cela allait se muter en un réseau de systèmes mondial — qui dépasse largement le domaine policier — dans lequel chaque personne est devenue une cible.

Mais nous ne sommes pas tous ciblés de la même façon. Les systèmes en question, qu'ils soient du domaine du bien-être, du commerce ou de la surveillance policière, répartissent les populations en

différentes catégories, qui seront traitées différemment les unes des autres, un peu comme le fait le centre de triage d'une urgence. Ce « tri social » est utilisé en marketing pour classer les gens en fonction de leur type de quartier — découvrez-le par vous-même en effectuant une recherche! Les données de nos dispositifs composent notre profil qui, pour les entreprises et d'autres, constitue notre réputation. En Chine, actuellement, des systèmes de crédit social de plus en plus importants sont exploités par le gouvernement; les nôtres sont utilisés par des entreprises.

Il n'y a pas que la vie privée, il y a aussi le droit des données

Dès ses débuts, l'informatique avait obligé les gouvernements à prendre conscience qu'une réglementation devait être adoptée, alors que des données personnelles étaient recueillies à des fins de plus en plus nombreuses. Initialement, les données provenaient des cartes de crédit, des permis de conduire et de l'assurance sociale; aujourd'hui, elles sont générées par l'utilisation constante de nos dispositifs. Mais la réglementation de la vie privée ne peut à elle seule suivre le rythme de développement des supersystèmes actuels de collecte, d'analyse et d'utilisation des données, qui engendrent le type de discrimination négative que devrait encadrer un nouveau droit des données.

Les lois sur la protection de la vie privée couvrent les domaines du corps, de l'espace et, en particulier, de l'information et de la communication, et ont pour but de préserver les libertés auxquelles on devrait avoir droit dans un monde démocratique. Elles ont été d'une grande utilité, mais nous demeurons très vulnérables. Une direction radicalement nouvelle doit être empruntée, une direction motivée par ce que nous savons des manières dont l'analyse des données, les algorithmes, l'apprentissage automatique et l'intelligence artificielle sont en train de remodeler notre environnement social. Nous ne devons pas seulement examiner la question de la collecte des données, mais également celles de leur analyse et de leur utilisation, en invoquant de nouvelles catégories telles que les droits numériques et le droit des données.

Défis posés par la surveillance

On peut se rendre compte, rien qu'en effleurant la surface de la surveillance effectuée au 21e siècle, à quel point les choses ont changé. Le paysage de la surveillance a évolué à une échelle tectonique, passant de la filature des suspects, du contrôle des travailleurs et de la classification des consommateurs, à la surveillance et au suivi de tout un chacun, actuellement pour la santé publique, exercés à une échelle sans précédent. La vie privée est indéniablement touchée, mais il en est de même pour les libertés fondamentales de la démocratie, pour les attentes en matière de justice et pour les espoirs liés à la solidarité sociale et à la confiance du public. Ces aspirations méritent l'attention sérieuse non seulement des responsables des politiques et des élus, mais aussi des scientifiques, des ingénieurs informatiques — et en fait de toute personne qui utilise un appareil intelligent.

Les enjeux sont importants, mais l'avenir n'est pas écrit.

David Lyon, sociologue, directeur du Centre d'études de la surveillance à la Queen's University, a développé le concept de surveillance en tant que « tri social » et dirige un projet international sur la « surveillance des mégadonnées ».

COVID-19 : Les dérives possibles de surveillance des données personnelles

Benoît Dupont | 24 juin 2020

Si nous n'y prenons garde, le droit à la vie privée pourrait constituer l'une des nombreuses victimes collatérales de la pandémie de Covid-19.

Afin de retrouver une liberté de mouvement temporairement suspendue et dans le but de protéger les populations contre une deuxième vague d'infection, on voit se mettre en place les éléments d'une infrastructure de surveillance dédiée à la santé publique.

Cette infrastructure se compose d'un ensemble de dispositifs de collecte des données personnelles tels que les téléphones intelligents, les caméras de vidéosurveillance, les bracelets connectés, les robots et les drones. Grâce aux innovations réalisées ces dernières années dans les domaines de l'infonuagique, des réseaux de télécommunication et de l'intelligence artificielle, les montagnes de données générées par ces dispositifs peuvent être stockées indéfiniment. Elles sont analysées en temps réel par de puissants algorithmes de surveillance que l'on retrouve dans les applications de traçage ou les logiciels de reconnaissance faciale.

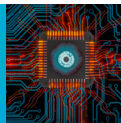
En tant que criminologue spécialisé dans l'étude des transformations numériques et de l'adaptation des mécanismes du contrôle social, je m'intéresse depuis de nombreuses années aux nouvelles formes de surveillance déployées par les gouvernements et les entreprises privées, ainsi qu'aux formes de résistance qui peuvent leur être opposées.

La tentation du techno-solutionnisme

Les technologies qui sous-tendent cette infrastructure ne sont pas nouvelles, et leurs implications dépassent la seule défense du droit à la vie privée, comme l'a souligné dans ces pages mon collègue David Lyon. Elles connaissent au contraire un développement accéléré depuis quelques années sous la pression d'un capitalisme de la surveillance qui cherche à traduire toute expérience humaine en information pouvant créer une valeur marchande pour les entreprises qui la détiennent et savent l'exploiter.

Dans un contexte d'exception où la pandémie a provoqué plus de 350 000 décès à l'échelle mondiale et alors que les systèmes de santé des pays les plus riches ont subi de nombreuses défaillances organisationnelles, un recours à la surveillance comme mode de gestion de la crise sanitaire s'avère séduisant. En effet, comment ne pas succomber aux sirènes d'outils numériques qui promettent d'automatiser la détection des cas suspects et de freiner — voire de stopper net — la propagation du virus, ce qui permettrait à l'économie d'éviter un effondrement généralisé ?

Cette tentation du « techno-solutionnisme », qui privilégie des solutions techniques pour répondre aux problèmes sociaux les plus complexes, comporte toutefois des risques importants. La frayeur collective générée par les ravages du virus n'est-elle en effet pas en train de nous précipiter dans une ère de surveillance totale dont il sera impossible de nous extraire une fois la crise passée et qui sapera de façon durable nos droits fondamentaux ?



La prolifération des outils de surveillance sanitaire

Dans l'attente d'un vaccin, un nombre croissant de pays et d'entreprises mobilisent une vaste panoplie de technologies de surveillance destinées à faciliter le traçage des personnes infectées et à faire respecter les règles de distanciation sociale. Ces applications mobilisent l'attention des défenseurs de la vie privée, mais elles ne représentent que la pointe de l'iceberg de la surveillance sanitaire.

Les pays asiatiques qui ont initialement obtenu les meilleurs résultats dans l'endiguement du virus se sont rapidement appuyés sur un accès massif aux données de téléphonie cellulaire de l'ensemble de leur population : la Corée du Sud a mis en place un système de partage de données unissant 28 organisations, incluant les trois principaux opérateurs télécoms et 22 compagnies de cartes de crédit, qui peut retracer les déplacements d'une personne infectée et ses contacts en moins de 10 minutes.

Les personnes placées en quarantaine à Hongkong doivent porter un bracelet électronique relié à leur téléphone intelligentqui veille à ce qu'elles ne quittent pas leur domicile et alerte la police dès que tout mouvement suspect est détecté. À Singapour, elles ont le devoir de répondre plusieurs fois par jour à des messages textes qui divulguent leur position géographique.

En Chine, une application dont l'usage est obligatoire dans plus de 200 villes et conçue par une filiale de l'entreprise de commerce électronique Alibaba assigne un code de couleur (rouge, jaune ou vert) symbolisant le risque de contagion présumé de chaque usager à partir de données relatives à son adresse résidentielle, ses habitudes de vie, ses symptômes autodéclarés, etc. Les données sont partagées de manière routinière avec la police. La rapidité d'implantation d'une telle solution technique découle directement des initiatives de traçage et de surveillance systématique des citoyens mises en œuvre par le gouvernement chinois dans le cadre de son système de crédit social.

À la mi-mai,une cinquantaine d'applications de traçage étaient ainsi disponibles dans une trentaine de pays. Toutefois, le quart d'entre elles n'avaient pas adopté de politiques de protection de la vie privée et 60 % d'entre elles n'avaient pas implanté de mesures spécifiques d'anonymisation.

De manière plus radicale, Israël a pour sa part enrôlé les capacités de surveillance de son service de renseignement interne, le Shin Bet, afin d'identifier les personnes ayant été en contact avec des patients infectés. À l'aide des données de géolocalisation fournies par les opérateurs de téléphonie mobile dans le cadre de son dispositif de lutte antiterroriste, le Shin Bet aurait localisé environ 4000 personnes qui ont ensuite été testées positives, inaugurant une forme hybride de surveillance mêlant sécurité nationale et santé publique.

Un véritable arsenal technologique

Les entreprises qui souhaitent remettre leurs employés au travail et accueillir leurs clients contribuent également à cette escalade de la soin-veillance.

Des start-up spécialisées en intelligence artificielle proposent des systèmes de vidéosurveillance intégrant des détecteurs de distanciation sociale qui peuvent automatiquement repérer toutes les situations où des personnes se croisent à moins de deux mètres d'intervalle. D'autres intègrent des capteurs thermiques à leurs technologies de reconnaissance faciale afin de mesurer en permanence et sans contact la température corporelle des employés lorsqu'ils circulent dans les locaux de l'entreprise.

Des opérateurs de transport public et privé testent des dispositifs de reconnaissance faciale pour vérifier le port du masque par leurs usagers ou les chauffeurs. Des entreprises manufacturières testent des montres intelligentes ou des badges qui mettent en garde ceux qui les portent chaque fois qu'ils violent les règles de distanciation sociale et construisent des profils de risque des employés.

Drones et robots viennent enfin compléter cet arsenal technologique. De nombreuses villes italiennes, espagnoles, françaises ou américaines ont déployé des drones munis de capteurs thermiques afin de

survoler les espaces publics et repérer les personnes fiévreuses ou violant les règles de confinement, pouvant même utiliser leurs haut-parleurs pour interagir avec celles-ci.

Toujours à la pointe des technologies de surveillance, Singapour expérimente l'usage de chiens robots équipés de caméras et de haut-parleurs pour faire respecter les règles de distanciation sociale dans les parcs publics.

Encadrer l'instauration rampante d'une infrastructure de surveillance totale

Prise séparément, chacune de ces technologies de surveillance apporte une réponse concrète à une menace sanitaire inédite et dévastatrice. Considérées globalement, elles dessinent les contours d'un monde à venir où l'ubiquité d'une surveillance bienveillante s'insinuera dans les replis les plus secrets de nos comportements et de nos habitudes.

Il est également probable que cette soin-veillance perpétuera de nombreuses formes de discrimination découlant de profils de risques dont les critères demeureront opaques, ce qui fragilisera un peu plus les groupes les plus vulnérables.

Loin de constituer un complot mis en œuvre par des forces occultes, la convergence de technologies de surveillance de plus en plus invasives traduit plutôt notre soif intarissable de sécurité et notre croyance aveugle dans la capacité de la technologie à maîtriser l'incertitude.

Mais ce constat ne constitue pas une fatalité dont l'issue nous pousserait vers la paralysie et l'impuissance, bien au contraire. Face au risque réel de voir cette infrastructure de surveillance renforcer son emprise bien au-delà de la pandémie, il devient urgent de débattre et de mobiliser afin de se doter de règles transparentes et strictes visant à restreindre les risques qu'elle fait peser sur nos libertés individuelles et notre solidarité sociale.

Benoît Dupont, criminologue, titulaire d'une Chaire de recherche en cybersécurité à l'Université de Montréal, s'intéresse aux conséquences de la prolifération des technologies de surveillance sur notre société.

Les règles canadiennes en matière de protection de la vie privée en ligne sont à revoir

Anatoliy Gruzd | 19 août 2020

Avec la pandémie, on est davantage coincé à la maison et on a tendance à passer beaucoup plus de temps en ligne en général et sur les médias sociaux en particulier.

Ce n'est pas surprenant, si l'on considère que 99 pour cent des ménages canadiens ont accès à l'Internet à large bande et que 94 pour cent des adultes canadiens en ligne ont un compte sur au moins une plate-forme de médias sociaux, ce qui fait du Canada l'un des pays les plus connectés au monde.

Cependant, plus nous nous servons de ces plates-formes pour aller en ligne et rester en contact avec les gens, plus nous créons de données sur nos intérêts et nos habitudes. Cette mine d'informations sur nous et les personnes de notre réseau peut être utilisée par beaucoup d'organismes, comme les plates-formes de médias sociaux et de nombreuses tierces parties.

Un malaise croissant

Dans ce contexte, il n'est pas surprenant de voir que les utilisateurs de médias sociaux sont de moins en moins à l'aise avec la quantité de données recueillies à leur sujet et la manière dont on peut les exploiter. Dans notre enquête auprès de 1 500 Canadiens, de 65 à 66 % des répondants ont déclaré ne pas être à l'aise avec le fait que des spécialistes du marketing, le gouvernement, des institutions financières et des partis politiques accèdent à des informations publiques les concernant ou qu'ils ont publiées sur les médias sociaux.

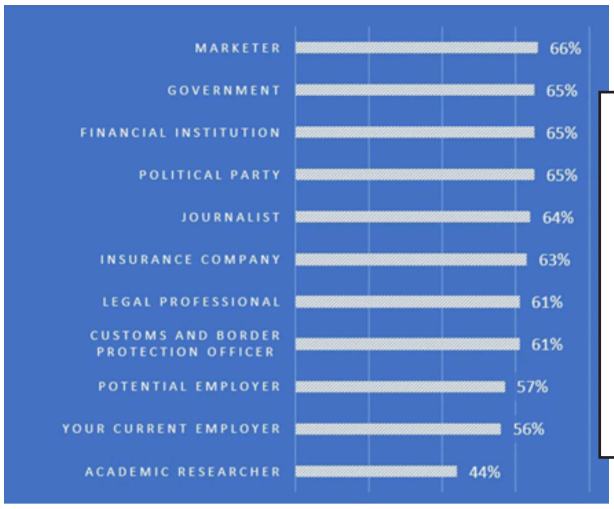


Figure 1. Pourcentage des 1 500 personnes interrogées qui déclarent ne pas être à l'aise avec le fait que des tiers aient accès aux données des médias sociaux qu'elles ont publiées elles-mêmes ou qu'on a publiées à leur sujet.

(Ryerson University Social Media Lab's Social Media Privacy in Canada Report, 2018), Author provided

Ce malaise est l'un des signes nous indiquant que les données en ligne des Canadiens ne sont pas suffisamment protégées en vertu de l'actuelle Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE).

La LPRPDE a 20 ans, et son harmonisation avec les principes de la nouvelle Charte numérique du Canada est l'une des priorités énoncées par notre gouvernement. Cependant, le processus a été retardé d'abord par les élections fédérales et ensuite par la pandémie. Par ailleurs, la pandémie a accéléré le

développement et le déploiement de nouveaux outils et techniques numériques qui reposent sur une grande quantité de données, telles que la recherche de contacts et la reconnaissance faciale, rendant la révision de la LPRPDE plus pressante que jamais.

Une nouvelle réglementation sur la protection de la vie privée et des données devra tenir compte des technologies émergentes et de leurs applications qui seront le moteur de notre économie numérique dans un avenir proche.

Et ailleurs ?

Lorsque l'Union européenne a adopté le règlement général sur la protection des données (RGPD) en 2018, toute une classe de technologies émergentes basées sur la chaîne de blocs s'est retrouvée en conflit avec celui-ci. La chaîne de blocs est la même technologie que celle utilisée pour créer les bitcoins, mais elle ne se limite pas aux cryptomonnaies. Des sites de médias sociaux comme Steemit, Minds et Memo reposent sur la chaîne de blocs et permettent aux utilisateurs d'avoir davantage de contrôle sur leurs données personnelles.

La nature décentralisée de ces sites rend difficile le respect de la RGPD, qui présume qu'il existe un seul responsable du traitement des données (personne physique ou morale) qui collecte les données des individus et veille à leur protection. Dans les réseaux de chaînes de blocs « pair-à-pair », le registre qui stocke toutes les données est distribué sur plusieurs nœuds et n'est pas contrôlé par une entité unique.

En réalité, cela engendre une « responsabilité conjointe », qui n'est pas évidente à appliquer et à interpréter dans le cadre de la RGPD. La conception décentralisée entre également en conflit avec le principe de minimisation des données de la RGPD, qui exige des responsables du traitement des données qu'ils minimisent la quantité et les types de données collectées sur les individus et stockées.

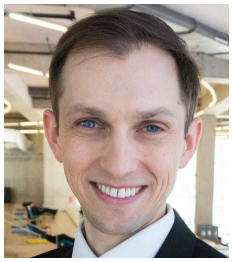
Une autre caractéristique de la chaîne de blocs, qui vise à protéger contre la modification ou la suppression de données, contredit l'article de la RGPD sur le « droit à l'effacement », qui attribue aux personnes le droit de demander la suppression de leurs données personnelles « dans les meilleurs délais ».

Protections futures

La réglementation actuelle nécessite de nouvelles lignes directrices portant sur les groupes de données décentralisées et axées sur l'utilisateur, comme les sites de médias sociaux basés sur la chaîne de blocs. Mais même si la RGPD requiert encore des améliorations, le Canada pourrait tirer quelques leçons de son exemple.

D'abord, il est crucial que la mise à jour de la LPRPDE ne se concentre pas seulement sur les technologies qui existent déjà, mais aussi sur celles que l'on voit poindre à l'horizon. Des technologies émergentes telles que la chaîne de blocs modifient les rapports de force entre les responsables du traitement des données et les utilisateurs en concevant de nouvelles façons de créer, de collecter et de partager leurs données.

Deuxièmement, il est important de comprendre que pour garantir la flexibilité et la reddition de comptes nécessaires pour apaiser les préoccupations des Canadiens concernant l'utilisation de leurs données, il faudra faire preuve de créativité dans la façon d'établir la collaboration entre les utilisateurs, les gouvernements, les fournisseurs de plates-formes, les courtiers en données, les industries axées sur les données, les concepteurs d'applications, les chercheurs et les groupes de la société civile.



Ce faisant, le Canada pourra soutenir la prochaine vague d'innovation numérique tout en protégeant et en renforçant les droits des Canadiens en matière de données.

Anatoliy Gruzd, technologue de l'information, est titulaire d'une Chaire de recherche sur les médias sociaux à la Ryerson University et étudie les impacts des réseaux sur la société moderne.

Les technologies de l'IA, telles que la reconnaissance faciale de la police, discriminent les personnes de couleur

Jane Bailey, Jacquelyn Burkell and Valerie Steeves | 2 septembre 2020

En janvier 2020, la police de Détroit arrêtait à tort Robert Julian-Borchak Williams pour un vol à l'étalage qui avait eu lieu deux ans plus tôt. Même si Williams n'avait rien à voir avec l'incident, le logiciel de reconnaissance faciale utilisé par la police de l'État du Michigan a « fait correspondre » son visage à une image granuleuse obtenue à partir d'une vidéo de surveillance du magasin montrant un autre Afro-Américain en train de s'emparer de montres d'une valeur de 3 800 dollars américains.

Deux semaines plus tard, l'affaire a été classée sans suite à la demande de l'accusation. Cependant, en se basant sur la correspondance erronée, la police avait déjà menotté et arrêté Williams devant sa famille, l'avait forcé à fournir une photo d'identité judiciaire, des empreintes digitales et un échantillon de son ADN, l'avait interrogé et l'avait emprisonné pendant 24h.

Des experts indiquent que le cas de Williams n'est pas isolé et que d'autres personnes ont subi des injustices similaires. La controverse actuelle portant sur l'utilisation de la technologie de Clearview AI par la police souligne indubitablement les risques pour la vie privée que représente la technologie de reconnaissance faciale. Cela étant, il est important de comprendre que nous n'endossons pas tous ces risques de la même manière.

Algorithmes fondés sur le racisme

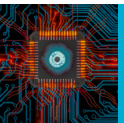
La technologie de reconnaissance faciale qui se fonde et s'accorde sur les visages de Caucasiens identifie systématiquement de manière erronée les personnes racialisées. De nombreuses études rapportent que la technologie de reconnaissance faciale est « imparfaite et biaisée, avec des taux d'erreur nettement plus élevés lorsqu'elle est utilisée à l'égard de personnes de couleur ».

Cette situation porte atteinte à l'individualité et à l'humanité des personnes racialisées qui sont davantage susceptibles d'être identifiées à tort comme des criminels. La technologie - et les erreurs d'identification qu'elle commet - reflète et renforce des divisions sociales qui subsistent depuis longtemps et qui sont profondément ancrées dans le racisme, le sexisme, l'homophobie, le colonialisme et d'autres oppressions croisées.

Catégorisation des utilisateurs par la technologie

Dans son livre révolutionnaire publié en 1993, intitulé The Panoptic Sort, le chercheur Oscar Gandy mettait en garde contre « la technologie complexe impliquant la collecte, le traitement et le partage d'informations sur les individus et les groupes, générées par leur vie quotidienne, et son utilisation en vue de coordonner et de contrôler leur accès aux biens et services qui définissent la vie au sein d'une économie capitaliste moderne ». Les forces de l'ordre s'en servent pour repérer des suspects parmi le grand public, et les organisations privées en font usage pour définir l'accès à des banques ou à l'emploi, entre autres.

Gandy avertissait, tel un prophète, que cette forme de « tri cybernétique » désavantagerait de façon exponentielle, si elle n'était pas sous contrôle, les membres des communautés en quête d'égalité,



telles que les groupes racialisés ou désavantagés sur le plan socio-économique, à la fois en termes d'attribution et de compréhension.

Environ 25 ans plus tard, nous vivons aujourd'hui avec le tri panoptique des stéroïdes. Les exemples de ses effets négatifs sur les communautés en quête d'égalité abondent, tels que l'identification erronée de Williams.

Préjugés préexistants

Ce tri par algorithmes s'infiltre dans les aspects les plus fondamentaux de la vie quotidienne, engendrant dans son sillage une violence à la fois directe et structurelle.

La violence directe vécue par Williams est immédiatement visible dans les événements entourant son arrestation et sa détention, les préjudices individuels qu'il a subis sont évidents et leurs origines remontent aux actions de la police qui a choisi de se fier à la « correspondance » de la technologie pour procéder à une arrestation. Plus insidieuse est la violence structurelle perpétrée par la technologie de reconnaissance faciale et d'autres technologies numériques qui évaluent, comparent, catégorisent et trient les individus de manière à amplifier les modèles discriminatoires préexistants.

Les préjudices causés par la violence structurelle sont moins évidents et moins directs, et portent préjudice aux groupes en quête d'égalité par un déni systématique du pouvoir, des ressources et des opportunités. Parallèlement, elle augmente les risques et les préjudices directs pour les individus appartenant à ces groupes.

La police prédictive utilise le traitement par algorithmes de données historiques pour prévoir quand et où de nouveaux délits sont susceptibles de se produire, affecte les ressources policières en conséquence et intègre une surveillance policière renforcée dans les communautés, généralement dans les quartiers à faibles revenus et racialisés. Cette situation augmente la détection et la sanction des activités criminelles, y compris les activités criminelles moins graves qui pourraient, dans d'autres circonstances, ne pas susciter de réaction de la part de la police, ce qui, en fin de compte, limite les chances de réussite des personnes vivant dans cet environnement.

De plus, les preuves d'inégalités dans d'autres secteurs continuent de s'accumuler. Des centaines d'étudiants au Royaume-Uni ont manifesté le 16 août dernier contre les résultats désastreux d'Ofqual, un algorithme défectueux utilisé par le gouvernement britannique pour déterminer quels étudiants seraient admissibles à l'université. En 2019, le service d'annonces de microciblage de Facebook a aidé des dizaines d'employeurs des secteurs public et privé à exclure des personnes de leurs listes de destinataires d'offres d'emploi sur la base de l'âge et du sexe. Des recherches menées par ProPublica ont documenté la discrimination des prix en fonction de la race pour les produits en ligne. En outre, les moteurs de recherche produisent régulièrement des résultats racistes et sexistes.

Perpétuation de l'oppression

Ces résultats sont importants car ils perpétuent et creusent les inégalités préexistantes fondées sur des caractéristiques telles que la race, le sexe et l'âge. Ils sont également importants parce qu'ils influencent profondément la façon dont nous apprenons à nous connaître et à connaître le monde qui nous entoure, parfois en présélectionnant les informations que nous recevons de manière à renforcer les perceptions stéréotypées. Les entreprises technologiques elles-mêmes reconnaissent l'urgence d'empêcher la perpétuation de la discrimination par les algorithmes.

Jusqu'à présent, les enquêtes ponctuelles menées par les entreprises technologiques elles-mêmes ont connu un succès irrégulier. Les entreprises impliquées dans la production de systèmes discriminatoires les retirent parfois du marché, comme lorsque Clearview AI a annoncé qu'elle ne proposerait plus de technologie de reconnaissance faciale au Canada. Cela étant, de telles décisions résultent souvent d'un examen réglementaire ou d'un tollé public mené à la suite des préjudices subis par des membres des communautés en quête d'égalité.

Il est temps de donner à nos institutions de régulation les outils dont elles ont besoin pour s'attaquer au problème. Les simples protections de la vie privée qui reposent sur l'obtention du consentement individuel pour permettre aux entreprises de saisir et de réutiliser les données ne peuvent être isolées des résultats discriminatoires de cette utilisation. Cela est particulièrement vrai à une époque où la plupart d'entre nous (y compris les entreprises technologiques elles-mêmes) ne peuvent pas comprendre pleinement le fonctionnement des algorithmes ou pourquoi ils produisent des résultats spécifiques.

La vie privée est un droit de la personne

Une partie de la solution consiste à briser les silos réglementaires actuels qui traitent la vie privée et les droits de la personne comme deux entités distinctes. S'appuyer sur un modèle de protection des données fondé sur le consentement va à l'encontre du principe fondamental selon lequel la vie privée et l'égalité sont deux droits de la personne qui ne peuvent être dissociés.

Même la Charte canadienne du numérique, la dernière tentative du gouvernement fédéral pour répondre aux lacunes de l'état actuel de l'environnement numérique, maintient ces distinctions conceptuelles. Elle traite la haine et l'extrémisme, le contrôle et le consentement, et une démocratie forte comme des catégories distinctes.

Pour remédier à la discrimination par algorithmes, nous devons reconnaître et structurer la vie privée et l'égalité en tant que droits de la personne. Nous devons également créer une infrastructure à la fois attentive et experte dans les deux domaines. Sans efforts de cette envergure, l'éclat des mathématiques et de la science continuera à camoufler les préjugés discriminatoires de l'IA, et l'on peut s'attendre à une multiplication des expériences telles que celle infligée à Williams.

Jane Bailey, professeure de droit à l'Université d'Ottawa, codirige le projet eQuality et étudie l'impact des technologies évolutives sur l'égalité, la vie privée et les droits, en particulier pour les membres des communautés en quête d'égalité.

Jacquelyn Burkell, membre de la faculté des études sur l'information et les médias à la Western University, étudie l'impact social de la technologie, en mettant l'accent sur la vie privée, l'accès à l'information et la technologie dans le contexte de la justice.

Valerie Steeves est professeure titulaire au sein du département de criminologie de l'Université d'Ottawa. Elle codirige le projet eQuality et effectue des recherches sur les expériences des jeunes en matière de vie privée et d'égalité dans les espaces virtuels.

The Royal Society of Canada
282 Somerset Street West
Ottawa, Ontario K2P 0J6
www.rsc-src.ca
613-991-6990

La Société royale du Canada
282, rue Somerset ouest
Ottawa (Ontario) K2P 0J6
www.rsc-src.ca
613-991-6990