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 ?

RSC SRC

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.

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).