Un peu partout s'accélère la mise en place d'un État de surveillance sociale et numérique, présenté comme une réponse impérative et inévitable à la crise du coronavirus. Ainsi s'impose l'idée qu'il faudrait sacrifier la protection de notre vie privée pour la santé publique. Comment affronter cette dynamique autoritaire qui se drape dans l'objectif, en lui-même incontestable, de sauver des vies ?

Dans cet article, Lucas Malaspina défend l'idée que pour le camp de l'émancipation, l'unique manière effective d'empêcher les abus des gouvernements et des entreprises n'est pas de refuser de façon abstraite l'utilisation des Big Data en santé publique, mais bien de construire une connaissance collective précise et exhaustive du sujet. Cet article est un modeste effort dans cette direction.

***

La crise mondiale provoquée par le coronavirus constitue un des événements les plus significatifs de l'histoire de l'humanité. La capacité à limiter les morts causées par des maladies infectieuses est au fondement du développement humain à partir du XIX^{ème} siècle et, en particulier, du développement urbain, du commerce mondial et du système capitaliste lui-même. Jamais le monde n'a été aussi connecté qu'aujourd'hui. Dans le même temps, l'ordre du monde (y compris ses dimensions numériques) n'a jamais été aussi autant remis en question.

Il y a deux semaines, le penseur coréen Byung-Chul Han déclarait, dans une retentissante tribune publiée dans *El País* : « La Corée du Sud a déjà surmonté la pire phase, comme le Japon. La Chine elle-même, pays d'origine de la pandémie, a la situation sous contrôle ». Le philosophe est convaincu que « pour combattre le virus, les asiatiques misent fortement sur la surveillance numérique » et que « en Asie, les épidémies ne sont pas seulement combattues par les virologues et les épidémiologistes, mais surtout par les informaticiens et les spécialistes en big data. C'est un changement de paradigme dont l'Europe ne s'est toujours pas aperçue ».

Tandis que la Chine et d'autres pays asiatiques sont en train de maîtriser le virus, les États-Unis s'approchent dangereusement d'un effondrement sanitaire et l'Europe a été incapable de réagir de manière coordonnée. Les situations de crise engendrent et stimulent l'autoritarisme et de nombreuses formes d' « états d'exception ».

L'expérience chinoise et le contrôle sanitaire

Le problème est sur la table. Le coronavirus pourrait marquer le début d'une ère de surveillance numérique intense dans le domaine de la santé, puisqu'il est ainsi possible de suivre très précisément la propagation des maladies.

La Chine a utilisé les données des opérateurs nationaux de téléphonie mobile pour localiser les personnes qui ne respectaient pas la quarantaine. Les principales entreprises du secteur des nouvelles technologies, comme Alibaba, ont développé des applications qui sont capables de trier les personnes en fonction leur historique de déplacement et de leur degré potentiel d'exposition au virus. Pour contenir la diffusion de l'épidémie, la Chine a également eu recours à des caméras thermiques qui prennent à distance la température des personnes. Elles ont été utilisées à Wuhan dès janvier, puis, entre autres, dans des villes comme Beijing, Shanghai et Shenzhen. Actuellement, elles sont utilisées comme des

outils de détection et d'alerte dans les aéroports afin de contenir l'avancée du coronavirus. Dans une atmosphère contrôlée, leur marge d'erreur pour la mesure des températures corporelles est de 0,3 degrés. Depuis le début du mois de mars, elles sont également installées à l'aéroport d'Ezeiza, à Buenos Aires [où l'auteur de cet article réside].

Ces mesures nous garantissent-elles le succès dans notre combat contre le virus ? C'est une des dimensions essentielles de la question. Ce qui est certain, sans réduire les politiques de santé à la mise en œuvre de telle ou telle technologie, c'est que ces dernières ont eu une forte influence sur les différentes évolutions épidémiologiques. Leurs utilisations, de fait, alimente l'imagination politique du reste du monde. L'usage des technologies de surveillance en Asie afin de freiner l'épidémie de COVID-19 est d'ores et déjà un facteur objectif qui pèse sur les prises de décisions politiques et économiques, publiques et privées, en l'Occident.

L'exemple de la Corée du Sud et les *coronapps*

Outre la situation chinoise, la presse occidentale a mis en avant les dispositifs élaborés par la Corée du Sud et, dans une moindre mesure, les expériences également couronnées de succès de Hong Kong, de Taïwan, de Singapour ou du Vietnam. Ces pays partagent une même expérience cruciale : la lutte contre l'épidémie de SRAS en 2003. Cela explique la plus grande préparation de leurs gouvernements face à la survenue d'une nouvelle épidémie.

En ce qui concerne la Corée du Sud, un article affirmait récemment : « la technologie constitue le complément parfait d'une équipe d'agent·es dédié·es à retracer l'itinéraire du virus et à tester chaque cas : « identifier et tester » est le mort d'ordre ». Par conséquent, le succès de la politique sud-coréenne ne s'appuie pas uniquement sur l'utilisation de la technologie pour réaliser une « carte de chaleur » de l'épidémie : elle repose également sur l'organisation de dépistages à grande échelle. En 2015 et 2018, les lois sur la protection des données personnelles dans le cadre de l'urgence sanitaire ont été modifiées. « La décision de recourir aux données de géolocalisation a alors été prise dans une réunion inter-ministérielle » explique Chris Lee, chercheur pour la société de conseil coréenne 2e Digital Lab et directeur de la branche nationale de l'ONG MyData. En Corée du Sud, « chaque cas positif fait l'objet d'une investigation. Si la déclaration personnelle est incomplète ou si la personne refuse de la faire, le Ministère de la Santé a le pouvoir de demander l'usage des données de ses cartes bancaires et du GPS de son téléphone portable. »

« Il y a beaucoup d'applications pour rechercher les cas et toutes sont privées. En Corée du Sud, aucune application publique ne retrace automatiquement les contacts d'un·e citoyen·ne malade. C'est le gouvernement qui obtient et publie les données, mais il les met à disposition pour que des entreprises ou des citoyen·nes les diffusent sur le web ou à travers des applications » assure Chris Lee. Cela a entraîné de nombreux problèmes liés à la vie privée (comme des infidélités ainsi révélées ou des mensonges dans le milieu professionnel finalement dévoilés) puisque, bien que l'information soit anonyme, il est possible d'inférer de qui il s'agit en croisant l'historique des localisations avec d'autres données. La Corée du Sud dispose d'un logiciel – qui inclut une application – pour effectuer le suivi de la quarantaine obligatoire des cas positifs. Un·e assistant·e social·e est assigné·e à ces malades. « Cette application, elle, est très clairement intrusive : elle surveille la

quarantaine à travers la localisation et elle assiste médicalement le patient, à distance, si son hospitalisation n'est pas nécessaire ».

L'exemple de la Corée du Sud a été perçu comme une opportunité par différents acteurs. Parmi eux se trouvent les *lobbies* des entreprises du secteur des nouvelles technologies et les gouvernements de nombreux pays, avec des intentions plus ou moins affichées. Cela a engendré une fièvre des *coronapps* à l'échelle mondiale, qui a également touché l'Amérique latine. Diverses variantes de *coronapps* se sont propagées au Honduras, en Uruguay, en Bolivie, en Colombie, en Argentine, au Guatemala, au Brésil, en Équateur et au Mexique ; dans le cas de ces trois derniers pays notamment, le Centre latino-américain de Droits Numériques a tiré le signal d'alarme.

Épidémiologie et droits humains

Des épidémiologistes disent que le recueil des contacts se transformera en une arme vitale pour contenir de futurs foyers du coronavirus, une fois que la fermeture des frontières nationales auront freiné la rapide propagation du virus. Selon le journaliste spécialisé Bryan Walsh, « les épidémiologistes peuvent affirmer faire partie des premiers scientifiques à avoir utilisé des bases de données, depuis que John Snow a ainsi découvert la source d'une épidémie de choléra à Londres en 1854 » (Snow est aussi un des précurseurs de la cartographie des données).

L'économie mondiale est déjà très fortement ébranlée. L'extension du confinement implique des coûts sociaux difficiles à surmonter, en particulier pour les pays les plus fragiles. L'utilisation de nouvelles technologies se présente alors à leurs gouvernements comme l'alternative la plus efficiente. « Aux États-Unis et dans les autres pays occidentaux, ces tentatives rencontreraient sans doute d'importantes barrières éthiques, légales et réglementaires », comme l'a suggéré Scott Rosenberg, analyste pour Axios.

Israël constitue une évidente exception. Le gouvernement de Benjamin Netanyahu a accordé des pouvoir d'urgence au Shin Bet (l'agence de renseignement intérieur) afin d'utiliser une technologie de collecte de données développées pour combattre le terrorisme en lui donnant une finalité nouvelle : suivre les mouvements des patient·es infecté·es par le coronavirus et des personnes qui ont été à leur contact. A travers cet outil, on leur fait parvenir des messages les obligeant à s'isoler. En faisant cela, l'État a révélé que le Shin Bet disposent des métadonnées des téléphones mobiles de tou·tes ses citoyen·nes depuis 2002 au moins, comme l'a signalé un article du *New York Times*.

Dans le même temps, l'entreprise israélienne NSO a commercialisé une application « d'usage civil » pour combattre le coronavirus, ne nécessitant donc pas de permis d'exportation délivré par le Ministère de la Défense. NSO a bâti sa réputation grâce à Pegasus, un logiciel sophistiqué d'espionnage accusé de violation de la vie privée et d'atteinte aux droits humains, qui s'introduit dans les téléphones par l'intermédiaire d'un lien envoyé par SMS, qui prend le contrôle sur toutes les communications (messages chiffrés compris) et envoie l'ensemble de ces informations à son client. Selon une source de *Bloomberg*, le nouveau logiciel de NSO « s'empare de deux semaines d'informations issues du téléphone de la personne infectée, le temps d'incubation du virus, et la croise ensuite avec les données de localisation archivées par les compagnies nationales de télécommunication, afin d'identifier les personnes qui ont été à proximité du patient pendant plus de 15 minutes et ont potentiellement été infectées ». Amnesty International a

demandé à Israël de révoquer la licence d'exportation du logiciel, mais il est déjà en phase de test dans 12 pays au moins.

Comme l'affirme María Paz Canalez, on doit établir une distinction claire – bien qu'il soit parfois difficile de le faire – entre la surveillance de la propagation du virus et la surveillance des personnes qui le véhiculent. De plus, elle soutient que « les droits fondamentaux sont des exercices de pondération, de là découle la nécessité que chaque restriction de l'exercice de ces droits soit proportionnée et qu'elle n'affecte pas l'essence du droit restreint ».

Le panorama de la situation aux États-Unis

Aussi bien Walsh que Rosenberg soutiennent que la géolocalisation ne pourrait jouer qu'un rôle très limité dans cette étape de l'épidémie, tout du moins aux États-Unis. Rosenberg souligne qu' « aucune quantité de données de géolocalisation ne peut compenser les données infectiologiques qui manquent » – c'est-à-dire la possibilité de déterminer qui est porteur·se du coronavirus et qui ne l'est pas. La précision du GPS est de 4,5 mètres, il peut ainsi permettre de savoir si quelqu'un·e est sorti·e de l'isolement et est allé·e de son domicile à un autre lieu, mais il ne permet pas de déterminer si cette personne a maintenu les distances physiques nécessaires. Selon lui, la géolocalisation peut servir pour suivre la propagation du virus, mais les tests de dépistage, la recherche d'un vaccin et les respirateurs artificiels ont un rôle bien plus important à jouer dans la lutte contre l'épidémie.

Malgré cela, selon un article du *Washington Post*, Google, Facebook et d'autres géants du numérique sont en train de négocier avec Donald Trump la manière de mobiliser les données de géolocalisation pour participer à la lutte contre le coronavirus. Au début du mois de mars, Trump a provoqué une immense déception, après avoir fait courir le bruit, lors d'une conférence de presse, que Google était en train de collaborer avec le gouvernement pour construire dans l'urgence un site web qui orienterait les personnes vers les lieux de dépistage les plus proches. Google a dû le démentir et clarifier la situation. Il s'agissait de Verify, un site dédié aux questions de santé, appartenant à Google et disponible uniquement dans la baie de San Francisco (Californie). Google a finalement lancé un site, mais il permet seulement de visualiser le nombre de cas par pays ou par région et il ne comporte absolument pas la fonctionnalité présentée par Trump. Google propose également des rapports par pays sur les mouvements de population au fil du temps, à partir de données anonymisées et agrégées, obtenue par Google Maps.

Un des principaux outils des États-Unis est le « thermomètre intelligent » de l'entreprise Kinsa, un avatar du fameux « internet des objets ». Les thermomètres de Kinsa chargent les températures de l'utilisateur·trice dans une base de donnée centralisée. « Depuis 2008, lorsque déjà plus de 500 000 thermomètres été distribués, ses prédictions ont habituellement deux ou trois semaines d'avance sur celles des Centres pour le Contrôle et la Prévention des Maladies ». Aujourd'hui, Kinsa a adapté son logiciel afin d'aider à la détection du coronavirus. Grâce aux données qu'elle collecte, Kinsa peut en effet élaborer une « carte de chaleur » qui met en évidence la progression de la fièvre dans le pays, tout du moins en ce qui concerne ses propres utilisateur·trices.

Pendant ce temps, les lobbyistes qui représentent les géants comme Google et Facebook ont demandé au procureur général de Californie « qu'il attende pour mettre en application

les nouvelles règles de protection des données personnelles sur internet, compte tenu de la pandémie de coronavirus qui frappe le monde ».

Pour sa part, le gouvernement de Trump est en train de retirer certaines règles de protection du secret médical, qui concernent les milliers d'entreprises ayant accès aux données personnelles de santé. Il s'agit d'une exemption afin que ces entreprises puissent utiliser ces informations pour leur propre compte, ou les transmettre directement à un large panel d'agences gouvernementales, tant que l'entreprise le fait « de bonne foi » et « pour des activités de santé publique ou de contrôle de la santé ». Parmi ces entreprises se trouve Google, qui « en août 2018 a signé un contrat avec Ascension, une chaîne de 2600 hôpitaux, cabinets et autres services médicaux, dont le siège est à Saint-Louis ». Ceci a octroyé à Google « l'accès aux données médicales détaillées de millions d'états-unien·nés dans 21 États ».

Dans ce paysage, les propositions de Tristan Harris (ancien « éthicien du design » chez Google et fondateur du Center for Humane Technology), une des voix critiques de la Silicon Valley, sont assez déconcertantes. Harris l'assure : « de la même manière que nous avons invoqué l'état de guerre pour réorienter l'industrie vers la production de fournitures médicales », Google et Facebook doivent être plus agressives dans la lutte contre le coronavirus. Dans une tribune pour *Wired*, il propose de modifier leurs algorithmes afin de rendre le danger de l'épidémie et sa possible évolution plus sensibles, de persuader les utilisatrices·eurs de respecter les consignes de prévention – en utilisant l'analyse de leur activité en ligne pour identifier et cibler celles et ceux qui ne les respectent pas – mais aussi d'utiliser l'information qui circule sur les plateformes pour organiser la solidarité, répartir les aides et approvisionnements. En somme, il propose de laisser les GAFAM manipuler à grande échelle ses concitoyen·nes pour lutter contre l'épidémie.

Protection des données personnelles ou santé publique : une fausse dichotomie

Dans la tribune citée précédemment, Byung-Chul Han s'est aventuré à déclarer : « En apparence, le *big data* est plus efficace pour combattre le virus que les absurdes fermetures de frontières qui se pratiquement actuellement en Europe. Néanmoins, en raison de la protection des données, une lutte contre le virus similaire à celle menée en Asie n'est pas possible ». Evgeny Morozov a quant à lui affirmé sur Twitter que « si le remède ne peut pas être pire que la maladie, les applications, elles, peuvent bel et bien l'être ». Mais devons-nous pour autant renoncer à l'utilisation des applications et des autres outils technologiques simplement parce qu'ils peuvent *potentiellement* être pires que la maladie ?

Certains développements en cours s'opposent à l'idée que l'usage de ces nouvelles technologies devrait être rejeté catégoriquement. Une étude du Big Data Institute de l'Université d'Oxford certifie qu' « une application de recherche des contacts (*contact tracing*) qui crée un mémoire des contacts de proximité et notifie immédiatement les contacts avec des personnes porteuses du virus peut permettre le contrôle de l'épidémie si elle est utilisée par suffisamment de personnes. En ciblant uniquement les personnes potentiellement infectées pour la mise en place des mesures de prévention, les épidémies pourraient être contenues sans recourir à des confinements massifs qui portent préjudice à la société ». Le Big Data Institute explique que cela ne peut fonctionner que si au moins

60 % de la population d'un pays participe à ce *contact tracing*.

En ce sens, il faudrait suivre attentivement le développement de l'initiative baptisée Seguimiento Paneuropeo de Proximidad para Preservar la Privacidad (PEPP-PT), à laquelle participent notamment l'Instituto Fraunhofer Heinrich Hertz (HHI) en Allemagne et plus de 130 chercheur·ses de 8 pays, en collaboration avec l'opérateur téléphonique Vodafone. PEPP-PT s'inspire de l'utilisation fructueuse des téléphones portables dans quelques pays d'Asie pour suivre la diffusion du virus et faire respecter les ordres de quarantaine. La plateforme PEPP-PT ferait un usage anonyme de la technologie Bluetooth à basse consommation, en respectant le règlement général sur la protection des données (RGPD) de l'Union européenne, et il n'impliquerait pas la collecte des données de géolocalisation (c'est pourquoi ce dispositif est moins intrusif que le recours au GPS ou aux connexions sur les antennes-relais de téléphonie mobile). Les personnes ne disposant pas d'un téléphone compatible pourraient utiliser des bracelets Bluetooth. PEPP-PT, qui suit le modèle de l'application TraceTogether de Singapour, enregistrerait les connexions réalisées entre téléphones intelligents dans des dispositifs décentralisés, pendant deux semaines, en utilisant un chiffrage sûr. Seules les autorités sanitaires locales pourraient télécharger les données collectées par l'application, pour demander aux personnes potentiellement infectées de s'isoler.

Il est nécessaire de dépasser la logique des gouvernements, des entreprises et des citoyen·nes-consommateur·trices pour mettre en place un système d'analyse et de contrôle de ces nouveaux programmes, dans lequel les organisations collectives aient la possibilité de veiller effectivement à leur bon fonctionnement et au respect des droits humains. Pour ce faire, les diverses organisations de la société civile doivent tisser des liens étroits avec des spécialistes de ces technologies qui partagent leurs valeurs et leurs inquiétudes, afin de pouvoir évaluer précisément ce dont il s'agit, d'utiliser leur pouvoir dans la gestion de crise et d'intervenir auprès du grand public. Sans cela, celles et ceux qui doutent des recettes technologiques magiques risquent de devoir s'abstenir systématiquement d'utiliser des outils utiles dans la lutte contre le coronavirus.

Ainsi, nous qui défendons le respect des droits humains dans le champ de la technologie, nous devons trouver une manière de débattre concrètement de la conception de ces dispositifs. En effet, si un dispositif ou un outil technologique (une application ou tout autre sorte de logiciel) remplit une fonction socialement utile (ici, éviter la propagation du coronavirus), il faut dans le même temps s'assurer que ce l'on appelle en droit le « principe de proportionnalité » est respecté. Cela signifie qu'il faut éviter que le « droit à la protection de la vie privée » ne soit sacrifié au nom du « droit à la santé », et vice-versa. Dans les cas concrets où des droits peuvent entrer en conflit, comme c'est le cas face à la pandémie de coronavirus, la défense d'un droit au détriment d'un autre doit se borner à une circonstance exceptionnelle.

Il nous faut pour cela réduire l'immense avantage qu'ont sur nous les gouvernements et les entreprises. Ainsi, nous avons besoin de plus étroites associations et coopérations entre les développeurs et les cheurcheur·ses en informatique qui adoptent des approches critiques. La « technophobie » n'est pas une issue viable.

Face à la puissante légitimité sociale des idées d'innovation et d'optimisation technologique, c'est seulement en développant cette perspective informée, critique et réflexive que nous pourrons construire, aux côtés de l'ensemble des populations, un rapport de force favorable. Comme le montre le panorama des dispositifs mis en place jusqu'à maintenant, le *contact tracing* n'est pas une priorité dans toutes les situations

sanitaires et toutes les solutions techniques qui le permettent ne se valent pas, comme ne se valent pas toutes les modalités de collecte de l'information.

Sous certaines conditions, le *contact tracing* par Bluetooth peut permettre de mieux respecter ce principe de proportionnalité, en limitant considérablement les atteintes à la vie privée. Néanmoins, cette solution, elle non plus, n'est pas toujours valable. Il faut par exemple alerter sur le danger que représente l'offre de Google et Apple, qui ont récemment proposé aux gouvernements et agences de santé d'unir leurs forces pour lutter contre le coronavirus en utilisant le *contact tracing* par Bluetooth.

Les GAFAM savent que la défiance face à leurs pratiques invasives gagne du terrain dans le monde. C'est pourquoi ils cherchent à se racheter une légitimité, en associant leur solution au projet européen PEPP-PT. En réalité, sous le parapluie du PEPP-PT différentes solutions coexistent, qui centralisent ou non les informations et sont plus ou moins exigeantes au sujet de la protection des données personnelles. Puisque les GAFAM cherchent à jeter le trouble, rendons plus explicites les reproches substantiels que l'on peut faire à leurs propositions.

Pour cela, mettons ici en avant le travail des chercheur·ses à l'origine de DP-3T (Rastreo de Proximidad para preservar la Privacidad Descentralizada), qui développent leur solution à travers un code ouvert, dont le fonctionnement concret peut être vérifié, et qui garantissent que toutes les données personnelles restent intégralement sur le téléphone de chaque individu. A l'inverse, Apple et Google ne permettent pas une évaluation extérieure du code de leur solution, de telle sorte qu'il est impossible d'être certain·es que son fonctionnement effectif correspond à ce qui est annoncé.

*

Il s'agit donc de décrire précisément ce que les différentes modalités d'utilisation du *big data* dans le domaine de la santé publique peuvent apporter. C'est pourquoi il faut éviter les généralisations simplistes et étudier chaque dispositif dans son contexte d'utilisation, comme cet article a commencé à le faire. Nous devons rechercher toutes les extractions ou manipulations excessives des données personnelles, afin d'éviter toute atteinte disproportionnée au « droit à la vie privée ».

Pour les organisations politiques anticapitalistes et démocratiques, féministes, écologistes, les organisations syndicales et tous les autres collectifs qui luttent contre les oppressions et pour l'émancipation collective, l'unique manière effective, aujourd'hui, d'empêcher les abus des gouvernements et des entreprises, ce n'est pas de refuser de façon abstraite l'utilisation des Big Data en santé publique, mais bien de construire une connaissance collective précise et exhaustive du sujet. Cet article est un modeste effort dans cette direction.

Traduit par Gilles Martinet.

Une première version de cet article a été publiée par *Nueva Sociedad*.