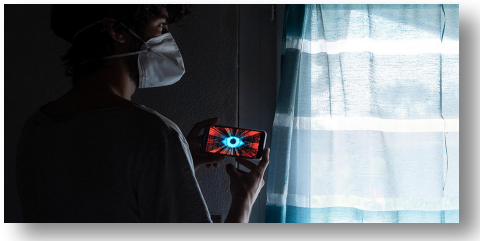
CNRS LE JOURNAL
Donner du sens à la science

Numérique
Sociologie
24.04.2020, par
Lydia Ben Ytzhak

"Il n'existe pas d'application capable de remplacer une politique de santé publique"

Le sociologue Antonio A. Casilli nous livre son regard sur l'utilisation d'outils numériques par de nombreux pays pour accompagner le déconfinement.



Valentino BELLONI / Hans Lucas / Hans Lucas via AFP

Membre de l'Institut interdisciplinaire de l'innovation et chercheur associé à l'Institut interdisciplinaire d'anthropologie du contemporain, vous étudiez depuis 2009 les effets des plateformes et des outils numériques sur la société et la vie privée. Alors que l'on commence à préparer le déconfinement en France, quels sont les différents scenarii observés dans le monde ?

☛ **Antonio Casilli** : La première possibilité est de ne suivre que les personnes infectées et d'en restreindre la circulation. C'est le cas en Corée du Sud où les itinéraires des personnes contaminées sont reconstruits grâce aux données des mobiles et des cartes bleues. Hong Kong, quant à lui, impose désormais des véritables bracelets électroniques pour assurer le respect de la quarantaine par les personnes venant de l'étranger.

Ensuite, il y a la possibilité de suivre tout le monde. En Chine, cela a été réalisé via les données de géolocalisation des citoyens de Wuhan, obtenues par les télécoms d'État. De son côté, Singapour a mis en place une application, TraceTogether, basée sur le Bluetooth. Même si elle ne géolocalise pas les usagers, elle relève toutes les personnes croisées sur une période de 14 jours. Elle a été très faiblement adoptée, par 12 % de la population. Impossible donc d'en évaluer l'efficacité contre le virus. La France, à l'instar d'autres pays européens, s'oriente vers cette même technologie, avec une application Bluetooth, StopCovid, dont l'installation serait volontaire mais qui aurait vocation à être adoptée par tout le monde, et pas seulement les personnes en quarantaine.

Système visualisant les données de géolocalisation recueillies pour lutter contre le coronavirus. - Abdesslam MIRDASS / Hans Lucas / Hans Lucas via AFP

Les scenarii de déconfinement sont multiples, et assez cohérents avec les orientations politiques de chaque pays. En France, on assiste par exemple depuis longtemps à une baisse importante des dépenses publiques dans certains secteurs retenus non stratégiques, et notamment dans la santé publique. L'exécutif a promis un plan massif d'investissement pour l'hôpital, mais pourrait aller plus loin dès à présent en misant plutôt et entièrement sur la consolidation des moyens à disposition des personnels soignants.

Le recours au pistage numérique n'est-il pas indispensable pour organiser un déconfinement ?

☛ En vérité, **la question de la surveillance numérique et celle du déconfinement sont entièrement décorrélées** : cantonner le numérique à des fins de surveillance est un choix politique. Pour moi, le succès du déconfinement est d'abord une question d'investissements dans des dépenses de santé publique, permettant de réaliser des tests massifs, de doter tout le monde de masques et d'optimiser la gestion de lits d'hôpitaux. Dans l'idéal, on pourrait ainsi imaginer un numérique au service du référencement de ces éléments, par exemple une application officielle qui permettrait de savoir combien de tests sont disponibles et où les effectuer autour de moi.

Il a été décidé d'aller dans un sens différent qui fait passer le pistage des êtres humains avant le dépistage de la maladie. C'est une tendance à la généralisation de la surveillance électronique qui se dessine depuis deux décennies, mais qui se retrouve aujourd'hui dans des expériences menées partout dans le monde au nom de la lutte contre le Covid-19.

Mais nous sommes en état d'urgence sanitaire et nos déplacement sont déjà contrôlés. En quoi cette surveillance numérique serait-elle selon vous si problématique ?

☛ A. C. : Avec le confinement, nous avons fait l'expérience d'une assignation à résidence collective ; avec les applications de surveillance, nous risquons d'assister à la banalisation du bracelet électronique. Autrement dit : si la surveillance numérique est la condition pour recommencer à circuler dans l'espace public, nous ne sommes pas face à la fin d'une restriction temporaire de nos libertés, mais à la continuation du confinement par d'autres moyens.

Un passager munis d'un bracelet électronique après avoir été testé au COVID-19 à l'aéroport de Hong Kong - ISAAC LAWRENCE / AFP

Or, rendre visible dans l'espace public les personnes malades comporte des risques, avec différentes dérives possibles.

En Chine, il existe ainsi une application de livraison de repas qui affiche la température des coursiers. En Corée du Sud, on a vu la prolifération d'applications non officielles qui permettent le traçage ciblé de personnes positives au virus, avec tous les risques de harcèlement que cela induit. Par exemple, l'appli "Corona 100m" vous permet de savoir si autour de vous quelqu'un a été déclaré positif au Covid-19.

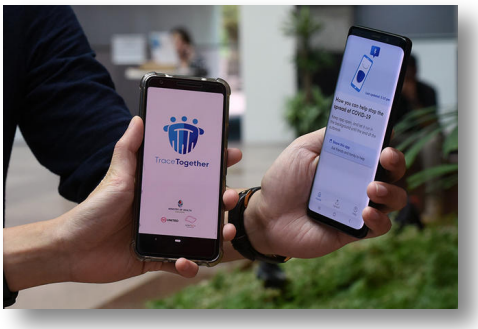
Outre la violation du secret médical, cette information est inutile puisqu'elle ne dit même pas si cette personne est encore contaminante, ou désormais immunisée...

Et puis pour chaque usage, des problèmes importants de consentement des usagers se posent. Lorsque par exemple des start-up proposent de construire des cartographies de la mobilité des Français au temps du Covid-19 en récupérant à notre insu les données d'applications en apparence aussi anodines qu'un jeu sur mobile ou des applis GPS, comment être sûr que ces mouchards respectent bien la loi ?

Justement quelle est plus précisément la voie envisagée en France ?

☛ A. C. : Le déploiement en Europe du "tracking", utilisé dans de nombreux pays où il permet grâce aux données mobiles ou à la reconnaissance faciale de suivre les déplacements des personnes et de mettre une amende en cas d'éloignement du domicile, n'est pas facile en Europe à cause des législations comme le Règlement général sur la protection des données (RGPD) et la directive ePrivacy. De même, l'utilisation des données de géolocalisation (la liste des antennes-relais auxquelles nos téléphones se connectent au fil de la journée) a été proposée par certains acteurs de télécommunications comme Orange. **Quels que soient les efforts pour anonymiser ces données, ceci est impossible une fois qu'elles ont été collectées**.

Ce que proposent Google et Apple et qui est sérieusement débattu en France est un système de "contact tracing" par Bluetooth. Là, si vous êtes testé positif, toutes les personnes qui auront été à proximité de votre smartphone recevront une notification du type : "au cours des deux dernières semaines vous avez été en contact avec une personne contaminée". Il s'agit de la version numérique d'une méthode qui existait bien avant l'arrivée des smartphones et qu'utilisaient les soignants pour enquêter sur les chaînes de contaminations en cas d'épidémie de tuberculose par exemple, et prévenir les personnes concernées si besoin.



L'application de "contact tracing" par Bluetooth TraceTogether a été déployée à Singapour à partir du 20 mars 2020. - Catherine LAI / AFP

Confier cette mission à une application mobile élimine le discernement des professionnels et introduit un fort risque de faux positifs. Si j'oublie le smartphone dans mon manteau, toute personne qui passe à proximité sera-t-elle notifiée ? Cela pourrait rendre le système inefficace.

De plus, il deviendra possible de discriminer les personnes qui n'installeront pas l'application ; ce qui constitue un risque notable en termes de libertés publiques. Imaginez qu'une telle application soit obligatoire pour monter dans les bus. Cette obligation pourrait être étendue indéfiniment, tout comme le plan Vigipirate, qui à l'origine devait être limité dans le temps. D'où l'importance d'avoir maintenant un débat au Parlement sur ce sujet .

N'est-il pas possible d'établir des garde-fous pour limiter les atteintes aux libertés et à la vie privée ?

☛ A. C. : **On peut les limiter, oui, mais pas les éliminer**. En France on envisage que l'application StopCovid produise des pseudonymes, des identifiants éphémères. De cette manière si je croise un individu, mon smartphone ne détecte pas son identité. Mais ces pseudonymes devraient être envoyés à une base de données centralisée. Et c'est là que, selon des experts en informatique, une ré-identification reste possible. En effet, dès que vous êtes déclaré positif, les personnes dans votre entourage sont informées; sous certaines conditions, ceci peut suffire à retrouver votre identité. Par ailleurs, ce genre d'application est très vulnérable au piratage et aux détournements: on peut notamment imaginer l'apparition d'applications "parasites" capables de croiser les données Bluetooth avec d'autres informations, voire des "blagues" informatiques où des plaisantins s'amuseraient à désanonymiser les identifiants de leurs voisins et de leurs connaissances testées positives.

Voulons-nous vraiment abolir le secret médical ? Il faut casser ce modèle dystopique auquel le discours ambiant semble nous avoir destinés.

Cette surveillance numérique est présentée comme inéluctable, alors qu'elle peut s'avérer inefficace, discriminatoire et atteindre la vie privée des citoyens si on ne permet pas aux citoyens de protéger leur vie privée et la confidentialité de leurs informations médicales.

En réalité, il ne s'agit pas de lutter contre une maladie difficile à détecter en renonçant à nos libertés, mais en nous efforçant de la détecter ! La question centrale est celle des tests, des masques et du nombre de lits d'hôpitaux, et il n'existe pas d'application "magique" capable de remplacer une solide politique de santé publique. ♦

❐ Antonio Casilli est chercheur à l'Institut interdisciplinaire de l'innovation (I3 – CNRS/École polytechnique/Mines ParisTech/Telecom Paris) et chercheur associé à l'Institut interdisciplinaire d'anthropologie du contemporain (IIAC - CNRS/EHESS).