Note n°12/20

30 mars 2020

Jean-Pierre Darnis
Chercheur associé, Fondation pour la recherche stratégique
Maître de conférence (HDR), Université Côte d'Azur, Nice
Conseiller scientifique à l'Istituto Affari Internazionali (IAI), Rome
Nicolas Mazzucchi
Chargé de recherche, Fondation pour la recherche stratégique

COVID-19 et instruments numériques : la délicate gestion des données

Introduction

La crise du COVID-19 que traverse à l'heure actuelle la quasi-totalité de la planète est un défi aux multiples facettes. Crise sanitaire d'abord, avec un virus nouveau qui, pour l'heure, résiste encore aux épidémiologistes et pour lequel le monde est en attente d'un traitement aussi bien que d'un vaccin. La recherche médicale, qui est en première ligne dans cette crise, est face à l'impératif de trouver au plus vite des solutions en regard de l'importance du nombre de malades et, malheureusement, de morts. Se pose donc une première question, celle de la capacité des systèmes de recherche à disposer d'outils leur permettant tout à la fois d'identifier les éléments pathogènes mais aussi d'expérimenter le plus efficacement possible les traitements en cours d'élaboration.

Le COVID-19 est aussi révélateur d'un certain nombre d'enjeux liés à la mondialisation, à commencer par la circulation rapide et sans beaucoup de contraintes des personnes et des biens. De fait, les mesures de « fermeture des frontières », redoutées en temps normal, ont ici été le plus souvent appliquées par les gouvernants européens et extra-européens comme moyen de freiner la propagation de l'épidémie. Au-delà de cette question de la gestion des entrées et des sorties sur les territoires nationaux ou régionaux se pose celle de la gestion de la circulation au sein même de ces territoires. L'histoire médicale a prouvé que le confinement, dans le cas de grandes épidémies, était un pis-aller efficace qui, aujourd'hui, transforme nos

villes en de modernes lazarets.

Face à ces enjeux qui relèvent à la fois du micro et du macro, les technologies numériques semblent en mesure d'apporter une aide efficace par leurs fonctionnalités intrinsèques, à savoir la capacité au partage de données de manière quasi instantanée, sur de grandes distances et pour la gestion de multiples éléments. Ces trois caractéristiques permettent ainsi, en théorie du moins, de gérer tout à la fois les partages de données médicales pour permettre aux équipes du monde entier de travailler de manière semi-collaborative, mais aussi aux forces de l'ordre de faire respecter les mesures de confinement. Toutefois, ces technologies ne sont pas sans soulever des enjeux éthiques et juridiques. Elles doivent être abordées avec un niveau le plus élevé possible de sécurité et d'éthique pour éviter le risque, une fois la crise passée, qu'elles ne se transforment en systèmes de contrôle massif ou d'espionnage des populations.

Le numérique, outil de gestion de crise sanitaire ?

La crise du COVID-19 a été jusqu'ici marquée par des différences entre les approches pour ce qui est de la gestion du problème sanitaire au niveau des grands ensembles de population. Au-delà de la Chine, dont la gestion sociale et sécuritaire des populations par les technologies numériques est bien connue[1], d'autres pays sont mis en avant pour leurs capacités numériques de gestion de crise. C'est le cas, en particulier, de la Corée du Sud, qui semble avoir connu des succès importants dans la limitation de la propagation de l'épidémie au prix d'un contrôle social ferme s'appuyant sur une cyber-béquille. Campagnes massives de dépistage et gestion numérique des confinements[2] apparaissent, sous la plume d'analystes admiratifs, comme la martingale permettant de résorber la crise le plus rapidement. Au niveau numérique, la Corée du Sud a mis en place un véritable système de suivi des malades avec des alertes pour la population lorsqu'un malade est détecté près de chez eux.

Identiquement, Singapour et Taïwan ont instauré des dispositifs de contrôle par le numérique, en particulier pour les personnes diagnostiquées positives au COVID-19. Ces exemples asiatiques ont semble-t-il inspiré certains pays européens, dont la Pologne : depuis le 20 mars, une application pour les smartphones est disponible qui permet, en prenant des selfies et en les envoyant sur une plateforme gouvernementale, de prouver que les citoyens infectés sont chez eux et respectent la quarantaine[3]. Si l'intention peut paraître louable en termes sanitaires, il importe aussi de se poser la question de la création d'un cyber-ostracisme, notamment en cas de révélation publique – suite à une cyberattaque par exemple – de l'identité des malades, d'autant plus qu'il est depuis longtemps évident que les procédés d'anonymisation ne sont pas vraiment robustes[4].

Se pose également la question de la mobilité européenne. Dans le contexte italien, nous assistons à des velléités régionales et nationales de s'inspirer des modèles sud-coréens pour proposer des applications de gestion des données personnelles finalisées au contrôle de

[1] V. Fortat, N. Mazzucchi, « L'intelligence artificielle en Chine, vers la supériorité technologique ? », Futuribles, 3 mars 2020.
[2] Y. Rousseau, « La Corée du Sud contre l'épidémie avec un dépistage de masse et de l'innovation », www.lesechos.fr, 17 mars 2020.
[3] « La Pologne crée une app qui oblige les malades du Covid-19 à prendre des selfies pour prouver qu'ils sont chez eux », www.businessinsider.fr, 23 mars 2020.
[4] L. Rocher, J. Hendrickx, Y.-A. de Montjoye, « Estimating the Success of Re-identifications in Incomplete Datasets Using Generative Models », *Nature Communication*, n° 10, 3069 (2019).

l'épidémie. C'est par exemple le cas de la région du Latium, qui a mis en ligne le 21 mars l'application « Lazio doctor »[5]. La multiplication d'applications locales suscite un problème non seulement de discontinuité des espaces au sein des Etats membres, mais crée également une barrière à la libre circulation des individus au sein de l'Union européenne (UE). Si l'intention est bien de développer des instruments digitaux permettant une reprise de la vie économique et sociale, alors ces instruments doivent être coordonnés ou interopérables au niveau européen de façon à ne pas recréer des frontières internes.

Toutefois, il faut également relever l'importance et l'intérêt des technologies numériques dans une telle crise. Le principal atout du cyberespace est de permettre le partage de données et d'informations en temps quasi réel et partout ou presque sur la planète. En ce sens, il est possible d'imaginer une forme de coopération mondiale ou du moins transnationale entre les équipes médicales pour la recherche sur le virus et ses traitements. De même, au niveau de la gestion de la santé publique, la mise en réseau en temps réel des capacités d'accueil en termes de lits de réanimation, de gestion des stocks médicaux, etc. pourrait très grandement bénéficier des technologies numériques, en particulier mobiles. La multiplication des terminaux mobiles personnels et professionnels rend ces hypothèses bien plus faciles à mettre en œuvre aujourd'hui car, *a priori*, il suffirait de développer uniquement des couches applicatives supplémentaires. Il importe cependant d'en considérer les limites afin d'encadrer strictement leur utilisation pour que celle-ci demeure bénéfique pendant et après la crise.

Le traitement automatique des données et la vie privée

L'importance de la crise sanitaire impose des mesures exceptionnelles aux gouvernants de l'ensemble des pays touchés. La difficulté d'instaurer un régime d'exception dans le contexte de cette crise est bien entendu à mettre en regard de ce que sera le mécanisme de retour à la normale une fois celle-ci terminée. Face aux décès liés au COVID-19, il est naturel de vouloir minimiser les pertes, même au prix d'un renoncement à la pleine protection des droits individuels. Cette mise en parenthèse de la démocratie dans le contexte digital peut s'apparenter à un recours à la « dictature » – au sens antique du terme – pour faire face à un moment de guerre, une expérience vécue dans le passé. Mais l'établissement de pouvoirs digitaux extraordinaires ne doit pas créer une étape de non-retour. Cela risque non seulement de générer des données de « contrôle absolu » -– lesquelles pourraient d'ailleurs tomber aux mains d'acteurs mal intentionnés –, mais il faut également s'assurer de respecter le droit à l'oubli, l'effacement et la propriété individuelle une fois la période de crise passée, principes présents dans le Règlement Général sur la Protection des Données (RGPD).

Au niveau européen, la question de la gestion des données en regard de la vie privée se pose tout naturellement puisque l'Union européenne a élaboré, depuis plusieurs décennies, sa politique numérique autour de la confidentialité des données. Bien avant le RGPD, qui est venu sanctuariser en 2018 cette centralité du citoyen européen dans la gestion de ses données personnelles par une série de droits imprescriptibles (accès, rectification, effacement, utilisation, portabilité), l'UE avait, au travers des travaux du G29 – inspirés du modèle français de la CNIL –, pris des positions importantes quant à la sanctuarisation de la vie privée en ligne. Dans le triptyque sécurité-disponibilité-confidentialité, constituant de la gestion responsable de l'information, l'Union a fait de longue date le choix de la confidentialité, à rebours d'autres acteurs, comme la Chine ou les Etats-Unis.

[5] http://www.regione.lazio.it/rl/coronavirus/scarica-app/

Il existe par ailleurs, au sein du RGPD, un régime spécifique pour les données médicales à caractère épidémiologique, mais celui-ci est lui-même fortement encadré puisqu'il s'agit là des données non seulement les plus intimes mais aussi les plus « valorisables ». Dans les études qui prétendent proposer des modèles économiques pour la monétisation des données personnelles, il ressort en effet que celles ayant une valeur dépassant les quelques euros ou dollars sont les données biomédicales personnelles, à partir desquelles nombre d'applications sont possibles[6]. Il apparaît donc que toute application qui permet de croiser des données médicales avec des données de mobilité devrait passer au préalable une série de garde-fous importants. Dans une note récente, la CNIL rappelle la nécessité de la gestion de telles données par les autorités sanitaires[7].

De la même manière, en droit français, la loi Informatique et Libertés de janvier 1978, avant sa modification par le RGPD, disposait qu'« *aucune décision de justice impliquant une appréciation sur le comportement d'une personne ne peut avoir pour fondement un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de sa personnalité.* » (art. 10). Or peut rapidement se poser la question de la transmission de ces données à des autorités de police chargées de faire respecter la quarantaine, ce qui soulève des questions d'interprétation du droit. A ce titre, il conviendra, en France, d'estimer les effets potentiels induits par la loi 2020-290 du 23 mars 2020, qui crée les dispositions liées à l'état d'urgence sanitaire, en particulier les nombreuses dérogations au fonctionnement habituel de certaines instances ou organismes, y compris en leur permettant un recours accru au numérique (pour exemple, l'article 10, qui prévoit le recours possible au vote électronique)[8]. Dans ce cadre, eu égard à la notion d'« urgence », il faut également considérer la problématique de la cybersécurité, en particulier dans une période propice au renforcement des cyberattaques – du fait du recours massif au télétravail ou de l'activité accrue des cybercriminels[9].

La sécurité des données en question

Une autre question se pose dans ce contexte, celle de la sécurité des données ainsi collectées. Que ce soit pour le développement d'applications spécifiques liées à l'épidémie elle-même ou pour le partage des données biomédicales, au-delà de l'éthique, la problématique de la sécurisation à la fois du stockage et de la transmission des données se pose inévitablement. L'un des grands problèmes liés à la cybersécurité vient de la compétition que se livrent les entreprises pour proposer le plus rapidement possible des applications innovantes. Cette ambition de réduire toujours plus le *time-to-market* est l'une des principales explications de la présence, au sein de nombreux logiciels, de failles profondes inconnues dites *zero-day*. Or dans un contexte particulièrement marqué par l'urgence, cette question de la porosité des applications tend à prendre un caractère secondaire vis-à-vis du service attendu.

De fait, la question de la sécurité et de la robustesse de l'application vis-à-vis d'entités commerciales ou publiques susceptibles d'utiliser les données récoltées est majeure une fois la crise passée. La création d'une application COVID-19 de contrôle de l'épidémie et des

[6] N. Mazzucchi, « Les données sont elles une marchandise comme les autres ? », *Notes de la FRS*, n° 12/2018, 26 juillet 2018.
[7] « Coronavirus (Covid-19) : les rappels de la CNIL sur la collecte de données personnelles », CNIL, 6 mars 2020.
[8] LOI n° 2020-290 du 23 mars 2020 d'urgence pour faire face à l'épidémie de covid-19 (1), JORF n°0072 du 24 mars 2020, texte n° 2.
[9] CORONAVIRUS – COVID-19 : Appel au renforcement des mesures de vigilance cybersécurité, www.cybermalveillance.gouv.fr, 16 mars 2020.

mouvements sur l'ensemble de la population crée de fait un fichier personnel extrêmement détaillé sur la vie privée des citoyens (habitudes, lieu de résidence, etc.). Si ces données ne sont pas gérées par une institution robuste du point de vue des procédures et de la sécurité technologique, avec un niveau important de chiffrement, alors il existe un risque réel que ces données soient captées par des intérêts externes pour des usages détournés, commerciaux ou autres. Cette question peut se révéler extrêmement délicate dans le cas d'un usage par des pays en compétition ou rivalité géopolitique avec l'Union européenne et ses membres (Chine ou Russie par exemple).

De la même manière, les risques d'une collaboration avec les GAFAM (Google, Apple, Facebook, Amazon, Microsoft) doivent être pris en compte, eu égard au fait que ces structures nourrissent leur *business model* avec les données personnelles des utilisateurs. Ces grands acteurs sont également les principaux fournisseurs d'*operating systems* des smartphones et tablettes, leur donnant un accès privilégié aux applications installées sur ceux-ci. Une solution fréquemment évoquée serait la mise à disposition des données déjà disponibles par les principales plateformes numériques. Or, dans ce contexte, le développement, depuis plusieurs années, de ces entreprises vers des modèles économiques liés à la santé – en particulier au travers d'objets connectés médicaux – peut constituer une forme de conflits d'intérêts. Il conviendrait donc ici de s'assurer que ces entreprises ne puissent, une fois la crise passée, utiliser les données biomédicales collectées pour des services commerciaux. Il existe donc un risque important de confusion et « d'abus de données dominantes ». De plus, la question du stockage de ces données dans le *cloud* et du droit appliqué représente un autre versant particulièrement délicat, l'Union européenne n'ayant pas fait le choix, contrairement à des pays comme la Chine ou la Russie, d'inscrire dans la loi l'obligation de stocker les données de ses citoyens sur le territoire de l'Union. Alors que certaines dispositions transnationales existent, comme le *Privacy Shield* avec les Etats-Unis, il serait bon de mesure quelle est leur robustesse dans le cas de l'urgence sanitaire.

Le droit européen apporte déjà des réponses potentielles avec les dispositions de la Directive Sécurité et Réseaux d'Informations (SRI) transcrite en 2018 dans le droit des Etats membres. La Directive SRI crée en particulier des obligations pour les fournisseurs de services numériques, au premier rang desquels les grandes plateformes de gestion des données. Celles-ci concernent d'abord la sécurisation de leurs prestations ainsi que celle des plateformes disponibles sous la forme de *clouds*, et permettent, jusqu'à un certain point, d'harmoniser les règles qui s'appliquent à ces fournisseurs avec celles des opérateurs d'importance vitale (énergie, eau, transports, médias, etc.). De fait, le cadre de cybersécurité créé par la Directive SRI permet d'ores et déjà d'obliger les gestionnaires de données à démontrer leur implication en termes de cybersécurité. Toutefois, dans le contexte présent, il s'agit d'aller plus loin en obligeant à ce que les données biomédicales soient chiffrées – au moment de leur stockage comme de leur transmission – grâce à des algorithmes de haut niveau, se rapprochant le plus possible des dispositifs de niveau gouvernemental (AES-256 notamment). Bien entendu, ces dispositifs de chiffrement auraient tendance à rendre le processus de partage plus complexe et, de fait, plus long, mais ils sont les seules garanties de la capacité sur le moyen-long terme d'éviter des fuites de données massives, bien plus inquiétantes vu leur nature que celles rencontrées habituellement.

Conclusion

La voie est donc particulièrement étroite pour concilier la mise en place d'instruments numériques dans la lutte contre l'épidémie, le maintien du cadre démocratique et la vigilance stratégique sur les intérêts de sécurité des données dans un contexte compétitif mondial. Il convient d'en prendre conscience à tous les niveaux et d'utiliser les mécanismes existants dans tous les Etats membres de l'UE, en coordination avec la Commission européenne, pour aboutir à un régime qui ne signifie pas une régression automatique en matière de libertés ni une perte irrémédiable dans la lutte pour le contrôle des données individuelles qui doivent nourrir les différents écosystèmes d'intelligence artificielle. A cet égard, il pourrait être particulièrement intéressant de s'inspirer de systèmes existants qui intègrent déjà ces contraintes, comme Auxylium, développé pour l'opération Sentinelle[10].

L'objet de la présente note n'est pas de se prononcer pour ou contre l'utilisation des technologies numériques dans la gestion de la pandémie actuelle. Les questions soulevées apparaissent légitimes en regard des implications à moyen et long terme de certaines initiatives. Si l'urgence sanitaire impose des décisions rapides et affirmées, la base des systèmes politiques européens, à savoir la démocratie représentative, impose quant à elle que ces mêmes décisions soient éclairées et cohérentes avec les valeurs portées par l'UE et inscrites dans le Traité sur l'Union européenne : liberté, Etat de droit et démocratie. Le COVID-19 est un défi majeur pour les systèmes de santé européens et mondiaux. Il est nécessaire d'éviter qu'il ne se débouche, à terme, sur une remise en cause des fondements politiques et philosophiques de nos sociétés.

[10] Reynald Fléchaux, « Auxylium : les smartphones ultra-sécurisés de l'opération Sentinelle », Silicon.fr, 20 avril 2017.

WWW.FRSTRATEGIE.ORG

4 BIS RUE DES PÂTURES 75016 PARIS TÉL : 01 43 13 77 77 FAX 01 43 13 77 78

ISSN : 2273-4643