Criminologie

Analyse sociotechnique des applications de traçage de la COVID-19
Protection de la vie privée et matérialisation de la méfiance envers l'État

A sociotechnical analysis of COVID-19 contact tracing applications
The protection of privacy and the materialization of distrust towards the state

Un análisis sociotécnico de las aplicaciones de rastreo de contactos COVID-19
Protección de la privacidad y materialización de la desconfianza hacia el Estado

Simon Hogue

Volume 55, numéro 2, automne 2022

Les impacts de la COVID-19 sur les populations judiciarisées et vulnérables et sur les institutions de prise en charge

URI : https://id.erudit.org/iderudit/1093871ar
DOI : https://doi.org/10.7202/1093871ar

Aller au sommaire du numéro

Éditeur(s)

Les Presses de l'Université de Montréal

ISSN

0316-0041 (imprimé)
1492-1367 (numérique)

Découvrir la revue

Citer cet article

Hogue, S. (2022). Analyse sociotechnique des applications de traçage de la COVID-19 : protection de la vie privée et matérialisation de la méfiance envers l'État. *Criminologie*, *55*(2), 213–238. https://doi.org/10.7202/1093871ar

Résumé de l'article

Le 6 octobre 2020, à l'instar d'une quarantaine d'États, Québec donna son feu vert à une application de traçage des contacts basée sur une technologie d'Apple et Google pour combattre la COVID-19. Les applications de traçage soulèvent toutefois plusieurs enjeux liés aux droits démocratiques et à la justice sociale, aux premiers chefs la protection de la vie privée et l'équité face à une technologie à laquelle tous n'ont pas accès. Or, comment cet objet est-il devenu un objet de convergence dans l'utilisation de la surveillance numérique ? L'argument développé ici suggère que l'adoption en masse masque des dynamiques de pouvoir entre les développeurs, la société civile, les autorités de santé publique et les gouvernements sur le design des technologies utilisées dans la gestion de la pandémie. Apple, Google et leurs partisans ont réussi à normaliser une technologie qui matérialise une méfiance envers l'État. Cette analyse éclaire les dynamiques de pouvoir derrière la promotion des outils techniques dans la lutte contre la COVID-19 et les angles morts générés par la primauté de la protection de la vie privée.

Analyse sociotechnique des applications de traçage de la COVID-19

Protection de la vie privée et matérialisation de la méfiance envers l'État

Simon Hogue[1,2]
Professeur adjoint en études internationales
Collège militaire royal de Saint-Jean
Simon.hogue@cmrsj-rmcsj.ca

RÉSUMÉ • *Le 6 octobre 2020, à l'instar d'une quarantaine d'États, Québec donna son feu vert à une application de traçage des contacts basée sur une technologie d'Apple et Google pour combattre la COVID-19. Les applications de traçage soulèvent toutefois plusieurs enjeux liés aux droits démocratiques et à la justice sociale, aux premiers chefs la protection de la vie privée et l'équité face à une technologie à laquelle tous n'ont pas accès. Or, comment cet objet est-il devenu un objet de convergence dans l'utilisation de la surveillance numérique ? L'argument développé ici suggère que l'adoption en masse masque des dynamiques de pouvoir entre les développeurs, la société civile, les autorités de santé publique et les gouvernements sur le design des technologies utilisées dans la gestion de la pandémie. Apple, Google et leurs partisans ont réussi à normaliser une technologie qui matérialise une méfiance envers l'État. Cette analyse éclaire les dynamiques de pouvoir derrière la promotion des outils techniques dans la lutte contre la COVID-19 et les angles morts générés par la primauté de la protection de la vie privée.*

MOTS CLÉS • *Applications de traçage, Apple et Google, surveillance, COVID-19, vie privée.*

---

1. Collège militaire royal de Saint-Jean, C. P. 100, Succ. Bureau-chef, Richelain (Québec), Canada, J0J 1R0.

2. Je tiens à remercier Noémie Morasse Lapointe, les éditeurs et les évaluateurs anonymes pour leurs généreux commentaires.

Introduction

Le 6 octobre 2020, le gouvernement du Québec donne officiellement son feu vert à l'application de traçage des contacts Alerte COVID développée par le gouvernement fédéral (Caillou et Crête, 2020). La décision survient quelques semaines après le rapport de la Commission des institutions de l'Assemblée nationale sur les outils technologiques de notification des contacts. Publié le 19 août 2020, le rapport notait que « la quasi-totalité des experts rencontrés en commission ont émis des réserves importantes sur l'efficacité et la fiabilité de ces technologies » (Commission des institutions de l'Assemblée nationale, 2020, p. 2). Écoutant d'abord les avis d'experts, de l'opposition parlementaire et de la société civile, le gouvernement Legault avait alors rejeté l'utilisation de telles technologies. Un mois et demi plus tard, face à une résurgence des infections à la COVID-19, le gouvernement fait volte-face et décide de mobiliser cet « outil additionnel » (Caillou et Crête, 2020).

Comme le suggère le rapport de la Commission, les applications de traçage soulèvent plusieurs enjeux liés aux droits démocratiques et à la justice sociale, aux premiers chefs la protection de la vie privée des utilisateurs et les inégalités que pourrait engendrer le déploiement d'une technologie à laquelle tous n'ont pas accès. Le rapport note par exemple qu'« il existe une opinion majoritaire d'experts selon laquelle les populations les plus vulnérables à la COVID-19 sont celles qui auraient le moins accès aux applications de notifications de contacts » (Commission des institutions de l'Assemblée nationale, 2020, p. 2). Même si plusieurs experts médicaux ont suggéré une contribution importante des outils numériques dans les efforts pour contrer la pandémie de la COVID-19 (Ferretti *et al.*, 2020), ces enjeux invitent à les considérer avec prudence.

Les interrogations sur le poids que fait peser la surveillance numérique sur les droits démocratiques et la justice sociale dans le contexte de la COVID-19 (Couch, Robinson et Komesaroff, 2020 ; Newell, 2021 ; Ram et Gray, 2020) s'inscrivent dans une réflexion plus vaste sur les conséquences sociopolitiques des solutions techniques aux problèmes sociaux (Amicelle, Aradau et Jeandesboz, 2015 ; Ericson, 2006 ; Feenberg, 1999 ; Monahan, 2010). Tant les champs des études de la surveillance que des études sur la science et la technologie rappellent que les technologies n'existent pas en vase clos. Elles sont modelées par « les pratiques sociales, les identités, les normes, les conventions, les

discours, les instruments et les institutions – en bref, tous les éléments constitutifs de ce que nous appelons l'environnement social » (traduction libre de Jasanoff, 2004, p. 3). Dans ce contexte, « lorsque les gens conçoivent des technologies, négocient leurs caractéristiques et les introduisent dans le domaine plus large des affaires humaines », explique Langdon Winner, « ils sont engagés dans quelque chose de bien plus profond que l'amélioration du bien-être matériel, car les dispositifs et systèmes technologiques reflètent et, en fait, incarnent matériellement et institutionnellement des formes de vie sociale et politique » (traduction libre de Langdon Winner, 2006, p. 278). Ainsi, dans cette optique, les applications de traçage ne sont pas des instruments neutres et ne peuvent être lues indépendamment des « dimensions culturelles, symboliques, structurelles et matérielles complexes… [qui] contiennent et configurent la vulnérabilité corporelle, la stigmatisation et la marginalisation, les inégalités structurelles et la violence, ainsi que la construction et la gestion de la maladie » et des angoisses engendrées par la pandémie (traduction libre de French et Monahan, 2020, p. 2).

Partant des réserves émises par la Commission et plus globalement dans le cadre du débat sur l'utilisation des applications de traçage, j'ai cherché à comprendre comment le système de notifications d'exposition d'Apple et Google vers lequel le gouvernement Legault s'est tourné, à l'instar d'une quarantaine de gouvernements à travers le monde (Google, 2022), est devenu un objet de convergence dans l'utilisation de la surveillance numérique. L'objectif n'est donc pas de comprendre pourquoi le gouvernement québécois, parmi d'autres, a finalement décidé de mettre en œuvre une application de traçage, mais bien de comprendre comment cette application spécifique est apparue comme la voie à suivre.

L'adoption d'applications de traçage basées sur cette plateforme ne saurait s'expliquer simplement par l'argument de la « meilleure » technologie. Le recours à ces applications masque des dynamiques de pouvoir entre les développeurs des applications, la société civile, les autorités de santé publique et les gouvernements sur la forme qu'a prise l'utilisation des technologies dans la gestion de la pandémie. Apple, Google et les partisans des applications de traçage décentralisées, en faisant obstacle au déploiement d'autres technologies et en construisant un cadre narratif selon lequel les applications centralisées génèrent de trop grands risques de détournement par les États, ont réussi à normaliser cette technologie en imposant la primauté de la non-malfaisance

de l'application – la confidentialité et la sécurité des données – sur les bienfaits possibles des applications de traçage dans la gestion de la pandémie.

Malgré la fin de course abrupte des applications de traçage, cette analyse éclaire le déplacement du débat, notamment québécois, sur les applications de traçage, jetant une lumière sur les dynamiques de pouvoir derrière la construction de ce cadre narratif, en particulier le rôle du système de notifications d'exposition d'Apple et Google comme étendard des partisans d'une application décentralisée (Sharon, 2020). Il s'agit en outre de réinsérer la réflexion sur l'utilisation des technologies de surveillance dans un schéma d'analyse sociopolitique dépassant l'individualisme du droit à la vie privée (Lyon, 2001). Comme le rappelait Benjamin Bratton (2021), voir et être vu peuvent être à la fois privilèges et vulnérabilités, ce qu'une lecture étroite du concept de vie privée ne permet pas de prendre en considération (Stoddart, 2014).

Le présent article est construit en cinq parties, en débutant par la présentation du cadre méthodologique. Après avoir présenté les risques et espoirs investis dans l'utilisation de la surveillance dans la lutte contre la COVID-19, l'article présente l'initiative conjointe d'Apple et Google. L'article explore ensuite les pressions qu'ils ont exercées pour normaliser leur système de notification des expositions. L'article suggère enfin que leur système matérialise une méfiance envers l'État qui laisse dans l'angle mort les autres principes, notamment d'équité et d'efficacité, guidant la gestion de la pandémie.

Assises méthodologiques : situer le cadre narratif des applications de traçage à partir du débat public

Pour comprendre la normalisation de l'application de traçage développée par Apple et Google comme choix technologique pour répondre à la pandémie de la COVID-19, je me suis penché sur l'objet et le débat public dans lequel il s'insère afin d'identifier les valeurs en conflit pour la structuration du cadre narratif des applications de traçage. J'ai procédé à une analyse du discours des promoteurs des applications de traçage, en particulier le système de notification d'exposition proposé par Apple et Google, mais aussi des acteurs gouvernementaux, des activistes, des éthiciens et des experts médicaux et techniques qui se sont spécialisés dans ces technologies.

Soucieux de respecter les principes de transparence, les développeurs ont déposé leurs protocoles et documents explicatifs sur la plateforme de programmation Github. Je me suis donc tourné vers ces documents publics mis à disposition par les deux entreprises et les développeurs d'autres protocoles et applications (par exemple, BlueTrace, PEPP-PT, ROBERT, D3-PT) sur la plateforme et sur leurs sites internet respectifs. J'ai analysé leur fonctionnement et ce qui les distingue. Mais comme le rappellent les études sur la science et la technologie, « la connaissance et la technologie sont sensibles au contexte social et politique, dialoguent avec lui et le reflètent » (traduction libre de Vertesi et Ribes, 2019, p. 4). Dans cette perspective, ces documents publics, qui justifient leurs choix techniques et leurs objectifs, permettent de comprendre le cadre narratif structurant ces technologies. Les documents techniques constituent, en d'autres mots, un accès aux valeurs et aux « programmes politiques et sociaux » (traduction libre de Law, 2017, p. 37) des applications de traçage.

Le champ des études sur la science et la technologie a montré que ce contexte sociohistorique est souvent propre à certains laboratoires ou milieux restreints de production de la science (Vertesi et Ribes, 2019, p. 5). Dans les années récentes, elles ont toutefois affiché un intérêt croissant pour les débats publics portant sur les technologies, déplaçant l'analyse, comme le suggérait Sheila Jasanoff (citée dans Marres, 2007), à l'extérieur des cadres institutionnels formels composés de l'État, de l'industrie et de l'université. Ces débats rassemblent des individus et des associations autour de controverses et, à travers celles-ci, construisent et contestent les cadres narratifs qui structurent le recours aux technologies (Marres, 2007). Le débat public, le scandale ou la controverse deviennent alors « un moment de transformation sociale… ne laiss[ant] jamais les choses en l'état [et] condui[sant] à des repositionnements, à une redistribution des cartes institutionnelles, voire à des remises en cause brutales des rapports institués » (de Blic et Lemieux, 2005, p. 11-12).

En plus des documents de référence publiés par les développeurs des technologies de traçage, je me suis aussi intéressé au public qui participe au débat sur les applications de traçage, cette « pluralité de voix, d'opinions et de positions… liées par une cause commune face à un problème partagé » (traduction libre de Dantec et DiSalvo, 2013, p. 243) qui se regroupent et s'affrontent et qui, en définitive, « n'agissent que dans la temporalité de la circulation qui les fait exister » (traduction libre de

Warner, 2002, p. 96). Méthodologiquement, expliquent de Blic et Lemieux (2005), l'observateur doit donc suivre le public « dans les réactions suscitées par un acte de dénonciation publique » (p. 15). Pour constituer le corpus d'analyse, j'ai donc suivi la circulation des interventions publiques à partir d'une veille de médias spécialisés sur les questions technologiques (*MIT Technology Review*, *Wired*, *The Verge*), politiques (*The Economist*, *Foreign Affairs*) ou généralistes (*The Guardian*, *Le Devoir*, *La Presse*). Ces médias reconnus ont fait place aux discussions sur les applications de traçage tôt dans les efforts de gestion pandémique, soit parce que la technologie est au cœur de leur mission soit à travers les comparaisons de l'évolution de la pandémie à l'international. Les médias généralistes québécois ont permis de comprendre les spécificités locales. *The Guardian* était intéressant à deux niveaux : pour la qualité de sa couverture des enjeux technologiques et parce que le Royaume-Uni fut pionnier dans le déploiement d'une application de traçage.

Ces médias ont servi de porte d'entrée pour comprendre le débat sur les applications de traçage. Cependant, comme le rappellent de Blic et Lemieux (2005), si les médias de masse ont un « immense pouvoir d'extension du scandale… il serait, en revanche, hasardeux d'en déduire que les scandales modernes ont pour origine les médias » (p. 32-34). En ce sens, mon attention ne portait pas sur les médias eux-mêmes, à savoir par exemple la façon dont ils rapportaient la nouvelle, mais plutôt les textes institutionnels ou scientifiques et les prises de parole gouvernementales ou activistes qu'ils amplifiaient. En cherchant qui parlait d'applications de traçage, cela a permis de repérer les textes autour desquels s'est constitué le débat. Ultimement, le critère de délimitation du corpus d'analyse a donc été la circulation des textes vue comme indicateur de leur pertinence sociale.

L'analyse de la circulation des textes a montré leur grande mobilité géographique et leur circularité. Plusieurs institutions reconnues (ACLU, Ada Lovelace Institute, Johns Hopkins, Harvard ou Oxford University, etc.) étaient régulièrement citées par les médias, se citaient entre elles et traversaient les frontières des débats locaux. La consultation menée par la Commission sur les outils de notification de contact, par exemple, a fait place à des experts étrangers, provenant notamment de l'American Civil Liberty Union, organisation emblématique de la défense des droits et libertés aux États-Unis, et de la Quadrature du Net, organisation française de défense des droits numériques. La vingtaine de témoins

qui y ont été entendus et le *Petit guide sur les enjeux et opportunités des applications de notifications d'exposition à la COVID-19* de l'Observatoire international sur les impacts sociétaux de l'IA et du numérique, vers lequel le document de référence de la Commission renvoie, citaient la presse québécoise, mais aussi américaine et internationale, la presse technologique, les avis juridiques européens, les expériences de surveillance en Asie et les initiatives d'application de traçage mondiale (Déziel *et al.*, s. d.). L'analyse de la circulation des textes a enfin permis de repérer des moments forts qui ont alimenté le débat public, notamment la publication de l'article de Ferretti et ses collègues dans la revue *Science* (Ferretti *et al.*, 2020), des lancements de projets nationaux de traçage des contacts, de la Déclaration commune sur le traçage des contacts signée par plus de 300 experts de la communauté scientifique mettant en garde contre les risques de dérives de la surveillance pandémique (Larus *et al.*, 2020), et enfin, au Québec, la présentation du projet COVI du Mila et la Commission sur les outils de notification de contact.

Les interventions publiques ont été intenses, mais relativement brèves, débutant avec la pandémie à l'hiver 2020 avant de s'essouffler progressivement après la mise en fonction d'applications de traçage dans plusieurs pays à l'été et l'automne 2021. Symptomatique de cette perte d'intérêt, le MIT a cessé de mettre à jour son projet de veille des applications de traçage mondial le 25 janvier 2021 (O'Neill, Ryan-Mosley et Johnson, 2020). Ce débat s'est développé en trois temps autour de trois questions distinctes : l'utilisation de la surveillance numérique dans la gestion de la pandémie ; la technologie de traçage comme forme préférable de surveillance numérique ; et l'adoption d'une application de traçage officielle au sein d'un État (Simon et Rieder, 2021). Au centre de mon analyse se trouve la question médiane : si l'on admet la pertinence de l'utilisation de la surveillance numérique, quelle forme de surveillance et d'application de traçage est la plus appropriée ? Cette phase du débat se concentre au printemps 2020.

Espoirs et angoisses face à la surveillance pandémique : à la recherche d'une solution équilibrée

L'annonce du lancement d'une technologie de traçage des contacts par Apple et Google le 10 avril 2020 doit être comprise dans son contexte sociohistorique : une anxiété généralisée face au virus et aux outils à

disposition pour l'endiguer (Marange, 2020). Malgré la nature exceptionnelle des mesures de confinement, le monde occidental semblait incapable d'endiguer la pandémie avec le même succès que les pays asiatiques[3]. L'usage de la surveillance numérique par les autorités semblait avoir contribué à y arrêter rapidement la progression du virus, notamment l'utilisation de « bracelets » de géolocalisation permettant de policer les quarantaines en Chine, à Hong Kong, à Taiwan, en Corée du Sud et en Inde. La Chine avait développé également une application utilisant l'intelligence artificielle pour évaluer et contrôler les déplacements. La Corée du Sud croisait quant à elle la vidéosurveillance et les données financières pour pister les déplacements et informer les efforts de traçage de contact manuel (Cassiano, Haggerty et Bernot, 2021 ; Kim, 2020 ; Johns Hopkins Center of Health Security, 2020 ; *The Economist*, 2020). Lancées dans l'urgence, ces diverses initiatives ont suscité enthousiasme et inquiétudes (Greitens, 2020).

D'un point de vue médical, le désir de recourir à la surveillance n'est pas incongru. Elle offre un outil de collecte d'informations nécessaires au contrôle épidémiologique. Selon l'Organisation mondiale de la santé (OMS), le recours à des pratiques de surveillance permet ainsi de répondre à quatre objectifs : « 1) surveiller les tendances de la maladie là où il y a transmission interhumaine ; 2) détecter rapidement les nouveaux cas dans les pays où le virus ne circule pas ; 3) fournir des informations épidémiologiques pour évaluer les risques sur le plan national, régional et mondial ; [et] 4) fournir des informations épidémiologiques pour guider les mesures de préparation et de réponse » (traduction libre, OMS, citée dans French et Monahan, 2020, p. 4). Dans ce contexte, le traçage des contacts est rapidement apparu comme l'une des stratégies de lutte contre la COVID-19, que les technologies de surveillance numériques pourraient au moins en partie automatiser. Le 31 mars 2020, une équipe de l'Université d'Oxford publia dans la revue *Science* un article dans lequel les auteurs développaient un modèle mathématique suggérant que les applications de traçage pourraient « réduire suffisamment la transmission pour obtenir un $R < 1$ et une suppression durable de l'épidémie » (traduction libre de Ferretti *et al.*, 2020, p. 6). Face aux risques, les auteurs rappelaient toutefois l'impor-

3. Au moment où les deux géants faisaient leur annonce, près des deux tiers de cas confirmés de COVID-19 étaient recensés dans l'Union européenne et aux États-Unis. En comparaison, la Chine, la Corée du Sud, le Japon, Hong Kong, et Taiwan cumulaient moins de cas confirmés que l'Italie ou l'Allemagne seule (Our World in Data, 2022).

tance de la « confiance du public ». En ce sens, ils énuméraient une série de principes éthiques devant veiller à « assurer les bienfaits pour la santé publique et à réduire les torts » : supervision inclusive et transparente, garanties d'équités, transparence des algorithmes utilisés, protection des données, et minimisation de l'imposition de mesures. En définitive, chaque décision sur les applications de traçage devait être guidée par « trois valeurs morales : le respect moral égal, l'équité et l'importance de réduire la souffrance » (traduction libre de Ferretti *et al.*, 2020, p. 5).

Prenant Ferretti et ses collègues de vitesse, Singapour avait déjà adopté, le 20 mars 2020, une application de traçage des contacts. L'application TraceTogether fonctionne par échange de clés anonymes entre utilisateurs grâce au signal Bluetooth. Ne collectant pas de données pouvant directement identifier un individu ni de données de localisation GPS ou cellulaires, mais uniquement des clés d'identification anonymes échangées entre les utilisateurs, elle fut présentée comme un « protocole de préservation de la vie privée » permettant de dépasser le « choix binaire » entre « santé publique et vie privée » (traduction libre de Bay *et al.*, 2020, p. 1). L'Allemagne, l'Australie, la France, l'Islande, l'Italie, le Royaume-Uni et la Suisse ont entamé des démarches pour mettre en œuvre un système similaire (O'Neill *et al.*, 2020) tandis que plusieurs protocoles étaient en cours de développement : DP-3T (2020), PACT (2021), PEPP-PT (2020c), ROBERT (2020) et TCN (2020)[4].

Anticipant la venue du débat au Québec, la Commission d'accès à l'information du Québec (2020) publie ses recommandations le 14 avril 2020. Les commissaires fédéral, provinciaux et territoriaux à la protection de la vie privée (2020) vont présenter une déclaration commune sur les applications de traçage quelques semaines plus tard. Mais c'est le 18 mai, avec la proposition du Mila, l'Institut québécois d'intelligence artificielle, de lancer l'application COVI que l'enjeu est arrivé plus concrètement dans l'espace public québécois (Mila, 2020). Le premier ministre François Legault se montre d'abord favorable à l'initiative, disant en conférence de presse « considérer utiliser l'application » (traduction libre d'Assemblée nationale du Québec, 2020). COVI devait fonctionner avec le signal Bluetooth, à l'instar des autres protocoles de traçage. D'autres éléments la distinguaient toutefois. COVI devait

4. Au long, les noms des protocoles sont *Decentralized Privacy-Preserving Proximity Tracing* (DP-3T), *Private Automated Contact Tracing* (PACT), *Pan-European Privacy Preserving Proximity Tracing* (PEPP-PT), *ROBust and privacy-presERving proximity Tracing protocol* (ROBERT) et *Temporary Contact Numbers* (TCN).

notamment collecter des données personnelles telles que l'âge, le sexe, le dossier médical et de géolocalisation, et promettait d'utiliser l'intelligence artificielle pour améliorer les analyses de risque. En outre, les données collectées devaient être conservées sur un serveur central géré par une organisation à but non lucratif (Alsdurf *et al.*, 2020). Le projet est accueilli froidement par la société civile québécoise, qualifié de « technosolutionnisme » (Maclure, 2020) et décrié pour sa volonté de confier la consolidation des données à une organisation privée. COVI fut officiellement rejeté, le 10 juin, par Ottawa qui travaillait sur une application développée en partenariat avec le gouvernement ontarien, les Services numériques canadiens et des employés du fleuron Shopify : une application fonctionnant à partir de la technologie d'Apple et Google (Deglise, 2020). Lorsque la question des applications de traçage est revenue dans l'espace public québécois quelques semaines plus tard avec le lancement des consultations publiques menées par la Commission sur les outils technologiques de notification des contacts, l'application canadienne était ainsi devenue le point de référence de la discussion. Québec disait vouloir « mesurer l'intérêt de la population pour une telle application » (Secrétariat du Conseil du trésor, 2020, p. 3).

Le système de notifications d'exposition d'Apple et Google : prévenir les risques de la surveillance pandémique à même la conception

Dans un rare moment de collaboration, Apple et Google ont développé conjointement une technologie de traçage des contacts – un système de notifications d'exposition – fonctionnant avec le signal Bluetooth, compatible entre leurs systèmes d'exploitation de téléphone intelligent respectifs, iOS et Android, et accessible aux autorités de santé publique désireuses de l'utiliser. Les géants californiens s'engageaient ainsi à « aider les gouvernements et les agences sanitaires à réduire la propagation du virus, en plaçant la confidentialité et la sécurité des utilisateurs au centre de la conception » (traduction libre d'Apple et Google, 2020a). Ils n'étaient pas les seuls ni les premiers à proposer cette approche, mais ils offraient leur savoir-faire et leur position dominante sur le marché des téléphones intelligents pour faciliter la mise en place de cette technologie.

Les deux entreprises ont mis à la disposition des États une interface de programmation d'application – connue sous l'acronyme anglais d'API

– facilitant et encadrant le développement d'applications de traçage. Chacun des États voulant mettre à profit la technologie d'Apple et Google devait développer une application par lui-même ou par le biais d'une entente avec une entreprise ou un regroupement de partenaires (Apple et Google, 2020a). Cette application avalisée par les autorités publiques devenait alors accessible aux utilisateurs sur les marchés d'applications App Store ou Play Store ; Alerte COVID fut développée au Canada en suivant cette voie (SNC, 2022).

Le système d'Apple et Google fait partie de la famille des applications décentralisées, avec les protocoles DP-3T, TCN, PACT, en opposition aux protocoles centralisés BlueTrace, PEPP-PT et ROBERT (Apple et Google, 2020b ; PRIVATICS team, 2020, p. 4). L'application fonctionne dans sa quasi-totalité à partir de l'appareil. Chaque utilisateur possède un trousseau unique (un identifiant permanent) composé de plusieurs clés (des identifiants temporaires), généré à partir de l'application et inconnu des autorités, qu'il diffuse en rotation à l'aide du signal Bluetooth Low Energy (BLE). Les clés diffusées sont enregistrées par les autres utilisateurs, conservées sur les appareils individuels et constituent l'historique des contacts de chaque utilisateur. Lorsqu'un utilisateur reçoit un diagnostic positif à la COVID-19, il est invité à téléverser l'ensemble des clés de son trousseau sur un serveur central administré par les autorités de santé publique. Au moins une fois par jour, l'application contacte ce serveur pour télécharger les clés des utilisateurs infectés. L'application vérifie alors si l'historique contient une de celles-ci. Le cas échéant, l'application évalue alors les risques de contagion, calculés notamment à l'aide de la puissance et de la longueur du signal Bluetooth échangé. Les utilisateurs ayant eu un contact jugé à risque sont ainsi avertis et invités à contacter à leur tour les autorités locales de santé publique pour faire un dépistage. Le rôle du serveur central se limite à contenir les identifiants temporaires des utilisateurs infectés.

À l'inverse, les modèles centralisés attribuent un plus grand rôle aux serveurs centraux. Ces derniers créent les identifiants permanents et temporaires qu'ils transmettent à chaque utilisateur (PRIVATICS team, 2020, p. 4). Cela permet de centraliser l'analyse des données. L'utilisateur positif à la COVID-19 remet au serveur central les identifiants temporaires de ses contacts – plutôt que ses propres identifiants temporaires. Le serveur central compare les clés partagées et évalue les risques de contamination. Selon le protocole, il contacte alors les utilisateurs en associant les identifiants temporaires à leur identifiant permanent (The

DP-3T Project, 2020a, p. 1-2), ou l'application se connecte au serveur central pour savoir si l'utilisateur était à proximité d'un cas positif à la COVID-19 (The DP-3T Project, 2020b, p. 1-2).

Des similitudes existent entre les systèmes centralisés et décentralisés. Les deux partagent le postulat selon lequel générer un historique des contacts de proximité par échange de clés est moins intrusif et plus précis que d'utiliser un système d'information de géolocalisation. Comme pour les protocoles décentralisés, le serveur central ne collecte pas les données personnelles de l'individu qui apparaît, au niveau du serveur, comme un identifiant chiffré[5]. Les utilisateurs ne sont jamais informés de l'identité réelle de leur contact. L'historique des contacts est conservé sur l'appareil, jusqu'au moment où un utilisateur accepte de le partager. Enfin, les clés collectées sont supprimées de l'appareil au bout de quelques semaines, qui correspondent à la fin de la période de contagion (INRIA et Fraunhofer AIESEC, 2020 ; PEPP-PT, 2020a).

Toutefois, parce que le modèle décentralisé minimise plus encore que le modèle centralisé les données collectées par les serveurs centraux, il offre, selon la quasi-totalité des observateurs, une meilleure protection de la confidentialité des données des utilisateurs. Les identifiants permanents et temporaires étant conservés sur les appareils plutôt que sur des serveurs centraux, les autorités n'ont accès ni aux trousseaux de clés ni aux échanges de clés. Les États ne peuvent donc reconstituer à partir de ces applications les historiques de propagation ni les graphiques sociaux des utilisateurs (Apple et Google, 2020b, p. 5). Les partisans du modèle centralisé arguent au contraire qu'en ne collectant pas de données personnelles, leurs protocoles demeurent respectueux de la vie privée des utilisateurs tout en constituant « un élément important dans la gestion de la pandémie, car les données statistiques sur la propagation et l'efficacité des mesures sont ainsi disponibles plus rapidement » (PEPP-PT, 2020b). L'approche centralisée permet aussi « d'ajuster facilement l'algorithme de calcul du risque (pour décider si un utilisateur doit être classé comme "à risque") » (PRIVATICS team, 2020, p. 2).

Le système d'Apple et Google a reçu un accueil positif (Bagchi *et al.*, 2020 ; Granick, 2020 ; Larus *et al.*, 2020). Pourtant, le succès de la technologie proposée par Apple et Google ne saurait cacher l'existence de relations tendues entre d'un côté les deux géants du numérique et

5. À l'exception du protocole BlueTrace (TraceTogether) qui lie l'identifiant permanent à un numéro de téléphone (Bay *et al.*, 2020, p. 2).

les partisans d'une application de traçage décentralisée, de l'autre les partisans d'une approche centralisée au nombre desquels on comptait des gouvernements. La seconde fut en effet rapidement présentée par le clan adverse comme constituant un trop grand risque pour la vie privée des utilisateurs et donc inacceptable. Les deux entreprises ont néanmoins pesé de leur poids pour contraindre à l'utilisation des applications centralisées et s'établir comme acteur incontournable du débat.

Une collaboration sous le signe de la contrainte

Avec leur API, Apple et Google ont investi leur technologie et leur savoir-faire dans la lutte pandémique. « Grâce à une coopération et une collaboration étroites avec les développeurs, les gouvernements et les prestataires de services de santé publique », expliquaient-ils lors de l'annonce de leur initiative, « nous espérons exploiter la puissance de la technologie pour aider les pays du monde entier à ralentir la propagation de la COVID-19 et à accélérer le retour à la vie normale » (traduction libre d'Apple et Google, 2020a). L'offre venait toutefois avec des contraintes techniques et des conditions d'utilisation strictes afin, selon les propos des deux géants, de préserver la confidentialité et la protection des données des utilisateurs.

Dans la foulée de l'initiative des deux entreprises, plusieurs des projets de traçage des contacts imaginés ont avorté ou ont été mis en œuvre malgré des limitations techniques. Les initiatives allemande (PEPP-PT), française (ROBERT), britannique (Gould et Lewis, 2020), singapourienne (TraceTogether), mais aussi l'application COVI[6] sont emblématiques de ces dynamiques. Fonctionnant ou devant fonctionner selon un protocole centralisé, elles ont rencontré le même problème : l'utilisation du signal Bluetooth sur les systèmes d'exploitation iOS. Pour assurer la confidentialité des utilisateurs, le signal Bluetooth des téléphones iPhone se met en veille après un certain temps d'inactivité. Or, le signal Bluetooth, qui fonctionne par intermittence, nuisait à la fiabilité du traçage des contacts. Selon les chiffres partagés par le NSH, le système de santé publique britannique, la période d'essai de leur application a montré que celle-ci « enregistrait près de 75 % des appareils Android à proximité, mais seulement 4 % des iPhones » (Kelion,

6. Le Mila faisait face à des limitations similaires en travaillant avec l'API d'Apple et Google et disait être en négociation avec les géants (Alsdurf *et al.*, 2020, p. 24-28).

2020). Malgré les demandes formulées par les États et les développeurs pour activer le signal Bluetooth, Apple refusa d'apporter des modifications à son système d'exploitation, arguant les risques de dérive des applications centralisées (Bay *et al.*, 2020, p. 7 ; Hern et Sabbagh, 2020 ; Loveluck, 2020, p. 82 ; Simon et Rieder, 2021, p. 340).

Les contraintes d'utilisation des signaux Bluetooth ne peuvent expliquer à elles seules l'abandon des initiatives de traçage des contacts par l'Allemagne, le Royaume-Uni ou le Canada, ni expliquer pourquoi la France ou Singapour ont conservé leur application nationale nonobstant les limitations techniques créées par l'intermittence du signal Bluetooth[7]. En ressort toutefois le pouvoir de « contrôleur d'accès » des plateformes Apple et Google (Srnicek, 2017). À travers les contraintes techniques de leurs systèmes d'exploitation, ils ont contrôlé directement, sinon le choix des applications, du moins leur performance. Au moment d'annoncer le projet britannique, le ministre de la Santé Matt Hancock (cité dans Kelion, 2020) a ainsi rappelé que « le logiciel d'Apple empêche l'utilisation efficace des iPhones pour la recherche de contacts, à moins que vous n'utilisiez la propre technologie d'Apple. Notre application ne fonctionnera pas parce qu'Apple ne veut pas changer ce système. » De la même manière, en contrôlant les marchés d'application, les deux acteurs ont pu limiter les applications à la disposition des utilisateurs, comme le notait d'ailleurs la présidente du Mila (Marquis, 2020). En privilégiant l'application de traçage avalisée par les autorités de santé publique nationale, les deux géants risquaient, par exemple, selon les promoteurs du protocole décentralisé TCN, de compromettre les initiatives privées qui « ne requi[èren]t la participation d'aucune autorité sanitaire » et leur évite d'imposer « des charges supplémentaires » (TCNCoalition/TCN, 2020). Le contrôle des plateformes leur permettait en outre de promouvoir leur initiative conjointe, rapidement déployable à grande échelle, et par leur API, de contraindre le fonctionnement des applications nationales participantes. Ce pouvoir a permis aux géants californiens d'imposer leur choix de politique (Lévesque, 2020, p. 6-7 ; Sharon, 2020) et de devenir le point de référence, étendard du débat sur la protection de la vie privée et étalonor des applications de traçage, éclipsant au passage les initiatives similaires, également décentralisées, DP-3T, TCN et PACT qui le précédaient chronologiquement.

7. Pour des analyses pour l'Allemagne (Simon et Rieder, 2021), la France (Loveluck, 2020), le Royaume-Uni (Kind et Parker, 2020).

Intégrer les valeurs dans la conception : matérialisation technique de la méfiance envers l'État

La technique matérialise des valeurs particulières. Alors qu'il semblait y avoir unanimité sur les protections offertes par l'utilisation d'une application de traçage fonctionnant à l'aide du signal Bluetooth, ce sont les risques associés à une dérive de la mission qui s'instituèrent au cœur de la controverse entre les modèles d'application. Symptôme d'un « empiètement des logiques sectorielles » qui rompt « l'autonomie relative » de chaque partie au débat (de Blic et Lemieux, 2005, p. 34-35), cette méfiance exprimée par plusieurs acteurs de la défense des droits civiques et numériques et de la communauté numérique entre en contradiction avec les promoteurs initiaux des applications de traçage, épidémiologistes, acteurs de la santé et institutions publiques directement aux prises avec la gestion de la pandémie, qui cherchaient à trouver un équilibre entre les bienfaits – supposés – des outils de surveillance intrusifs et coercitifs déployés notamment en Asie et les coûts sur la vie privée.

Les 300 signataires de la déclaration commune sur les applications de traçage des contacts, issus de la communauté scientifique mondiale, mettaient ainsi en garde contre le fait que « certains pays cherch[ai]ent à mettre en place des systèmes qui pourraient leur permettre d'accéder et de traiter [le] graphe social [des utilisateurs] » et ainsi « [d']espionner les activités des citoyens » (Larus *et al.*, 2020, p. 1-2). Cette méfiance envers les institutions publiques est palpable parmi les développeurs. Le Mila a défendu la constitution d'une organisation à but non lucratif indépendante pour gérer les données centralisées afin que « l'application ne puisse être utilisée comme un moyen de surveillance par les institutions publiques » (Dilhac *et al.*, 2020)[8]. Les promoteurs du protocole décentralisé DP-3T s'estimaient quant à eux incapables d'accepter le postulat initial des développeurs du protocole centralisé ROBERT, selon lequel les « serveurs centraux sont honnêtes, mais curieux. […] Compte tenu de la fluidité de l'environnement politique actuel, il n'est pas certain qu'il s'agisse d'hypothèses appropriées », avertissaient les promoteurs du protocole DP-3T (The DP-3T Project, 2020b, p. 2, traduction libre).

8. COVI fait figure d'anomalie : sa proposition d'une application centralisée tient probablement au besoin particulier lié à l'utilisation de l'intelligence artificielle pour analyser les données.

Ils y voyaient au contraire un « potentiel élevé de dérive de la mission » et de collusion entre l'État-providence et l'État répressif. « [L]es scientifiques et les espions ne sont pas si différents », rappelaient du même souffle les employés de Shopify derrière Alerte COVID (Healy, cité dans Gruber, 2020)[9]. Dans ce contexte, la technologie de notification d'exposition était considérée comme « l'approche la plus respectueuse de la vie privée actuellement disponible » ("COVID Shield", s. d.).

Au cœur des différences techniques se trouve donc un désaccord sur la confiance : qui les utilisateurs doivent-ils craindre et à qui les utilisateurs doivent-ils accorder leur confiance ? Ainsi, plutôt que de craindre la proximité entre les « scientifiques » et « l'État », ROBERT justifiait son approche centralisée en évoquant une plus grande sécurité contre les attaques provenant « d'autres utilisateurs malveillants » (traduction libre de PRIVATICS team, 2020, p. 1). Or, en insistant sur les risques générés par les applications centralisées, non seulement passe-t-on sous silence ceux qui existent pour toute forme d'application centralisée ou décentralisée (Bonnetain *et al.*, 2020), mais les participants au débat minent en outre la confiance envers les institutions publiques responsables de réguler l'utilisation des applications. Reconnaissant les risques d'atteinte à la vie privée, les institutions publiques qui se sont penchées sur la question ont proposé des principes pour encadrer le déploiement d'une technologie de surveillance numérique, qui incluaient la proportionnalité et le besoin d'efficacité, la confidentialité et la transparence, sans exclure de facto aucune option (Commission à la protection de la vie privée du Canada, 2020 ; Commission de l'éthique en science et en technologie du Québec, 2020 ; European Data Protection Board, 2020). Au Canada, la Déclaration commune des gardiens du droit à la vie privée sur les applications de traçage des contacts exposés à la COVID-19 a laissé une latitude d'options aux décideurs, en indiquant qu'ils devraient « justifier clairement » leur choix (Commission à la protection de la vie privée du Canada, 2020). De son côté, le Comité européen de la protection des données (2020) reconnaissait que si, « en général, la solution décentralisée est plus conforme au principe de minimisation… Les deux doivent être considérées comme des options viables… chacune comportant un ensemble d'avantages et d'inconvé-

9. À la question « pourquoi utiliser la technologie d'Apple et de Google ? », le site web de l'application COVID Shield ("COVID Shield", s.d.), sur laquelle est fondée Alerte COVID, renvoie vers une entrée du blogue spécialisé en informatique Daring Fireball du programmeur américain John Gruber.

nients » (paragr. 42, traduction libre). Or, la persistance des craintes au sujet des applications centralisées suggère que ces avis demeurent insuffisants pour convaincre leurs opposants.

Cette méfiance envers les institutions publiques, qui s'est cristallisée dans une composante technique, a contribué à écarter les autres valeurs et considérants à la base de la réflexion éthique sur l'utilisation des applications de traçage et, plus généralement, de la surveillance numérique en temps de pandémie. Or, la question de la vie privée offre une lunette d'analyse importante, mais incomplète, pour comprendre la surveillance (Cinnamon, 2017, p. 610-611 ; Lyon, 2001). Les enjeux d'efficacité et de proportionnalité, d'équité et de stigmatisation sociale, d'égalité des chances face à la pandémie et dans l'accès aux traitements, de transparence et d'encadrement institutionnel sont devenus secondaires. La minimisation des torts associés à l'application décentralisée a de facto écarté la recherche de l'équilibre entre d'une part les risques provenant de la technologie, et plus largement ceux générés par la pandémie, et d'autre part, les bénéfices possibles de l'automatisation du traçage des contacts.

Conclusion : Remise à l'ordre de l'État ou occasion manquée ?

Comment le système de notifications d'exposition d'Apple et Google est-il devenu un objet de convergence dans l'utilisation de la surveillance numérique dans la gestion de la pandémie de COVID-19 ? La discussion sur le recours aux applications de traçage, d'abord portée par des acteurs de la santé publique et des épidémiologistes à la recherche d'une solution à une pandémie en apparence hors de contrôle, prend un nouveau tournant lorsqu'elle sort de ces cercles restreints et se confronte à des communautés numériques et de défense des droits qui se méfient du regard curieux et pas toujours honnête de l'État – comme le rappellent les révélations Snowden, le scandale Facebook/Cambridge Analytica et l'utilisation par la police singapourienne des données collectées par l'application TraceTogether (Han, 2021). Les considérations traditionnelles de la réflexion sur l'éthique de la pratique médicale laissent alors place aux enjeux qui animent ces communautés : les promesses d'efficacité des technologies, la confidentialité et la sécurité des données. Ces communautés ont reçu l'appui des géants du numérique Apple et Google, qui ont pris position pour les applications

décentralisées et y ont investi leurs ressources et leur pouvoir de contrainte pour faire pencher le débat. Au passage, les deux entreprises se sont imposées comme point de référence normatif et technique, nouveau cadre narratif du débat sur les applications de traçage faisant primer la minimisation des torts sur les autres principes éthiques guidant la gestion de la santé publique. La suite des événements allait se structurer autour de leur système de notifications d'exposition, comme ce fut le cas avec les consultations sur les outils technologiques de notification des contacts menées par la Commission des institutions de l'Assemblée nationale du Québec.

Cela ne signifie pas pour autant que les États auraient dû écarter les deux géants et adopter une application centralisée. Comme plusieurs l'ont suggéré, le projet de recourir à la surveillance numérique était, à la base, une démarche « d'apprenti sorcier » (Casilli *et al.*, 2020). Son efficacité est au mieux hypothétique. Des enjeux d'équité et de sécurité demeurent (Bonnetain *et al.*, 2020 ; Stanley et Callas, 2020). Elle masque d'autres problèmes criants de la gestion pandémique, notamment le sous-financement des systèmes de santé publique (French et Monahan, 2020, p. 7).

Le débat sur les applications de traçage éclaire enfin la barrière de la confiance. En voulant protéger les individus contre le regard indiscret de l'État, les partisans de l'approche décentralisée ont semé le doute sur les intentions des gouvernements. Ce faisant, ils ont ignoré l'importance de la confiance dans la décision des utilisateurs de partager ou non des données personnelles (Cheung, 2020, p. 5). Dans une enquête d'opinion comparant l'acceptabilité sociale des applications de traçage en Chine, en Allemagne et aux États-Unis, Kotska et Habich-Sobiegalla (2022) avancent que, même lorsqu'ils craignent les violations du droit à la vie privée, « les citoyens sont prêts à accepter le traçage numérique des contacts, malgré les inquiétudes concernant les atteintes à la vie privée et la surveillance gouvernementale, pour autant que les outils soient efficaces et qu'ils soient associés à des taux d'infection plus faibles » (p. 22, traduction libre). Les auteures notent au passage que « malgré les efforts » déployés par les gouvernements allemand et américain pour minimiser ces risques en adoptant notamment le système de notifications d'exposition, « les préoccupations des citoyens persistent dans ces pays » (traduction libre de Kotska et Habich-Sobiegalla, 2022, p. 20). Or, structurer le débat sur la minimisation des torts que pourraient causer les applications de traçage plutôt que sur les bénéfices

qu'elles pourraient apporter aux autorités de santé publique construit un cadre narratif marqué par la méfiance. Il devient, dans ce contexte, difficile de convaincre les gens d'utiliser des applications définies par le risque. Si, comme le soutient le Johns Hopkins Project on Ethics and Governance of Digital Contact Tracing Technologies (2020), il est important d'introduire des valeurs au cœur de la conception des applications de traçage, il faut néanmoins se rappeler que « ces valeurs peuvent inclure la vie privée, mais aussi l'autonomie, l'efficacité, l'équité ou autres. La conception de la technologie doit refléter un équilibre et un ordre de priorité appropriés entre les valeurs identifiées » (Johns Hopkins Project on Ethics and Governance of Digital Contact Tracing Technologies, 2020, p. 10).

Références

Alsdurf, H., Bengio, Y., Deleu, T., Gupta, P., Ippolito, D., Janda, R., … Yu, Y. W. (2020). *Livre blanc de COVI – Version 1.0*. Montréal, QC : Mila. Repéré à https://mila.quebec/wp-content/uploads/2020/05/Livre-Blanc-COVI_V1.pdf

Amicelle, A., Aradau, C. et Jeandesboz, J. (2015). Questioning security devices : Performativity, resistance, politics. *Security Dialogue*, *46*(4), 293-306. https://doi.org/10.1177/0967010615586964

Apple et Google (2020a, 10 avril). Apple and Google partner on COVID-19 contact tracing technology. Repéré à https://blog.google/inside-google/company-announcements/apple-and-google-partner-covid-19-contact-tracing-technology/

Apple et Google (2020b, septembre). Exposure Notifications Frequently Asked Questions. Repéré à https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-FAQv1.2.pdf

Assemblée nationale du Québec (2020, 18 mai). Conférence de presse de M. François Legault, premier ministre, et Mme Danielle McCann, ministre de la Santé et des Services sociaux. Repéré à http://www.assnat.qc.ca/fr/actualites-salle-presse/conferences-points-presse/ConferencePointPresse-60543.html

Bagchi, K. K., Bannan, C., Franklin, S. B., Hurlburt, H., Sarkesian, L., Schulman, R. et Stager, J. (2020). *Digital Tool for COVID-19 Contact Tracing : Identifying and Mitigating the Equity, Privacy and Civil Liberties Concerns*. Cambridge, MA : Edmond J. Safra Center for Ethics, Open Technology Institute, New America. Repéré à https://ethics.harvard.edu/files/center-for-ethics/files/22civilliberties.pdf

Bay, J., Kek, J., Tan, A., Hau, C. S., Yongquan, L., Tan, J. et Quy, T. A. (2020). *BlueTrace : A privacy-preserving protocol for community-driven contact tracing across borders*. Singapour, Singapour : Government Technology Agency.

Repéré à https://bluetrace.io/static/bluetrace_whitepaper-938063656596c104632def383eb33b3c.pdf

de Blic, D. et Lemieux, C. (2005). Le scandale comme épreuve. *Politix*, *71*(3), 9-38. https://doi.org/10.3917/pox.071.0009

Bonnetain, X., Canteaut, A., Cortier, V., Gaudry, P., Hirschi, L., Kremer, S., … Vuillot, C. (2020). *Le traçage anonyme, dangereux oxymore : Analyse de risque à destination des non-spécialistes*. Repéré à https://risques-tracage.fr/

Bratton, B. (2021, 24 août). L'artificiel et le synthétique : intelligence, langage, modèle. Communication présentée au MUTEK Festival international de créativité numérique et musiques électroniques, Montréal.

Caillou, A. et Crête, M. (2020, 6 octobre). Le gouvernement Legault donne son feu vert à Alerte COVID. *Le Devoir*. Repéré à https://www.ledevoir.com/politique/quebec/587253/le-gouvernement-legault-donne-finalement-son-feu-vert-a-alerte-covid

Casilli, A., Dehaye, P.-O., Soufron, J.-B., Binet, S., Kotlicki, M.-J. et Radaut, R. (2020, 25 avril). « StopCovid est un projet désastreux piloté par des apprentis sorciers ». *La Quadrature du Net*. Repéré à https://www.laquadrature.net/2020/04/25/stopcovid-est-un-projet-desastreux-pilote-par-des-apprentis-sorciers/

Cassiano, M. S., Haggerty, K. D. et Bernot, A. (2021). China's Response to the COVID-19 Pandemic : Surveillance and Autonomy. *Surveillance & Society*, *1*(19), 94-97. https://doi.org/https://doi.org/10.24908/ss.v19i1.14550

Cheung, S. (2020). Disambiguating the benefits and risks from public health data in the digital economy. *Big Data & Society*, *7*(1), 205395172093392. https://doi.org/10.1177/2053951720933924

Cinnamon, J. (2017). Social Injustice in Surveillance Capitalism. *Surveillance & Society*, *15*(5), 609-625.

Commission à la protection de la vie privée du Canada (2020, 7 mai). *Déclaration commune des gardiens du droit à la vie privée sur les applications de traçage des contacts exposés à la COVID-19*. Repéré à https://www.newswire.ca/fr/news-releases/declaration-commune-des-gardiens-du-droit-a-la-vie-privee-sur-les-applications-de-tracage-des-contacts-exposes-a-la-covid-19-844869511.html

Commission d'accès à l'information du Québec (2020). *Pandémie, vie privée et protection des renseignements personnels : Éléments de réflexion concernant le recours à certaines technologies (ex. : traçage des contacts, bracelets connectés, utilisation de données de géolocalisation)*. Québec, QC : Gouvernement du Québec. Repéré à https://www.cai.gouv.qc.ca/pandemie-vie-privee-et-protection-des-renseignements-personnels/

Commission de l'éthique en science et en technologie du Québec (2020). *Les enjeux éthiques de l'utilisation d'une application mobile de traçage des contacts dans le cadre de la pandémie de COVID-19 au Québec*. Québec, QC : Gouvernement du Québec. Repéré à https://www.ethique.gouv.qc.ca/fr/publications/l-utilisation-d-une-application-mobile-de-tracage-des-contacts-dans-le-cadre-d-une-pandemie/

Commission des institutions. (2020). *Rapport – Consultations particulières au sujet d'outils technologiques de notification des contacts ainsi que sur la pertinence de ce type d'outil, leur utilité et le cas échéant, les conditions de leur acceptabilité sociale dans le cadre de la lutte contre la COVID-19.* Repéré à http://www.assnat.qc.ca/fr/travaux-parlementaires/commissions/ci/mandats/Mandat-43205/index.html

Couch, D. L., Robinson, P. et Komesaroff, P. A. (2020). COVID-19 – Extending Surveillance and the Panopticon. *Journal of Bioethical Inquiry*, *17*(4), 809-814. https://doi.org/10.1007/s11673-020-10036-5

COVID Shield. (s. d.). Repéré à https://www.covidshield.app/

Deglise, F. (2020, 10 juin). Ottawa dit non à Mila et son application COVI de recherche de contacts de personnes contaminées. *Le Devoir*. Repéré à https://www.ledevoir.com/societe/580507/ottawa-dit-non-a-mila

Déziel, P.-L. (s. d.). Petit guide sur les enjeux et opportunités des applications de notifications d'exposition à la COVID-19. *OBVIA*. Repéré à https://observatoire-ia.ulaval.ca/qa_covid/

Dilhac, M.-A., Bengio, Y., Rish, I., Janda, R., Ghosn, J., Borreman, S., … Prud'homme, B. (2020, 23 mai). COVI : Une application de suivi de contacts intelligente…et éthique. *Mila*. Repéré à https://mila.quebec/covi-une-application-de-suivi-de-contacts-intelligenteet-ethique/

DP-3T (2020, 30 septembre). *DP-3T/documents*. Repéré à https://github.com/DP-3T/documents

The DP-3T Project (2020a). *Security and privacy analysis of the document "PEPP-PT : Data Protection and Information Security Architecture."* Repéré à https://github.com/DP-3T/documents/blob/master/Security analysis/PEPP-PT_Data Protection Architechture–Security and privacy analysis.pdf

The DP-3T Project (2020b). *Security and privacy analysis of the document "ROBERT : ROBust and privacy-presERving proximity Tracing."* Repéré à https://github.com/DP-3T/documents/blob/master/Security analysis/ROBERT–Security and privacy analysis.pdf

Ericson, R. V. (2006). *Crime in an insecure world*. Londres, Royaume-Uni : Polity Press.

European Data Protection Board (2020). *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*. Repéré à https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf

Feenberg, A. (1999). *Questioning Technology*. New York, NY : Routledge.

Ferretti, L., Wymant, C., Kendall, M., Zhao, L., Nurtay, A., Abeler-Dörner, L., … Fraser, C. (2020). Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. *Science*, *368*(6491), eabb6936. https://doi.org/10.1126/science.abb6936

French, M. et Monahan, T. (2020). Dis-ease Surveillance : How Might Surveillance Studies Address COVID-19 ? *Surveillance & Society*, *18*(1), 1-11.

Google (2022). *Vérifier si une application de notifications d'exposition est disponible dans votre région – Aide Android*. Repéré à https://support.google.com/android/answer/10289696

Gould, M. et Lewis, G. (2020, 24 avril). Digital contact tracing : protecting the NHS and saving lives. *NSHX*. Repéré à https://www.nhsx.nhs.uk/blogs/digital-contact-tracing-protecting-nhs-and-saving-lives/

Granick, J. S. (2020, 16 avril). Apple and Google Announced a Coronavirus Tracking System. How Worried Should We Be ? *ACLU*. Repéré à https://www.aclu.org/news/privacy-technology/apple-and-google-announced-a-coronavirus-tracking-system-how-worried-should-we-be/

Greitens, S. C. (2020). Surveillance, Security, and Liberal Democracy in the Post-COVID World. *International Organization*, 1-22. https://doi.org/10.1017/s0020818320000417

Gruber, J. (2020, 18 mai). Thinking Through the Manifold Ramifications of Collecting Smartphone Data for Contact Tracing. *Daring Fireball*. Repéré à https://daringfireball.net/linked/2020/05/18/healy-privacy-exposure-notification

Han, K. (2021, 11 janvier). Broken promises : How Singapore lost trust on contact tracing privacy. *MIT Technology Review*. Repéré à https://www.technologyreview.com/2021/01/11/1016004/singapore-tracetogether-contact-tracing-police

Hern, A. et Sabbagh, D. (2020, 6 mai). Critical mass of Android users crucial for NHS contact-tracing app. *The Guardian*. Repéré à https://www.theguardian.com/world/2020/may/06/critical-mass-of-android-users-needed-for-success-of-nhs-coronavirus-con tact-tracing-app

INRIA et Fraunhofer AIESEC. (2020). *ROBERT : un protocole de suivi des contacts respectueux de la vie privée*. Repéré à https://github.com/ROBERT-proximity-tracing/documents/blob/master/ROBERT-summary-FR.pdf

Jasanoff, S. (2004). States of Knowledge. Dans S. Jasanoff (dir.), *States of Knowledge : The Co-Production of Science and Social Order* (p. 1-12). Londres, Royaume-Uni : Routledge. https://doi.org/10.4324/9780203413845

Johns Hopkins Center for Health Security (2020). *Review of Mobile Application Technology to Enhance Contact Tracing Capacity for COVID-19*. Johns Hopkins Bloomberg School of Public Health. Repéré à http://www.centerforhealthsecurity.org/our-work/pubs_archive/pubs-pdfs/2020/200410-national-plan-to-contact-tracing.pdf

Kahn, J. (dir.). (2020). *Digital Contact Tracing for Pandemic Response*. Baltimore, MD : Johns Hopkins University Press. https://doi.org/10.1353/book.75831

Kelion, L. (2020, 18 juin). UK virus-tracing app switches to Apple-Google model. *BBC*. Repéré à https://www.bbc.com/news/technology-53095336

Kim, M. S. (2020, 6 mars). South Korea is watching quarantined citizens with a smartphone app. *MIT Technology Review*. Repéré à https://www.technologyreview.com/2020/03/06/905459/coronavirus-south-korea-smartphone-app-quarantine/

Kind, C. et Parker, I. (2020, 18 juin). Turn it off and on again : lessons learned from the NHS contact tracing app. *Ada Lovelace Institute*. Repéré à https://www.adalovelaceinstitute.org/blog/lessons-from-nhs-contact-tracing-app/

Kostka, G. et Habich-Sobiegalla, S. (2022). In times of crisis : Public perceptions toward COVID-19 contact tracing apps in China, Germany, and the United States. *New Media & Society*, 146144482210832. https://doi.org/10.1177/14614448221083285

Larus, J., Paterson, K., Veale, M., Smart, N., Preneel, B., Cremers, C., … Fiore, D. (2020, 19 avril). Déclaration commune sur le traçage des contacts. Repéré à https://www.esat.kuleuven.be/cosic/sites/contact-tracing-joint-statement/wp-content/uploads/sites/7/2020/04/déclaration-commune-tracage-contacts.pdf

Law, J. (2017). STS as Method. Dans U. Felt, R. Fouché, C. A. Miller et L. Smith-Doerr (dir.), *The Handbook of Science and Technology Studies* (p. 31-57). Cambridge, MA : MIT Press.

Le Dantec, C. A. et DiSalvo, C. (2013). Infrastructuring and the formation of publics in participatory design. *Social Studies of Science*, *43*(2), 241-264. https://doi.org/10.1177/0306312712471581

Lévesque, M. (2020). *Mémoire. Consultations particulières et auditions publiques au sujet d'outils technologiques de notification des contacts ainsi que sur la pertinence de ce type d'outils, leur utilité et le cas échéant, les conditions de leur acceptabilité sociale dans le cadre de la lutte contre la COVID-19*. Repéré à http://www.assnat.qc.ca/fr/travaux-parlementaires/commissions/CI/mandats/Mandat-43205/memoires-deposes.html

Loveluck, B. (2020). L'application StopCovid : une solution hasardeuse pour lutter contre l'épidémie. *Bulletin de la Société Informatique de France*, 79-88. Repéré à https://hal.telecom-paris.fr/hal-03020158

Lyon, D. (2001). *Surveillance society : Monitoring everyday life*. Philadelphie, PA : Open University Press.

Maclure, J. (2020, 19 mai). Entre le technosolutionnisme et le catastrophisme. *La Presse+*. Repéré à https://plus.lapresse.ca/screens/a6b42637-0450-4ae8-bddd-a890d5809da7__7C___0.html

Marange, V. (2020). Malaise dans la biopolitique. *Chimères*, *97*(2), 15. https://doi.org/10.3917/chime.097.0015

Marquis, M. (2020, 10 juin). Application de traçage COVI : les gens de Mila rendent les armes. *La Presse*. Repéré à https://www.lapresse.ca/covid-19/2020-06-10/application-de-tracage-covi-les-gens-de-mila-rendent-les-armes

Marres, N. (2007). The Issues Deserve More Credit. *Social Studies of Science*, *37*(5), 759-780. https://doi.org/10.1177/0306312706077367

Yoshua Bengio et ses collaborateurs dévoilent le nom de leur application de traçage de la COVID-19 et lancent un Livre blanc (2020, 18 mai). *Mila*. Repéré à https://mila.quebec/yoshua-bengio-et-ses-collaborateurs-devoilent-le-nom-de-leur-application-de-tracage-de-la-covid-19-et-lancent-un-livre-blanc/

Monahan, T. (2010). *Surveillance in the Time of Insecurity*. New-Brunswick, NB : Rutgers University Press.

Newell, B. C. (2021). Introduction : Surveillance and the COVID-19 Pandemic : Views from Around the World. *Surveillance & Society, 1*(19), 81-84. https://doi.org/ https://doi.org/10.24908/ss.v19i1.14606

O'Neill, P. H., Ryan-Mosley, T. et Johnson, B. (2020, 7 mai). A flood of coronavirus apps are tracking us. Now it's time to keep track of them. *MIT Technology Review*. Repéré à https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/

Our World in Data (2022, 27 avril). COVID-19 Data Explorer. *Our World in Data*. Repéré à https://ourworldindata.org/explorers/coronavirus-data-explorer

PACT (2021). PACT : Private Automated Contact Tracing. Repéré à https://pact.mit.edu/

PEPP-PT (2020a). *High-Level Overview*. Repéré à https://raw.githubusercontent.com/pepp-pt/pepp-pt-documentation/master/PEPP-PT-high-level-overview.pdf

PEPP-PT (2020b, 24 avril). What is the PEPP-PT position on centralized vs decentralized ? Repéré à https://github.com/pepp-pt/pepp-pt-documentation/blob/master/FAQ.md

PEPP-PT (2020c, 10 juin). *pepp-pt/pepp-pt-documentation*. Repéré à https://github.com/pepp-pt/pepp-pt-documentation/

PRIVATICS team (2020). *Proximity Tracing Approaches Comparative Impact Analysis*. INRIA. Repéré à https://raw.githubusercontent.com/ROBERT-proximity-tracing/documents/master/Proximity-tracing-analysis-EN-v1_0.pdf

Ram, N. et Gray, D. (2020). Mass surveillance in the age of COVID-19. *Journal of Law and the Biosciences, 7*(1), lsaa023. https://doi.org/10.1093/jlb/lsaa023

ROBERT (2020, 4 septembre). ROBERT-proximity-tracing/documents. Repéré à https://github.com/ROBERT-proximity-tracing/documents

Secrétariat du Conseil du Trésor (2020). *Consultations particulières et auditions publiques au sujet d'outils technologiques de notification des contacts ainsi que sur la pertinence de ce type d'outils, leur utilité et le cas échéant, les conditions d'acceptabilité sociale dans le cadre de la lutte contre la COVID-19 : Document de consultation*. Repéré à http://www.assnat.qc.ca/fr/travaux-parlementaires/commissions/ci/mandats/Mandat-43205/index.html

Service numérique canadien (2022, 5 avril). Qui a conçu Alerte COVID ? Repéré à https://github.com/cds-snc/covid-alert-app

Sharon, T. (2020). Blind-sided by privacy ? Digital contact tracing, the Apple/Google API and big tech's newfound role as global health policy makers. *Ethics and Information Technology*, 1-13. https://doi.org/10.1007/s10676-020-09547-x

Simon, J. et Rieder, G. (2021). Trusting the Corona-Warn-App ? Contemplations on trust and trustworthiness at the intersection of technology, politics and public debate. *European Journal of Communication, 36*(4), 334-348. https://doi.org/10.1177/02673231211028377

Srnicek, N. (2017). *Platform Capitalism*. Cambridge, Royaume-Uni : Polity.

Stanley, J. et Callas, J. (2020, 6 août). Tracking Apps are Unlikely to Help Stop COVID-19. *American Civil Liberties Union*. Repéré à https://www.aclu.org/news/privacy-technology/tracking-apps-are-unlikely-to-help-stop-covid-19/

Stoddart, E. (2014). (In)visibility Before Privacy : A Theological Ethics of Surveillance as Social Sorting. *Studies in Christian Ethics*, *27*(1), 33-49. https://doi.org/10.1177/0953946813509335

TCNCoalition (2020, 19 août). Specification and reference implementation of the TCN Protocol for decentralized, privacy-preserving contact tracing. Repéré à https://github.com/TCNCoalition/TCN

Creating the coronopticon : Countries are using apps and data networks to keep tabs on the pandemic (2020, 26 mars). *The Economist*. Repéré à https://www.economist.com/briefing/2020/03/26/countries-are-using-apps-and-data-networks-to-keep-tabs-on-the-pandemic

Vertesi, J. et Ribes, D. (2019). Introduction. Dans J. Vertesi et D. Ribes (dir.), *digitalSTS : A Field Guide for Science and Technology Studies* (p. 1-10). Princeton, NJ : Princeton University Press.

Warner, M. (2002). *Publics and Counterpublics*. New York, NY : Zone Books.

Winner, L. (2006). Technology Studies for Terrorists : A Short Course. Dans T. Monahan (dir.), *Surveillance and Security : Technological Politics and Power in Everyday Life* (p. 275-291). New York, NY : Routledge.

A sociotechnical analysis of COVID-19 contact tracing applications : The protection of privacy and the materialization of distrust towards the state

ABSTRACT • *On October 6, 2020, Quebec, along with some 40 other states, gave the green light to a contact tracing application based on technology developed by Apple and Google to combat COVID-19. Contact tracing applications, however, raise a number of issues related to democratic rights and social justice, most notably privacy and equality in the face of a technology to which not everyone has access. How did this object become an object of convergence in the use of digital surveillance ? The argument developed in this article suggests that mass adoption masks power dynamics between developers, civil society, public health authorities and governments in regard to the design of technologies used for pandemic management. Apple, Google and their supporters have succeeded in normalizing a technology that materializes a distrust of the state. This analysis illuminates the power dynamics behind the promotion of technical tools in the fight against COVID-19, as well as the blind spots generated by the primacy of privacy.*

KEYWORDS • *Contact tracing applications, Apple & Google ; surveillance, COVID-19, privacy.*

Un análisis sociotécnico de las aplicaciones de rastreo de contactos COVID-19 : protección de la privacidad y materialización de la desconfianza hacia el Estado

RESUMEN • *El 6 de octubre de 2020, el Quebec, como hicieron otros 40 estados, dio luz verde a una aplicación de rastreo de contactos basada en la tecnología de Apple y Google para combatir el COVID-19. Sin embargo, las aplicaciones de rastreo de contactos plantean una serie de cuestiones relacionadas con los derechos democráticos y la justicia social, sobre todo en lo que se refiere a la protección de la vida privada y la equidad ante una tecnología a la que no todo el mundo tiene acceso. ¿Cómo este elemento ha podido convertirse en un objeto de convergencia en el uso de la vigilancia digital ? El argumento desarrollado aquí sugiere que su adopción masiva esconde las dinámicas de poder entre los desarrolladores, la sociedad civil, las autoridades de salud pública y los gobiernos sobre el diseño de las tecnologías utilizadas en la gestión de la pandemia. Apple, Google y sus partidarios han conseguido normalizar una tecnología que materializa la desconfianza hacia el Estado. Este análisis saca a relucir las dinámicas de poder que hay detrás de la promoción de las herramientas técnicas en la lucha contra el COVID-19 y los puntos ciegos que genera la primacía de la protección de la vida privada.*

PALABRAS CLAVE • *Aplicaciones de rastreo de contactos, Apple y Google, vigilancia, COVID-19, vida privada.*