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.

RSC SRC

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.

La SRC a créé un groupe de travail sur l'infoveillance en charge de l'examen des répercussions de la surveillance, des données, de la vie privée et de l'égalité. Le groupe de travail a commencé à analyser la transition des notions individualistes de « protection de la vie privée » à l'arrivée du capitalisme de surveillance, qui désigne un système économique d'accumulation fondé sur la marchandisation des données personnelles. Le capitalisme de surveillance présente de nombreuses caractéristiques, notamment la mise en données (action sociale transformée en données quantifiées), le dataïsme (croyance naïve en la capacité des données à résoudre les problèmes humains), la surveillance des données (utilisation des données pour la surveillance des populations et des individus) et le profilage discriminatoire (avec des implications particulières pour les personnes issues de communautés déjà marginalisées).

Les membres du groupe de travail sont : Jane Bailey (Université d'Ottawa) ; Benoît Dupont (Université de Montréal) ; Anatoliy Gruzd (Ryerson University) ; et David Lyon (Queen's University).