L'application StopCovid : une solution hasardeuse pour lutter contre l'épidémie

Benjamin Loveluck

L'application StopCovid : une solution hasardeuse pour lutter contre l'épidémie

Benjamin Loveluck [1]

Parmi les mesures décidées par les pouvoirs publics afin d'endiguer la propagation du COVID-19, il en est une qui fut particulièrement sujet à controverse. Il s'agit du développement et du déploiement d'une application dite de « suivi de contacts » (*contact tracing*) appelée StopCovid en France, dont le principe semble à première vue très simple : l'application, une fois installée sur un téléphone de type *smartphone*, doit permettre de détecter et d'enregistrer la présence d'autres utilisateurs lorsqu'ils sont à proximité, créant ainsi un historique de contacts ; si l'un des utilisateurs est diagnostiqué positif à la maladie, il pourra transmettre l'information au système, qui se chargera ensuite d'avertir toutes les personnes concernées pour qu'elles s'isolent et se fassent tester à leur tour.

L'idée est donc d'enrayer les chaînes de transmission du virus, en automatisant un procédé bien connu des épidémiologistes : en effet, la recherche de contacts est une méthode courante et ancienne de lutte contre les maladies infectieuses telles que la tuberculose, le virus Ebola ou encore les maladies sexuellement transmissibles. Elle demande d'importantes ressources logistiques ainsi que des personnels formés et habilités à recueillir des informations sensibles et confidentielles, mais aussi capables d'évaluer si des situations présentent un risque sanitaire en fonction du type de contact établi, de sa fréquence et de sa durée, etc.

La recherche de contacts numérisée ou suivi de contacts consiste à s'appuyer sur l'équipement individuel en téléphonie mobile pour systématiser cette approche et la

1. i3-SES, Télécom Paris.

déployer à large échelle – et à moindre coût –, dans un contexte d'austérité budgétaire. Il s'agit également de pouvoir remonter des chaînes de transmission entre individus qui ne se connaissent pas, mais qui auraient simplement occupé brièvement un même espace public (transports en commun, commerces). Lancée le 27 mai après un vote (symbolique) à l'Assemblée nationale et au Sénat, StopCovid a suscité d'intenses débats chez les représentants politiques, y compris au sein de la majorité elle-même [2], mais a aussi donné lieu à de nombreuses prises de positions de médecins, d'épidémiologistes, d'informaticiens ou encore de juristes.

La France est loin d'être le seul pays à avoir mis en œuvre ce type de solution, qui a trouvé une justification scientifique avec notamment la parution d'une étude dans la prestigieuse revue Nature (Ferretti et al. 2020). Elle ne doit pas être confondue avec d'autres moyens numériques et systèmes d'information également mobilisés pour faire face à la pandémie. On trouve en effet d'un côté, par exemple, des applications d'auto-évaluation des symptômes ou des plateformes de suivi des enquêtes sanitaires par le personnel médical, qui s'apparentent à des systèmes d'information classiques. De l'autre, des solutions qui se présentent comme des instruments de contrôle des populations : surveillance du respect de la quarantaine ou du confinement à travers la géolocalisation des individus (via leur téléphone ou un bracelet électronique) comme en Chine, ou encore l'octroi de laissez-passer numériques en Russie.

Potentiellement très intrusif, le suivi de contacts présente des risques évidents pour la vie privée et les libertés publiques. En Israël, le traçage de contacts ainsi que la surveillance des personnes infectées a été directement délégué aux services de renseignement intérieur mobilisant les moyens du contre-terrorisme, qui s'appuient notamment sur les informations fournies par les opérateurs téléphoniques, surveillant ainsi toute la population sans le consentement des utilisateurs et sans aucune transparence. En Corée du Sud, aucune application dédiée n'a été développée mais les autorités se sont aussi appuyées sur les données de bornage des mobiles fournies par les opérateurs ainsi que les relevés de paiement communiqués par les banques, afin de générer des messages d'alerte aux personnes qui auraient partagé un espace – par exemple une salle de cinéma ou un restaurant – avec une personne infectée. Mais la diffusion de ces informations a conduit à des situations embarrassantes voire humiliantes, à la stigmatisation de personnes ou de lieux, voire dans certains cas à des chantages (des cas positifs réclamant de l'argent à des restaurants qu'ils avaient fréquentés, pour qu'en échange ils ne se déclarent pas malades auprès des autorités sanitaires, ce qui entraînerait la fermeture du restaurant) [3].

---

2. « Application StopCovid : le Parlement donne son feu vert au traçage numérique », Le Monde, 28 mai 2020, https://www.lemonde.fr/politique/article/2020/05/28/application-stopcovid-le-parlement-donne-son-feu-vert-au-tracage-numerique_6041013_823448.html.

3. « *More scary than coronavirus : South Korea's health alerts expose private lives* », The Guardian, 6 mars 2020, https://www.theguardian.com/world/2020/mar/06/more-scary-than-coronavirus-south-koreas-health-alerts-expose-private-lives.

Les solutions les plus répandues ont donc cherché à minimiser ces risques, en proposant des applications qui s'appuient d'une part sur la technologie Bluetooth plutôt que sur la géolocalisation, et qui veillent d'autre part à « anonymiser » les données recueilles par le système. L'idée étant de détourner l'utilisation du Bluetooth, normalement destiné à établir une connexion directe entre deux appareils et échanger des données à courte distance par ondes radio UHF. Il s'agit ici d'utiliser la durée et la puissance du signal établi entre deux téléphones pour déterminer une mesure d'exposition, en fonction de critères susceptibles d'être propices à une infection : dans le cas de StopCovid, deux utilisateurs situés à moins d'un mètre l'un de l'autre pendant au moins 15 minutes. L'application conserve ensuite les données de contact pendant 14 jours, soit la durée maximum pendant laquelle une personne peut être contagieuse en tenant compte du temps d'incubation de la maladie.

Confidentialité des données et choix techniques

Comme nous l'avons dit, la première préoccupation que soulève StopCovid concerne les données personnelles qui y sont collectées et traitées : non seulement des données de santé, qui sont intrinsèquement sensibles et auxquelles doivent s'appliquer des mesures de confidentialité ; mais également l'enregistrement des interactions sociales (le « graphe social ») et la mobilité des personnes, qui constituent aussi des informations à protéger. Le système doit donc offrir des garanties en termes de sécurité informatique, pour que des acteurs tiers malveillants ne puissent pas le détourner.

À cet égard, différents protocoles ont été développés afin d'assurer, d'une part la création et la gestion d'identifiants temporaires, c'est-à-dire de clés horodatées ou « pseudonymes » (permettant de créer les *logs* de chaque contact), et d'autre part le signalement aux personnes concernées lorsqu'un utilisateur est déclaré positif – le tout sans divulguer d'informations nominatives, en chiffrant ces clés et en les renouvelant fréquemment. Certaines approches ont été qualifiées de « décentralisées », notamment parce que les opérations de création de clés (ou « identifiants éphémères ») et d'enregistrement des *logs* de contact sont réalisées localement par l'application : c'est le cas notamment du protocole DP-3T (*Decentralized Privacy-Preserving Proximity Tracing*)[4]. À l'inverse, les approches dites « centralisées » telles que l'initiative du consortium européen PEPP-PT (*Pan-European Privacy-Preserving Proximity Tracing*) ou encore le protocole ROBERT développé en France par Inria pour StopCovid (mais aussi l'application TraceTogether dont elle s'inspire, utilisée à Singapour), transmettent les *logs* de contacts pour traitement

4. Une représentation simplifiée de son fonctionnement peut être consultée à l'adresse suivante `https://github.com/DP-3T/documents/tree/master/public_engagement/cartoon`.

voire attribuent les clés par l'intermédiaire d'un serveur central [5]. Dans tous les cas, cependant, un serveur central est nécessaire pour permettre d'avertir les utilisateurs concernés qu'une personne contact a été déclarée infectée.

Par ailleurs, ces enjeux de sécurité sont également étroitement liés aux décisions prises par deux grands acteurs privés : Google et Apple, qui contrôlent la majorité des *smartphones* du marché. En effet les fabricants – notamment Apple pour les iPhones – ont mis en place des garde-fous destinés justement à empêcher le Bluetooth de fonctionner en permanence et ainsi prévenir les utilisations intrusives qui pourraient en découler. Leur coopération semblait donc initialement un passage obligé pour permettre le développement d'une application destinée à communiquer constamment avec les appareils alentour. Les deux entreprises ont rapidement mis en place une API (interface de programmation) commune, désormais directement intégrée au système d'exploitation des téléphones, appelée *Exposure Notification* : celle-ci accorde des privilèges spéciaux aux applications développées par les autorités nationales de santé, leur permettant notamment de faire fonctionner le Bluetooth en tâche de fond, et elle a l'avantage d'être facilement interopérable. En contrepartie cependant, elle les contraint d'adopter un protocole spécifique d'attribution des identifiants et de signalement des cas positifs, mis au point par Apple et Google et qui est très proche du protocole « décentralisé » DP-3T.

De nombreux pays initialement alignés avec l'initiative PEPP-PT, tels que l'Allemagne, se sont finalement résolus à utiliser la plateforme proposée par Apple et Google, notamment pour des raisons d'efficacité et d'interopérabilité sur le plan européen. Mais la France refuse d'utiliser ce protocole propriétaire, arguant qu'il revient aux autorités sanitaires de contrôler la circulation de données de santé, que l'approche « centralisée » est plus protectrice des données personnelles, et enfin qu'elle permet aussi de produire un tableau global de la situation sanitaire en suivant le niveau d'exposition des utilisateurs et donc d'adapter le dispositif en conséquence. Devenu un enjeu de « souveraineté numérique », il s'agit, avec StopCovid, d'affirmer l'indépendance de l'État français en montrant que le pays dispose des ressources scientifiques et industrielles nécessaires. Cependant, l'adoption du protocole de Inria par StopCovid ne permet pas d'accéder à une utilisation optimale du Bluetooth [6] et empêche toute interopérabilité avec les autres pays.

De manière générale, ces différentes options d'architecture techniques ont donné lieu à des discussions enflammées au sein des communautés de chercheurs en informatique et d'experts en cybersécurité, qui ont souligné les vulnérabilités de l'une

5. Une « troisième voie » qualifiée d'« hybride » a également été proposée par Inria qui, suite aux critiques, a fait évoluer son protocole désormais appelé DESIRE, `https://github.com/3rd-ways-for-EU-exposure-notification/project-DESIRE/blob/master/DESIRE-summary-FR.pdf`

6. Les iPhones ne peuvent pas émettre en tâche de fond lorsque l'appareil est en veille (verrouillé) et dépendent des appareils Android alentour pour être « réveillés ».

ou l'autre approche [7], et qui ont parfois pris position pour [8] ou contre [9] l'application à travers des tribunes et des pétitions. Des failles techniques ont été décelées aussi bien au niveau des protocoles, décentralisés [10] ou non, que de leur implémentation et de l'application elle-même. Mais au-delà des aspects techniques, un site internet (`https://risques-tracage.fr`) a été mis en place par des chercheurs appartenant aux mêmes institutions que celles impliquées dans le développement des différents protocoles (Inria, EPFL) pour montrer, à l'aide d'une série d'études de cas, que le « traçage anonyme » constitue un « dangereux oxymore » quelle que soit la solution adoptée. Il est en effet très souvent possible, au moins en théorie, de déduire par recoupements ou par des moyens détournés si quelqu'un est malade ou quelle personne vous a infecté, de constituer des fichiers pseudonymisés des utilisateurs (susceptible d'être ré-identifiés en combinaison avec d'autres informations), ou encore de tracer les utilisateurs de l'application par une simple détection des signaux Bluetooth.

Une solution à l'efficacité douteuse

La deuxième grande interrogation que soulève l'application est celle de son efficacité réelle. Notons tout d'abord que le système ne peut fonctionner que s'il est articulé à une stratégie solide de dépistage, qui suppose un accès rapide à des tests pour les cas suspects et des résultats délivrés tout aussi rapidement, mais également de s'assurer que les cas positifs (et seulement eux) puissent se déclarer malades dans l'application. Mais surtout, la technologie Bluetooth n'a pas été initialement conçue pour mesurer des distances avec précision, la puissance du signal pouvant varier en fonction de nombreux facteurs (modèle de téléphone, obstacles, réverbérations dans l'environnement, etc.). Son détournement pose donc des problèmes de fiabilité. D'autre part, le simple rapprochement entre deux téléphones peut difficilement être

7. « Coronavirus : les applications de traçage des malades divisent les chercheurs en Europe », Le Monde, 23 avril 2020, `https://www.lemonde.fr/planete/article/2020/04/23/covid-19-les-applications-de-tracage-des-malades-divisent-les-chercheurs-en-europe_6037513_3244.html`.

8. Par exemple, en appui à la solution « centralisée », les directeurs de recherche à Inria Claude Castelluccia et Daniel Le Métayer, « Coronavirus : Sur l'application StopCovid, il convient de sortir des postures dogmatiques », Le Monde, 18 mai 2020, `https://www.lemonde.fr/idees/article/2020/05/18/coronavirus-sur-l-application-stopcovid-il-convient-de-sortir-des-postures-dogmatiques_6040038_3232.html`.

9. Voir les centaines de signataires sur le site « Mise en garde contre les applications de traçage », `https://attention-stopcovid.fr/`.

10. Par exemple dans le cas de SwissCovid qui s'appuie sur la plateforme Google-Apple, analysé en détail par le chercheur Serge Vaudenay (« *The dark side of SwissCovid* », `https://lasec.epfl.ch/people/vaudenay/swisscovid.html`). Voir également « Covid-19 : une énorme faille découverte dans l'API de *contact tracing* conçue par Apple et Google », 01net, 4 septembre 2020, `https://www.01net.com/actualites/covid-19-une-enorme-faille-decouverte-dans-l-api-de-contact-tracing-concue-par-apple-et-google-1972451.html`.

considéré comme suffisant pour déterminer une probabilité d'infection : les individus impliqués respectaient-ils les gestes barrières et portaient-ils un masque, ont-ils été en contact avec des surfaces, étaient-ils dos à dos ou bien face-à-face, séparés ou non par une paroi vitrée, l'espace était-il fermé ou ventilé, etc.

L'application est donc susceptible de générer de nombreux faux positifs, mais aussi des faux négatifs (par exemple lorsque quelqu'un entre dans un espace qu'une personne infectée vient de quitter). Dans le premier cas, le risque est de solliciter inutilement les filières de test déjà saturées ; dans le second, de procurer un faux sentiment de sécurité aux utilisateurs, qui pourraient être conduits à relâcher leur vigilance et leur pratique des gestes barrières. Ainsi la solution StopCovid pourrait-elle s'avérer non seulement inefficace, mais contre-productive pour la stratégie globale de lutte contre l'épidémie.

Pour terminer, l'efficacité de la démarche dépend également du taux d'adoption de l'application, mais à cet égard les modélisations sont très variables en fonction des mesures de santé mises en place (masques, distanciation) et du type de sous-population (jeune, active et urbaine ou non). Soulignons également qu'une partie de la population n'est pas équipée en *smartphones* ou possède un modèle trop ancien et ne sera donc pas en mesure d'installer l'application (bien que pour ces personnes, il ait été envisagé de développer des bracelets connectés capables d'assurer cette fonction...). La revue médicale *The Lancet* a publié au mois d'août 2020 une recension de travaux portant sur l'automatisation des techniques de traçage de contacts, utilisés dans différents contextes (syndromes respiratoires aigus, grippe, virus Ebola) depuis l'année 2000 (Braithwaite et al. 2020). L'étude souligne que les preuves de leur efficacité sont très maigres – en particulier si l'adoption par la population n'est pas massive (supérieure à 75 %) et si les quarantaines ne sont pas mises en place efficacement – et que la recherche manuelle de contacts validée par des praticiens reste décisive.

La question de l'efficacité est donc centrale, la CNIL ayant rappelé que la légalité du dispositif en dépendait, ce qui a conduit à la création d'un Comité de contrôle et de liaison (CCL) du COVID-19. Celui-ci est chargé d'évaluer « *l'apport réel des outils numériques* » pour les équipes sanitaires ainsi que de vérifier « *le respect des garanties entourant le secret médical et la protection des données personnelles* », ne remet pas en question l'utilité de StopCovid. Or, il relève dans son avis du 15 septembre 2020 [11] « *le décalage existant entre l'importance de l'investissement engagé dans la conception et le développement de l'application StopCovid et la faiblesse de son utilisation* ». En effet, à cette date, l'application aurait été téléchargée seulement 2,4 millions de fois soit par moins de 4 % de la population et désinstallée 700 000 fois (sans compter tous ceux qui l'auraient téléchargée mais pas activée), et « *le nombre*

11. https://solidarites-sante.gouv.fr/IMG/pdf/avis_du_ccl-covid_du_15_09_20._pour_un_systeme_d_information_au_service_d_une_politique_coherente_de_lutte_contre_l_epidemie.pdf

de notifications à des cas contacts est (...) inférieur à 200 sur trois mois, ce qui est dérisoire ». Par contraste, un quart des allemands auraient téléchargé l'application équivalente (*Corona-Warn-App*) malgré un scepticisme grandissant sur l'efficacité réelle de l'application [12]. Au Royaume-Uni, l'application lancée le 24 septembre 2020 a été téléchargée plus de 12 millions de fois en 5 jours [13]. Cet échec, pour le CCL comme pour d'autres membres du gouvernement, est imputé à un manque de publicité et une mauvaise « pédagogie » [14] – et ce alors même que le Premier ministre lui-même admet en direct, lors d'une émission télévisée [15], ne pas avoir installé l'application.

Effets collatéraux et normalisation d'une surveillance diffuse et « participative »

La troisième et dernière catégorie d'objections qui peuvent être opposées aux applications de suivi de contacts relève davantage des choix de société dans lesquelles elles s'inscrivent. En effet, si personne ne conteste la nécessité de mettre en œuvre des mesures exceptionnelles pour faire face à une situation qui n'a rien d'ordinaire et qui pose des risques immédiats pour la santé et la sécurité, il semble également légitime de s'interroger sur les conséquences à moyen et long terme de telles infrastructures de traçage des personnes. Les périodes d'urgence et de crise sont propices à des évolutions qui peuvent durablement affecter les libertés publiques – comme on peut en juger au regard de précédents récents (terrorisme, « gilets jaunes »), qui ont vu des dispositions initialement présentées comme temporaires être intégrées dans le droit commun (Sureau 2019). De tels risques ont d'ailleurs été évoqués lors des débats parlementaires mentionnés plus haut, au cours desquels la députée PS Laurence Dumont a souligné que « *les démocraties ont parfois du mal à rendre les libertés confisquées en temps de crise* », tandis que le député LREM Sacha Houlié s'inquiétait de « *franchir des lignes sur lesquelles on ne revient pas* » [16].

Pourtant les promoteurs de StopCovid ont parfois été prompts à caricaturer toute forme de remise en question. C'est le cas par exemple du secrétaire d'État chargé

12. « En Allemagne, le succès en trompe-l'œil de l'appli Corona-Warn-App contre le Covid-19 », Le Monde, 15 septembre 2020, https://www.lemonde.fr/pixels/article/2020/09/15/en-allemagne-le-succes-en-trompe-l-il-de-l-appli-corona-warn-app-contre-le-covid-19_6052317_4408996.html

13. Le Royaume-Uni a initialement cherché à développer sa propre solution sur un modèle « centralisé », mais après des mois de développement et devant l'échec des tests réalisés en conditions réelles sur l'île de Wight, a finalement refondu son application en s'appuyant sur la plateforme Google-Apple.

14. Selon le secrétaire d'État chargé du numérique Cédric O sur France Culture le 6 septembre 2020, https://www.franceculture.fr/emissions/soft-power/soft-power-le-magazine-des-internets-emission-du-dimanche-06-septembre-2020

15. « Vous avez la parole », France 2, 24 septembre 2020.

16. « Application StopCovid : le Parlement donne son feu vert au traçage numérique », Le Monde, 28 mai 2020.

du numérique et responsable du projet Cédric O, accusant de manière fallacieuse ceux qui refuseraient ces outils « *pour des raisons philosophiques* » d'« *accepter un risque significatif de malades et de morts supplémentaires* » [17]. Comme on l'a vu cependant, et sans qu'il soit nécessaire de convoquer Kant ou Aristote, aussi bien la sécurité de l'application que son efficacité ne vont pas de soi. Surtout, l'idée implicite que ceux qui s'opposeraient « par principe » à StopCovid auront des morts sur la conscience vise non seulement à clore toute discussion possible sur les éventuels effets indirects ou de plus long terme de l'application : elle vient également saper l'idée que son utilisation doit se faire sur une base volontaire, ceux qui la refuseraient se rendant moralement coupables de complicité avec la maladie. Rappelons en outre que le député LREM Damien Pichereau a proposé en mai 2020 que ceux qui installent l'application bénéficient de contreparties à travers un assouplissement des mesures de confinement ; tandis que le sénateur LR de l'Ain Patrick Chaize arguait en septembre qu'elle devrait être rendue obligatoire.

Pour certains défenseurs de StopCovid, le fait de devoir encourager la population à utiliser l'application plutôt que de l'obliger à le faire constitue donc une fâcheuse contrariété. Or, le volontariat figure parmi les conditions de légalité de StopCovid telles qu'elles ont été stipulées par la CNIL s'appuyant sur le RGPD (règlement général sur la protection des données) : un refus d'installer l'application ne doit entraîner aucune conséquence négative, et ne doit pas conditionner l'octroi de certains services, droits ou libertés, aussi bien par les institutions et services publics (tels que par exemple les transports en commun) que par les employeurs [18]. Enfin, au-delà de la liberté formelle laissée aux utilisateurs d'installer ou non l'application, la Commission nationale consultative des droits de l'homme (CNCDH) a pointé les limites de la notion de consentement individuel dans un contexte de peur de l'épidémie mais aussi de pressions sociales multiples « *tant à titre individuel que familial ou professionnel* », qui pourraient pousser les individus à installer StopCovid afin d'éviter toute stigmatisation [19].

Tout en admettant la difficulté de répondre à une crise sanitaire marquée par les incertitudes sur les effets et la circulation du virus, il est également indispensable de soupeser avec soin le précédent qu'un tel système d'information, nécessairement inabouti car développé dans l'urgence et impliquant de nombreux partenaires industriels (au rang desquels Orange, Capgemini, Dassault Systèmes mais aussi Accenture, Atos ou encore Thales), pourrait établir. En effet, il s'agit à la fois d'anticiper

17. Cedric O, « StopCovid ou encore ? », Medium.com, 3 mai 2020, `https://medium.com/\spacefactor\@m{}cedric.o/stopcovid-ou-encore-b5794d99bb12`.

18. CNIL, avis du 26 mai 2020, `https://www.cnil.fr/fr/la-cnil-rend-son-avis-sur-les-conditions-de-mise-en-oeuvre-de-lapplication-stopcovid`.

19. Celia Zolynski et Lucien Castex (rapporteurs), « Avis sur le suivi numérique des personnes », CNCDH, 28 avril 2020, `https://www.cncdh.fr/fr/publications/avis-sur-le-suivi-numerique-des-personnes`.

autant que possible les conséquences imprévues ou lointaines d'une technologie donnée, tout en identifiant les seuils ou paliers qui, lorsqu'ils sont franchis, rendent tout retour en arrière très coûteux voire impossible – et de s'assurer à l'inverse que tout développement technologique demeure « réversible » (Collingridge 1980).

Or il s'agit bien, avec StopCovid, de passer une étape qui peut sembler anodine, ou du moins justifiée par le contexte, mais qui représente malgré tout une collaboration inédite entre les industries du numérique et de la communication et les acteurs de la santé, avec un déploiement à grande échelle sur l'ensemble de la population. Et rien ne garantit que des fonctionnalités ne puissent pas être ajoutées ultérieurement, ou que les accès aux données et la finalité de leur traitement ne soient pas élargis au cours du temps, face à de nouveaux impératifs ou parce que des avantages seront présentés aux utilisateurs ou aux institutions impliquées. Il faut ici rappeler à quel point les données de santé constituent des « trésors » convoités par les géants du numérique, qu'il s'agisse des GAFAM ou d'entreprises que la « souveraineté numérique » aura conduit à favoriser : leur valorisation implique une course à la collecte, l'hébergement et le traitement d'un maximum d'informations, visant notamment à entraîner et optimiser des intelligences artificielles – dont les finalités n'ont pour l'heure pas été clairement définies [20]. Et si le développement et la gestion de StopCovid représentent un marché guère juteux pour l'instant, les collaborations ou partenariats établis peuvent constituer une étape supplémentaire autant qu'un moyen d'accoutumer les utilisateurs à partager ce type d'informations.

Plus largement, au-delà du « solutionnisme technologique » qu'il incarne et qui renvoie aux projets anciens de pilotage des populations par la cybernétique, le projet StopCovid cristallise les passions parce qu'il participe d'une acculturation à la surveillance, elle-même poussée par une combinaison d'intérêts marchands, de gouvernance technocratique et d'exigences sociales de sécurité. Par petites touches, des infrastructures de pistage numérique s'enracinent et des pratiques de surveillance mutuelle se banalisent, qui transforment en profondeur le tissu de nos existences.

Références bibliographiques

Braithwaite, I., Callender, T., Bullock, M. et Aldridge, R. (2020), « Automated and partly automated contact tracing : a systematic review to inform the control of COVID-19 », The Lancet, https://www.thelancet.com/journals/landig/article/PIIS2589-7500(20)30184-9/fulltext.

Collingridge, D. (1980), *The Social Control of Technology*, London, Pinter.

20. « Les données de santé, un trésor mondialement convoité », Le Monde, 2 mars 2020, https://www.lemonde.fr/sciences/article/2020/03/02/les-donnees-de-sante-un-tresor-mondialement-convoite_6031572_1650684.html.

Ferretti, L., Wymant, C., Kendall, M., Zhao, L., Nurtay, A., Abeler-Dörner, L., Parker, M., Bonsall, D. et Fraser, C. (2020), « *Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing* », Science, vol. 368 n° 6491, https://science.sciencemag.org/content/368/6491/eabb6936.

Sureau, F. (2019), Sans la liberté, Paris, Gallimard.