OBSERVATOIRE INTERNATIONAL
SUR LES IMPACTS SOCIÉTAUX
DE L'IA ET DU NUMÉRIQUE

Analyse sur l'application de notification de contacts COVI

et commentaires de l'équipe de Mila

Document préparé des chercheur·e·s
membres et non membres de l'OBVIA

Version 2 - 18 juin 2020

Cette analyse a été préparée dans le cadre des travaux de l'Observatoire international sur les impacts sociétaux de l'IA et du numérique (OBVIA) sur les effets des systèmes d'intelligence artificielle et des outils numériques déployés pour lutter contre la propagation de la COVID-19 sur les sociétés soutenus par les Fonds de recherche du Québec (FRQ).

18 juin 2020
Deuxième version

ISBN 978-2-9818996-4-4

Préparée dans le cadre d'une crise sanitaire et en pleine période de confinement, cette analyse est le fruit d'efforts de recherche entrepris par des chercheur·e·s membres et non membres de l'OBVIA provenant de divers horizons disciplinaires, comme le droit, l'éthique, l'apprentissage automatique, le génie, les politiques publiques et la cybersécurité. Elle met en évidence des questions soulevées par le développement d'une application de notification de contacts, COVI et formule une série de recommandations sur l'application COVI.

La première version du présent document a été déposée le 3 juin 2020 sous la forme d'un avis qui se voulait préliminaire et se basait uniquement sur le fonctionnement décrit de COVI par Mila dans un « white paper » rendu public le 18 mai 2020.

Cette deuxième version, intitulée Analyse, a été produite après la tenue d'échanges avec Yoshua Bengio, directeur scientifique de Mila qui apporte un complément d'informations à l'analyse des chercheur·e·s. Ces compléments d'information sont clairement identifiés dans des encadrés. Cette version de l'analyse des chercheur·e·s intègre aussi quelques corrections sur des éléments de faits à la lumière d'autres documents communiqués par Mila et des informations échangées lors d'une rencontre organisée le 8 mai 2020 entre le comité Covid-19 de l'OBVIA, Yoshua Bengio et Benjamin Prud'homme de Mila.

L'ensemble des travaux effectués à l'OBVIA s'inscrit dans une démarche scientifique ouverte et publique. Ce document se veut itératif et évolutif, il pourra être bonifié au fil des développements et des travaux effectués sur l'application de notification COVI.

N.B. Dans ce document, le genre masculin est utilisé comme générique, dans le seul but de ne pas alourdir le texte.

Crédits

Équipe de rédaction du document

- Lyse Langlois, professeure titulaire, Département des relations industrielles, Université Laval, Directrice générale de l'OBVIA
- Réjean Roy, conseiller aux projets spéciaux, OBVIA
- Guillaume Macaux, conseiller scientifique, OBVIA
- Eve Gaumond, candidate à la maîtrise en droit, Université Laval, et responsable du programme Incubateur d'idées innovantes, OBVIA

Contributeurs (ordre alphabétique)

- Céline Castets-Renard, professeure titulaire, Faculté de droit, Université d'Ottawa
- Pierre-Luc Déziel, professeur adjoint, Faculté de droit, Université Laval
- Benoit Dupont, professeur titulaire, École de criminologie, et directeur scientifique, Réseau intégré sur la cybersécurité (SERENE-RISC)
- Audrey Durand, professeure adjointe, Département d'informatique et de génie logiciel et Département de génie électrique et de génie informatique, Université Laval
- Christian Gagné, professeur titulaire, Département de génie électrique et de génie informatique, Directeur de l'Institut intelligence et données, Université Laval
- Sébastien Gambs, professeur agrégé, Département d'informatique, Université du Québec à Montréal
- Karine Gentelet, professeure agrégée, Département des sciences sociales, Université du Québec en Outaouais
- Steve Jacob, professeur titulaire, Département de science politique, Université Laval
- Lyse Langlois, professeure titulaire, Département des relations industrielles, Université Laval, Directrice générale de l'OBVIA
- Denis Laurendeau, professeur titulaire, Département de génie électrique et de génie informatique, Université Laval

- Allison Marchildon, professeure agrégée, Département de philosophie et d'éthique appliquée, Université de Sherbrooke
- Cécile Petitgand, chercheuse postdoctorale OBVIA - H-POD, Université de Montréal et Centre de recherche du Centre hospitalier de l'Université de Montréal
- Denis Poussart, professeur émérite, Département de génie électrique et de génie informatique, Université Laval
- Stéphane Roche, professeur titulaire, Département des sciences géomatiques, Université Laval
- Bryn Williams-Jones, professeur titulaire, École de santé publique, Université de Montréal

Conseillers

- François Laviolette, professeur titulaire, Département d'informatique et de génie logiciel, Université Laval
- Catherine Régis, professeure titulaire, Faculté de droit, Université de Montréal
- Daniel Weinstock, professeur titulaire, Faculté de droit, et directeur, Institut de recherche sur les politiques sociales et de santé, Université McGill

Table des matières

Présentation de l'OBVIA

L'Observatoire international sur les impacts sociétaux de l'IA et du numérique (OBVIA) est un réseau de recherche ouvert et financé par les Fonds de recherche du Québec et qui fédère les expertises de plus de 220 chercheur·e·s en sciences humaines et sociales, en sciences et génie, et en santé. C'est un espace ouvert de discussion et de réflexion pour l'ensemble des parties prenantes au développement et à l'utilisation de l'IA et du numérique qui permet, dans une dynamique interdisciplinaire et intersectorielle de relever des défis reliés à la conception et au déploiement d'outils numériques efficaces et responsables

Sa mission, en se fondant sur une interrogation critique des innovations technologiques et dans une perspective d'innovation responsable, est de soulever des enjeux cruciaux et d'identifier des solutions plausibles aux problèmes et opportunités posés par les développements de l'IA et du numérique au Québec et ailleurs dans le monde.

L'OBVIA mène des projets de recherche et de recherche-création ; réalise des activités de veille et des enquêtes ; soutient le débat public et fait des propositions de politiques publiques. Un de ses axes d'intervention prioritaires porte sur la santé durable.

Schéma 1 — Principes favorisant le développement et le déploiement responsables de solutions fondées sur le numérique et l'IA[1]

[1] Lehoux, P. et autres (2020), Peut-on innover de façon responsable en temps de pandémie? L'Intelligence artificielle et le numérique face au SARS-CoV-2, document de travail produit pour l'OBVIA, mai 2020. En ligne : https://observatoire-ia.ulaval.ca/peut-on-innover-de-facon-responsable-en-temps-de-pandemie/. Silva H.P. et autres, "Introducing responsible innovation in health: A policy-oriented framework", Health Research Policy and Systems, 2018, 16(1), p. 90.

But de ce document

En mai 2020, Mila — Institut québécois d'intelligence artificielle, l'un des principaux centres de recherche en apprentissage automatique au monde, a déposé la première version d'un livre blanc sur COVI, une application de notification de contacts[2] et de collecte de données qui pourra notamment servir à modéliser l'évolution de la pandémie de Covid-19 dans les provinces et les territoires du Canada et, en fin de compte, à contrôler la propagation du nouveau coronavirus.

Qu'est-ce que COVI ?

Le site de COVI Canada décrit COVI comme « une application mobile qui utilise l'intelligence artificielle pour permettre à chacun de nous de combattre la Covid-19. Créée au Canada par un collectif de chercheurs et d'experts dirigés par Yoshua Bengio et gérée par un organisme sans but lucratif, l'application permet à chaque citoyen de prendre des décisions en temps réel au quotidien quant à ses activités, et ce afin de se protéger, protéger [ses] proches et les autres. »

Le livre blanc publié par Mila et ses partenaires donne plus de renseignements sur les objectifs de COVI. La publication de ce document par Mila doit être saluée, puisqu'elle permet aux acteurs de l'écosystème du numérique et de l'IA de mieux comprendre de quoi COVI retourne. Il est important de souligner que tous les acteurs actifs dans le développement d'applications du genre n'ont pas produit des livrables aussi complets ni rendu accessibles les informations permettant de comprendre leur fonctionnement. Les objectifs de COVI sont les suivants :

"The primary aim of COVI is to reduce the spread of Covid-19, in order to: 1) reduce the morbidity and mortality associated with Covid-19 infection; and 2) reduce the burden of Covid-19 on healthcare systems. To achieve this aim, the primary strategy of COVI is to inform individuals of their infection risk so they can act responsibly to protect themselves and others and limit the spread of the virus.

'COVI leverages probabilistic risk levels (as detailed below), rather than binary results of confirmed infection (or not), to assign Covid-19 infection risk levels to app users. This probabilistic risk is modified and updated based on two main categories of information—users' individual profile and interaction profile. Individual profiles arise from user-entered information including demographic information, baseline comorbidities, occupation and the presence of

[2] L'expression « application de notification de contacts » est utilisée dans ce document pour présenter COVI. Elle renvoie au fait que COVI cherche à avertir les individus du niveau de risque qu'ils encourent en fonction des contacts qu'ils ont eus avec d'autres personnes. L'expression « traçage de contacts » est parfois utilisée pour décrire ce type d'application, mais elle réfère plutôt au moyen d'arriver à une estimation du niveau de risque. Actuellement, le traçage de contacts est le principal moyen d'estimer ce niveau de risque, mais on pourrait imaginer qu'à l'avenir, d'autres méthodes fassent leur apparition. Pour information, l'API actuellement développée par Google-Apple porte le nom de « exposure notification API » en anglais alors qu'au départ elle s'appelait « contact tracing API ». Voir : https://www.google.com/covid19/exposurenotifications/.

new symptoms. The interaction profile arises when two or more users converge in physical proximity. The probability of transmission depends on details such as distance apart, time spent in an interaction, the prior contacts of an individual, and the use of masks or other physical separation devices. The combination of this information generates a machine learning (ML) derived personalized probability distribution of the user's likeliness of being infected, when the infection may have occurred, and the expected contagiousness on different days after infection.

'COVI then empowers citizens to take a progressive, proactive approach to managing infection risk for themselves and others. The specific individual risk level will not be displayed as the response to receiving a specific risk number can be heterogeneous and elicit counterproductive behavior. Instead, when a user's risk level increases, evidence-based messaging previously approved by public health authorities will be provided through the app. This messaging will recommend various actions that can be taken by the user to reduce Covid-19 infection risk."

Rédigé par un groupe de chercheurs membres et non membres de l'OBVIA (voir la section « Crédits »), le présent document constitue principalement une analyse du contenu du livre blanc de Mila. Il examine aussi l'information recueillie par les membres du Comité Covid-19 de l'OBVIA[3] lors d'une rencontre organisée le 8 mai 2020 avec Yoshua Bengio et Benjamin Prud'homme de Mila. Cette rencontre visait à mieux comprendre COVI et à échanger sur les enjeux associés à son développement et son déploiement. Le document porte enfin sur des renseignements relayés par un groupe de chercheurs mis en place en avril 2020 pour faire le relais entre Mila et les chercheurs du Comité Covid-19 de l'OBVIA. Trois rencontres ont été tenues par ce groupe avec un représentant de Mila.

Pertinence de COVI

Du point de vue éthique, la première question à se poser relativement à une application, en tant qu'application de notification de contacts, consiste à savoir si l'adoption de cette application procurera une réelle plus-value sociale ou un bénéfice social tangible en matière de santé publique et si ce type d'application peut être une réponse efficace aux enjeux de santé publique. Ces questionnements ont été en toile de fond des réflexions.

COVI ne serait pas la première application de notification de contacts lancée dans un pays ou une région pour lutter contre le coronavirus. Un travail de veille réalisé par une équipe de chercheurs de l'OBVIA a montré que plus de 70 applications du genre existaient à la fin de mai 2020 à travers le monde.

[3] Le comité Covid-19 a été mis en place en mars 2020 après la réception par l'OBVIA d'une subvention exceptionnelle du FRQ pour analyser les effets des outils numériques et des outils de l'IA déployés pour lutter contre la propagation de la COVID-19 dans nos sociétés. Ce comité est composé des chercheurs suivants: Philip Jackson, Pascale Lehoux, Daniel Weinstock, Catherine Régis, Francois Laviolette, Lyse Langlois, Jean-Louis Denis, Christian Lévesque, Nathalie de Marcellis, Bryn William-Jones, Colette Brin, Céline Castets-Renard, Pierre-Luc Déziel, Philippe Després et Aude Motulsky.

Certains rapports laissent croire que ces applications n'ont pas, à ce jour, donné l'ensemble des résultats escomptés. Le Guardian rapporte ainsi qu'en Australie,

> Covidsafe was sold as the key to unlocking restrictions [...] but as the country begins to open up, the role of the Covidsafe app in the recovery seems to have dropped to marginal at best. "This is an important protection for a Covid-safe Australia," the prime minister, Scott Morrison, said in late April. "I would liken it to the fact that if you want to go outside when the sun is shining, you have got to put sunscreen on." [...] Yet nearly a month since launch, the contact tracing app has barely been used—*just one person has been reported to have been identified using data from it*[4]. And the language from public officials has been toned down. No longer is it the key to freedoms, but an add-on to existing contact tracing methods, to work in concert with social distancing rules and continued testing to keep a lid on outbreaks.

À Singapour, le développeur de l'application TraceTogether a lui-même fait valoir dans un article que cet outil de notification a été moins utile et efficace qu'anticipé au départ.

> Jason Bay, the product lead for Singapore's has also warned against the "technological triumphalism" that all too often accompanies automated solutions, explaining that you cannot ""big data" a way out of a 'no data' situation." "If you ask me whether any Bluetooth contact tracing system deployed or under development, anywhere in the world, is ready to replace manual contact tracing, I will say without qualification that the answer is, No," he wrote in a Medium post.

Cela dit, ni les applications ci-dessus ni les autres applications de notification déployées jusqu'ici dans le monde n'ont utilisé une approche prédictive tirant partie des symptômes, comme le fait l'application COVI de Mila. Celle-ci se démarque de celles qui ont été lancées à ce jour par l'inclusion d'un module d'apprentissage automatique.

À ce propos, Yoshua Bengio précise que les améliorations rapportées dans la présente version du livre blanc de Mila sont le résultat d'une étude épidémiologique par simulation. Elles restent à être validées par un véritable essai avec déploiement de l'application.

Cette crise a des composantes biologiques, sociales, politiques et émotives dont la résolution requiert l'application de différentes approches. Il faut prendre garde au technosolutionnisme et veiller à ne survendre aucune application, quelle qu'elle soit.

[4] Nos italiques

Une des approches qui nous apparaît en tout temps judicieuse pour contrer le technosolutionnisme[5] est celle faisant appel à la participation[6] des parties prenantes au design d'une application en formulant leurs besoins et leurs attentes quant aux fonctionnalités à implanter et leurs craintes quant à l'utilisation des données personnelles. Dans le domaine des technologies, le design d'un outil se fait parfois sans impliquer la population et l'ensemble des acteurs.

Yoshua Bengio note que les ministères fédéraux de la santé et de l'innovation, science et développement économique, ainsi que l'Agence de santé publique du Canada, ont pris part au design de COVI. Les autorités de santé publique ont été impliquées dès la fin mars 2020. De plus, plusieurs changements ont été apportés au design de COVI pour répondre aux besoins exprimés par des autorités de santé publique provinciales, dont le Ministère de la santé de l'Ontario et le Ministère de la santé de la Colombie-Britannique. Des consultations ont également eu lieu auprès d'autres autorités, dont la Direction de la santé publique de Montréal. Les artisans de COVI souhaitent aussi consulter la direction centrale de la Santé publique du Québec et le ministère de la Santé et des Services sociaux afin qu'ils participent aux prochaines étapes de son développement et déploiement.

La notion de conception éthique (*ethics by design*) va bien au-delà de la simple énonciation de principes éthiques généraux qu'il faut respecter et couvre un champ plus large que celui de la seule vie privée. C'est en incluant tous les acteurs interpellés par la conception et le déploiement d'une solution aux discussions relatives à cette dernière, et en tenant compte de l'ensemble des enjeux perçus par ces acteurs qu'il est possible de bien contextualiser les choix technologiques à faire et d'intégrer des balises éthiques exigeantes dès le départ.

L'inclusion de toutes les parties prenantes au processus de développement d'une application favorise en premier lieu la bonne évaluation de sa plus-value. Elle permet ensuite, lorsqu'il a été précisé que le projet est pertinent, de composer et de déterminer les finalités, les objectifs et les caractéristiques de l'outil envisagé. Elle permet d'entendre les acteurs et les groupes potentiellement touchés par l'application, d'intégrer leurs préoccupations et de sensibiliser les développeurs aux diverses réalités sociales avec lesquelles il importe de composer. Elle sert à mieux évaluer la nature des impacts potentiels de l'application. Cette démarche de consultation inclusive favorise enfin le développement de la capacité des individus à exercer un meilleur contrôle de leurs actes.

---

[5] Le technosolutionnisme, comme le rappelait récemment Jocelyn Maclure, président de la Commission de l'éthique en science et en technologie, est la tendance à présenter « les innovations technologiques comme des réponses nécessaires ou particulièrement efficaces à des problèmes sociaux complexes et persistants ».

[6] La participation active du public va au-delà de la transmission d'information et peut prendre différentes formes telles que la consultation, la concertation ou la co-construction. Voir en ce sens le Guide de planification d'une démarche de participation publique du Secrétariat à l'Accès à l'information et à la Réforme des institutions démocratiques.

Au final, l'adoption d'une approche de conception éthique permet de construire la confiance, de jeter les bases d'un processus d'acceptabilité sociale plus large auprès de la population en général. Elle diminue les risques de faire travailler les développeurs sur des solutions qui répondent inadéquatement aux besoins, qui visent les « mauvais » problèmes ou qui s'attardent à des problèmes qui ne sont pas prioritaires.

L'intégration du public, en général, dans la conception de COVI pourrait en particulier contribuer à éliminer les obstacles à son adoption par certains groupes, comme les groupes marginalisés.

À ce sujet, Yoshua Bengio précise que la direction de COVI a réfléchi aux enjeux concernant les groupes marginalisés et a élaboré un plan pour les inclure dans la structure de l'organisation. De plus, la direction de COVI inclut notamment un avocat spécialisé en droits de la personne dont le mandat est lié à l'inclusion des populations dites vulnérables dans la construction de la technologie et sa gouvernance. Nous nous sommes également assurés, dit Yoshua Bengio, de présenter dans le livre blanc un plan de surveillance et de correction pour veiller à ce que le prédicteur fonctionne aussi bien pour ces groupes que pour la population en général. Ceci contribuera à éviter des biais possibles dans les données

Cette préoccupation de représenter les intérêts des populations vulnérables par une personne experte constitue certainement une étape significative, elle ne peut cependant pas remplacer un processus de consultation directe avec les groupes concernés. En effet, plusieurs groupes marginalisés s'opposent maintenant aux principes de données ouvertes et à la notion d'inclusion. Selon ces groupes, ces notions cachent des problèmes plus profonds de non-représentation ou de mauvaise représentation au sein des données déjà existantes. Ces groupes ne doivent pas être consultés seulement une fois que les technologies ont été développées et, donc, ladite inclusion ne doit pas se faire que dans des termes définis unilatéralement par les organisations qui développent une application. Les bases de données représentent un construit qui ne prend pas toujours en compte les relations de pouvoir ni les inégalités sociales. Elles peuvent enchâsser des dynamiques sociales inégalitaires qui peuvent se trouver par la suite reproduites à un niveau structurel.

Pour s'assurer de développer un outil pertinent qui réponde aux besoins et priorités réels de la santé publique et de la population, il sera enfin capital de déployer un processus de consultation inclusif auquel les différents groupes concernés par l'utilisation d'une application comme COVI peuvent prendre part afin de rendre plus explicites les enjeux reliés à son usage. Certes, le contexte de la crise COVID-19 et le confinement ont eu pour effet que les relations de la société avec la technologie n'ont pu faire l'objet de discussions démocratiques. Bien que la situation évolue rapidement, il est possible d'organiser des délibérations sur le sujet. Les outils de notification de contact ne deviendront des outils efficaces que s'ils obtiennent la confiance du public, et ils n'obtiendront cette confiance que si ces outils sont bien expliqués (principes éthiques d'explicabilité et de respect de l'autonomie) et compris par toutes et tous.

Robustesse de COVI

Pour aller plus loin que les simulations épidémiologiques, il serait éventuellement recommandé d'effectuer un déploiement pilote de COVI sur le terrain. Cependant, compte tenu des risques liés au caractère sensible de ce genre de données, de l'historique de la propagation du virus dans certains quartiers et des effets que engendrés sur la stigmatisation des populations qui les habitent, il sera impératif que le déploiement se fasse en fonction des règles éthiques de la recherche menée avec des êtres humains, en toute collaboration avec la population concernée et avec leur consentement obtenu de manière préalable avant tout déploiement sur le terrain. Les résultats de tests permettraient de lever une partie de l'incertitude qui existe quant à la robustesse de COVI, mais rien dans le livre blanc de Mila n'indique que l'application a été mise à l'épreuve, à échelle réduite, dans des conditions aussi proches que possible de celles de la vie réelle au Québec ou au Canada. Comme mentionné précédemment, des simulations épidémiologiques sont présentées (figure 1 du livre blanc), mais peu de détails sur les hypothèses sous-jacentes à celles-ci sont fournies. Une façon de valider la robustesse de l'approche serait de présenter différents scénarios pour couvrir les différentes situations qui pourraient être rencontrées relativement aux éléments encore inconnus avant le déploiement de l'application (taux d'adoption, performance de la détection de contacts, performance de la prédiction du risque).

SwissCovid fait l'objet de tests

D'autres États ont réalisé des tests avant d'approuver le lancement à grande échelle d'une application de notification de contacts. Par exemple, le responsable de SwissCovid, l'Office fédéral de la santé publique de Suisse, a commencé à tester cette application en mai et il la mettra à l'épreuve pendant plusieurs semaines auprès du personnel de l'armée suisse, de certains hôpitaux et de certaines administrations régionales. L'objectif de l'Office fédéral est de commencer à recueillir des données réelles et de déployer l'application dans l'ensemble de la Suisse au mois de juin.

En l'absence d'information sur la tenue ou non de tests rigoureux, il est actuellement impossible de savoir si le modèle épidémiologique privilégié par Mila est réellement robuste.

> Nonobstant le fait que le modèle épidémiologique de COVI intègre les données les plus récentes de la littérature sur la COVID-19, celui-ci demeure une approximation de la réalité. La validité des résultats obtenus par simulation pour la prédiction du risque reste à vérifier, et c'est le genre de modèle où la différence entre la modélisation et la propagation de la COVID-19 en pratique peut être importante, au point d'être radicale si le modèle n'inclut pas des éléments essentiels, ici la physique du mécanisme de détection de proximité. De plus, ces modèles de simulations sont souvent calibrés pour évaluer l'effet de différents scénarios sur des populations, l'applicabilité pour la prédiction du risque individuel étant plus périlleuse. Lors des premières semaines ou

premiers mois, il est donc possible qu'il y ait des erreurs importantes dans les prédictions de niveau de risque faites par COVI, jusqu'à ce que suffisamment de données soient récoltées sur le terrain afin d'ajuster le modèle de simulation.

Yoshua Bengio souligne que l'avantage de l'approche prédictive proposée est que les données récoltées permettront justement d'ajuster les constantes épidémiologiques du modèle.

On peut en outre s'interroger sur le fonctionnement du module d'apprentissage automatique qui serait intégré à l'application. Selon les experts de l'OBVIA, le modèle proposé semble approprié et bien réfléchi sur papier, mais beaucoup d'éléments devront être validés en pratique. Même si Mila dispose d'une expertise remarquable sur le sujet, il ressort que les applications sont assez difficiles à bien faire fonctionner du premier coup. Des ajustements délicats devront être réalisés au fur et à mesure que s'accumuleront les données provenant des cellulaires des usagers. Beaucoup d'essais devront être menés pour déterminer ce qui fonctionne bien et moins bien, pour éviter que le modèle sous-prédise pour les cas à risque (ce qui mènerait à des contaminations qui auraient pu être évitées) et surprédise pour les cas positifs (ce qui provoquerait des quarantaines inutiles).

Yoshua Bengio apporte des précisions quant à l'approche choisie. Il note que ce qui est intéressant avec l'approche prédictive c'est qu'en simulation, elle donne lieu à moins de quarantaines que le traçage de contacts binaire. Il est important de noter que le problème de quarantaines inutiles qu'occasionne le traçage binaire a aussi été soulevé par une étude que des chercheurs de l'Université Oxford réalisait récemment sur le traçage de contacts[7]. La proposition de COVI est de réduire le nombre de ces quarantaines inutiles grâce à son approche prédictive et l'utilisation des symptômes. Elle est la seule à ce jour qui utilise cette approche.

En outre, il faut réaliser que la qualité de la performance de COVI reposera sur l'estimation robuste de la distance à une source possiblement infectée[8]. Le problème le plus grave des applications qui utilisent le Bluetooth BLE est la non-fiabilité des mesures que permet cette technologie, qui n'a pas été conçue pour mesurer les distances (ses spécifications ne concernent que l'éloignement minimal joignable[9]). Des considérations relatives à la puissance émise et le diagramme de rayonnement des antennes des téléphones intelligents devraient minimalement être prises en compte dans le modèle d'estimation de proximité entre deux dispositifs.

[7] Voir à cet effet, l'étude d'Oxford : Digital contact tracing can slow or even stop coronavirus transmission and ease us out of lockdown.

[8] Cette estimation constitue le point de départ incontournable de la chaîne de traitements, interprétations, diagnostics, anticipation, modélisation, et décisions ultérieures, pour l'individu et pour les autorités sanitaires.

[9] Voir à ce sujet le document Exposure Notifications - Android API Documentation.

La non-robustesse des mécanismes de détection de distance de Bluetooth BLE est le talon d'Achille de tous les outils de notification de contacts. Il ne s'agit pas d'un problème lié seulement à COVI, d'une question d'informatique ou d'intelligence artificielle qu'il est possible à un expert ingénieux d'aborder avec facilité, mais bien d'une question de propagation des ondes électromagnétiques. Le comportement physique de ces dernières dépend de différents facteurs, comme la topologie d'un lieu ou la géométrie des obstacles qui y sont présents. La présence de ces facteurs mène à des variations d'intensité substantielles du signal qui risquent à leur tour d'engendrer un grand nombre de fausses alertes (la circulation, autour de l'usager, de personnes contaminées qui respectent bien les règles de distanciation ne devrait pas être comptabilisée comme un danger nouveau).

Distance et risques de contamination

La non-robustesse de Bluetooth BLE (et forcément de COVI) comme outil de calcul des distances est d'autant plus préoccupante qu'une étude récente de The Lancet a montré que « nine key studies found that the transmission risk when people stood at least one meter away was around 3%, but rose to 13% when people were standing within one meter. The risk of transmission roughly halves for every extra meter of distancing up to three meters, the modeling suggested. » En d'autres mots, Bluetooth estime mal les distances, alors que le risque réel de propagation dépend très fortement de la distance précise qui sépare l'utilisateur de COVI des autres personnes dans son entourage.

Si l'utilisation de l'apprentissage automatique dans COVI a le potentiel de pouvoir pallier à l'imprécision des mesures, notamment via des prédictions probabilistes plutôt que binaires, l'essence hautement contextuelle de ces imprécisions risque de poser des défis lors de la mise en place de solutions[10].

Il serait ainsi important pour Mila de bien examiner les conséquences possibles de ces erreurs sur la fiabilité de COVI. Il serait aussi crucial que Mila prenne les mesures nécessaires pour bien présenter les limites de Bluetooth BLE au grand public et aux autorités et, ainsi, les aider à faire une évaluation juste des risques et des bénéfices associés à l'utilisation de COVI.

Yoshua Bengio relève que le fait d'utiliser l'apprentissage automatique pour intégrer plusieurs sources de mesures (par exemple plusieurs contacts et rapports de symptômes), chacune de ces mesures étant incertaine, permet d'obtenir une réponse graduée et probabiliste et évite d'avoir à prendre une décision grave, telle que mettre les gens en quarantaine ou pas, comme le ferait le traçage binaire sur la base d'une seule mesure incertaine. Le fait de ne pas produire une alerte binaire, mais plutôt un avertissement graduel, et d'intégrer toutes les mesures

[10] On peut envisager que le recours à des approches participatives (crowdsourcing) permettrait de corriger ce problème en partie. Cette approche est toutefois trop embryonnaire pour être développée ici.

incertaines, ce que fait COVI, permet de mitiger cet enjeu qui pose problème pour toutes les approches binaires.

Adoption de COVI

COVI ne sera pas la première application de notification lancée dans un État pour lutter contre le coronavirus. Comme ailleurs, le succès de COVI à cet égard dépendra en forte partie du niveau d'adoption de la solution par la société québécoise ou canadienne et par les différentes communautés la constituant.

Certains chercheurs doutent que sans coercition, l'application puisse être adoptée par un nombre suffisant de Québécois ou Canadiens pour fonctionner adéquatement[11].

Les simulations épidémiologiques faites pour évaluer l'effet du taux d'adoption sur l'efficacité du traçage de contact binaire suggèrent qu'il faudrait un taux d'environ 60% pour amener le R0 en dessous de 1. En réalité, un tel outil devrait être combiné avec d'autres mesures, comme la distanciation sociale.

Pour Yoshua Bengio, les simulations réalisées par des chercheurs d'Oxford concernent cependant le traçage binaire et il faudrait évaluer la robustesse de COVI par rapport au taux d'adoption de l'application. Par ailleurs, il est important de mentionner que COVI resterait utile pour produire des alertes par quartier même avec un taux d'adoption beaucoup plus faible puisque ces alertes dépendent de données agrégées et du fait que des utilisateurs rapportent leurs symptômes dans l'application.

On peut aussi déplorer que certains des groupes les plus frappés par le coronavirus comptent en fait parmi ceux qui seront les moins susceptibles de pouvoir adopter COVI On note ainsi que, selon les données du CEFRIO, 23 % des Québécois ne possèdent pas de téléphone intelligent, un taux qui grimpe à 32 % chez les habitants de la ville de Québec, à 45 % chez les travailleurs qui gagnent moins de 20 000 $ par an et à 48 % chez les personnes de 65 à 74 ans et 65% chez les 75 ans et plus.

On peut aussi penser qu'une partie de la population pourrait décider, pour d'autres facteurs que son non-branchement, de ne pas utiliser COVI.

Ainsi, il est indéniable que Mila a fait de grands efforts pour consulter les experts de différentes disciplines dans le cadre du développement de COVI (notamment des experts en droit). Toutefois, cette consultation semble s'être faite de façon relativement informelle, avec pour résultat qu'il est

[11] Un seuil d'adoption élevé, pensent certains, ne pourra être atteint à moins que l'utilisation ne soit imposée comme seule une autorité totalitaire peut le faire. « Nous ne sommes pas en Chine, note un expert. Ça sera difficile, voire impossible à faire ».

difficile d'avoir une vue d'ensemble du processus de consultation et que différents acteurs sont intervenus dans les médias en portant un regard sévère sur l'opération. Ces interventions pourraient avoir des effets importants sur une partie de la population et sur certains groupes.

Ensuite, l'inclusion dans l'application de fonctionnalités qui n'ont rien à voir avec la notification de contacts pourrait avoir pour effet de repousser certains utilisateurs.

D'autre part, certaines communautés minoritaires constituant des groupes vulnérables en contexte de pandémie, du fait de conditions socio-sanitaires difficiles, risquent fortement de percevoir la notification de leurs contacts comme une mesure supplémentaire de contrôle et de coercition imposée par la société majoritaire. Par exemple, les Premiers Peuples, qui ont développé des pratiques de souveraineté des données, pourraient ne pas vouloir du tout interagir avec l'application et ne pas collaborer avec l'OBNL qui gère les données. Nombreuses sont les communautés autochtones qui refusent la collecte et l'usage de leurs données si cela ne se fait pas en toute collaboration avec les développeurs. Ces groupes ont développé des protocoles de collaboration. Il existe également au Québec un institut de recherche en santé et services sociaux organisme géré par et pour les Premières Nations, la Commission de la santé et des services sociaux des Premières Nations du Québec et du Labrador[12]. Cet institut collecte des données à partir du concept autochtone de santé. À la lecture du livre blanc, il est cependant difficile d'évaluer quelles mesures seront prises pour collaborer avec ces groupes et ces communautés.

COVI et groupes particuliers

Un contre-argument aux critiques exprimées quant à la nécessité que 50-60 % des Québécois ou Canadiens doivent adopter l'application pour que celle-ci soit très efficace est que cette application pourrait très bien fonctionner dans les groupes particuliers qui l'adopteront de façon marquée. Par exemple, on peut penser que le taux d'adoption chez les étudiants et le personnel universitaires sera beaucoup plus élevé que dans d'autres milieux (comme celui des personnes âgées ou celui des personnes économiquement désavantagées). Donc, il est possible que COVI donne de bons résultats dans le milieu universitaire (même si, en fin de compte, les différences entre milieux favorisés-technophiles et défavorisés-moins connectés se seront accentuées).

Pour maximiser l'adoption aussi large que possible de COVI ou de toute autre application, il faudra d'abord et avant tout veiller à organiser un véritable débat public sur les applications de notification de contacts.

Seule une conversation étendue impliquant les développeurs, le public, les communautés les plus vulnérables du Québec ou du Canada et l'ensemble des acteurs susceptibles d'évaluer COVI et toute autre application semblable permettra de bien comprendre le fonctionnement de ces outils (par

[12] Assemblée des Premières Nations du Québec et du Labrador – APNQL, Protocole de recherche des Premières Nations du Québec et du Labrador, Wendake, 2014, 98 pages.

exemple d'informer le public pour qu'il prenne conscience du souci que les concepteurs ont eu, ou non, à protéger la vie privée et la sécurité de leurs données), de mesurer leurs impacts en tous genres et d'échanger sur les recommandations à appliquer pour assurer leur déploiement efficace et responsable et leur appropriation (par exemple, des recommandations sur la manière de solliciter le consentement des utilisateurs).

Entre-temps, les développeurs de COVI devraient notamment rendre public, comme ils prévoient de le faire, le code informatique de l'application pour permettre son analyse poussée par différentes communautés, dont celle des chercheurs (au 1er juin 2020, ce code demeurait inaccessible).

Les développeurs gagneraient aussi à produire des outils techniques, en langue française (et non seulement en langue anglaise), qui permettent à l'ensemble des parties prenantes de très bien comprendre le détail intime du fonctionnement de COVI. En effet, le livre blanc actuellement disponible est d'abord et surtout un document de design. D'autres documents seront nécessaires pour rendre transparentes les modalités techniques d'apprentissage du prédicteur IA [lequel ressemble beaucoup à une boîte noire, actuellement, même s'il est dit dans le livre blanc que l'IA rendra cette application si différente des autres outils du genre et si sécuritaire]. Ces modalités sont par exemple celles d'évaluation des probabilités individuelles de contagiosité et celles de prise en compte des variations de force de signal et d'évaluation des distances entre appareils.

En conclusion, différents défis devront être relevés pour maximiser l'utilisation de l'application par la population, mais le rejet, par les développeurs, de stratégies comme celle des incitations dites douces (*nudging*) doit être souligné et salué. Ce rejet paraît entre autres choses susceptible d'augmenter la confiance du public dans l'application et, en fin de compte, de contribuer à son adoption. Les développeurs notent à plusieurs endroits de leur document qu'ils souhaitent adopter une perspective coopérative axée sur la communication et la collaboration avec le public. Plusieurs études montrent que cette perspective est plus efficace et aussi plus respectueuse des droits fondamentaux et des libertés individuelles que celle des incitations douces, qui est une méthode basée sur la persuasion pouvant créer une certaine dépendance auprès de groupes vulnérables.

Protection de la vie privée

Pour assurer la confiance du public et l'adoption large de COVI, il sera important de bien protéger le caractère confidentiel des renseignements personnels des usagers, notamment quand cela touche à leur santé. Mais assurer le plein respect de la vie privée des utilisateurs de technologies est aussi, en soi, un impératif dans une société démocratique comme la nôtre.

Il ne fait aucun doute que l'équipe pilotée par Mila a porté une très grande attention à cette question dès le début du projet COVI et a cherché à intégrer la protection de la vie privée dès la conception (*privacy by design*). Le document de Mila traduit en fait une réelle volonté de mettre en place une application qui soit en mesure à la fois d'apporter une solution concrète à la crise sanitaire actuelle et de bien protéger les droits fondamentaux et les libertés individuelles, surtout en ce qui a trait au droit à la vie privée. Par exemple, le livre blanc établit que les données sensibles resteront

décentralisées sur les téléphones et que les données centralisées (celles nécessaires, entre autres, à l'entraînement du prédicteur de COVI) seront placées dans une fiducie de données (ou quelque chose s'en approchant), sous la surveillance d'un OBNL.

Il est aussi louable que les auteurs du livre blanc précisent que le fait de choisir entre le respect du droit à la vie privée et la protection de la santé publique est un faux dilemme. Il est possible, voire même nécessaire, d'arrêter d'appréhender la relation entre le droit à la vie privée et d'autres intérêts collectifs (ex. : la santé, la sécurité, l'économie) comme étant conflictuelle et antinomique.

Nous saluons le fait que Mila ait réalisé une analyse d'impact relative à la protection des données et sur la vie privée (*privacy impact assessment*, ou PIA) pour minimiser les risques de dérapage de l'application en amont et pour vérifier dans le temps (au fur et à mesure que COVI est utilisé et que des données sont collectées) si les principes de protection de la vie privée et des renseignements personnels sont bien pris en compte. Selon la *Loi sur la protection des renseignements personnels et les documents électroniques* du Canada, il n'y avait pas d'obligation pour les acteurs comme Mila de mener une telle étude d'impacts.

La réalisation d'une analyse d'impact relative à la protection des données et sur la vie privée permet à Mila d'être en conformité avec le *Règlement général sur la protection de données* (RGPD) qui est en vigueur depuis mai 2018 dans toute l'Union européenne. La réalisation de cette étude témoigne d'une bonne pratique et contribue à augmenter la confiance des parties prenantes.

La réalisation rigoureuse et transparente d'une évaluation formelle des incidences de COVI sur la vie privée va aider Mila à nommer les principaux points de risque à traiter pour assurer la protection de la vie privée, puis à définir la manière dont ces risques ont été atténués ou le seront (par exemple, dans la conception technique, le processus de mise en œuvre et le processus de surveillance).

Cependant, quelques questions relatives à la protection de la vie privée des usagers de COVI gagneraient à être abordées ou clarifiées.

La notion de consentement est ainsi un enjeu clé. Il est important que les utilisateurs d'une application puissent accepter ou refuser que son promoteur l'utilise pour recueillir ou distribuer certaines des données qui se rapportent à eux. Il est aussi impératif que les utilisateurs comprennent très bien ce à quoi ils acquiescent, exactement, quand ils donnent leur consentement au promoteur.

Il paraît clair dans le livre blanc que Mila prend au sérieux la notion de consentement. On peut ainsi s'attendre, selon le document, à ce que les explications fournies aux usagers pour qu'ils comprennent ce à quoi ils adhèrent soient simples et à ce que Mila vérifie le niveau de compréhension des usagers. Cela dit, Mila devra prendre des mesures pour que les utilisateurs donnent leur consentement de manière éclairée, libre et continue.

Il faudra ainsi que les utilisateurs obtiennent toutes les informations nécessaires pour comprendre les avantages et les limites de leur utilisation de COVI, et aussi savoir qu'ils peuvent cesser d'utiliser l'application à tout moment. Lors de l'abandon de l'application, les utilisateurs devront savoir que

leurs données seront conservées dans une entité indépendante et détruites lorsqu'elles ne seront plus nécessaires, au plus tard après 90 jours, ou immédiatement si leur consentement est révoqué. Ils devront aussi être rassurés sur le fait que cet abandon n'aura pas de conséquences négatives directes sur leurs libertés.

En outre, il est important pour Mila de s'assurer que les usagers prennent la notion de consentement au sérieux, notamment en évitant de leur demander ce consentement trop souvent. Le consentement doit être demandé pour chaque finalité et prolongation dans le temps de l'utilisation des données, mais le demander trop souvent crée un effet pervers : cela revient à ne plus donner un caractère aussi fort à l'expression du consentement. Le design du mode de collecte du consentement est aussi important. Il faut par exemple éviter le choix d'un modèle de type « pop up » basé sur l'ouverture intempestive de fenêtres qui gênent l'expérience de l'utilisateur, qui peut seulement s'en débarrasser en acceptant les conditions présentées par les développeurs. En sollicitant le consentement séparément pour différents éléments d'informations personnelles et en rendant le consentement facultatif dans la mesure du possible, Mila montre son intérêt à conserver le consentement manifeste et significatif.

Mila devra de plus trouver une solution à une difficulté majeure, celle voulant que COVI serve actuellement à atteindre plus d'un objectif à la fois. En effet, le fait de poursuivre plusieurs objectifs avec une application crée une ambiguïté, notamment sur la nature des données collectées (respect du principe de limitation). Selon le livre blanc, COVI veut à la fois automatiser la notification de contacts (niveau micro) et permettre la collecte d'informations pour modéliser l'épidémie et soutenir les politiques publiques de santé à des fins de recherche (niveau macro). Tout en excluant les pouvoirs publics et les autorités de santé de l'accès direct aux données personnelles, ces données vont être collectées en raison de ce deuxième objectif et on peut contester le cumul des objectifs et fonctions, même s'il semble dans le document qu'un consentement devrait être exigé par les développeurs pour chaque finalité. Bien que Mila choisisse explicitement de ne pas partager les données personnelles pour protéger la vie privée des utilisateurs, le principe de finalité n'est pas respecté si on cumule les finalités avec un système unique qui va collecter toutes les données pour l'ensemble des finalités. Il sera porté atteinte au principe de finalité qui concerne chaque traitement isolément. Il risque en conséquence d'être aussi porté atteinte aux principes de nécessité et de limitation.

Yoshua Bengio fait cependant remarquer que c'est l'unique fonctionnalité principale, soit de pouvoir fournir un prédicteur de risque dans chaque téléphone, qui mène aux deux finalités, soit d'une part de calculer ces niveaux de risque sur les téléphones à partir des signaux reçus des autres téléphones, et d'autre part de centraliser des données dé-identifiées qui servent à entraîner le prédicteur de risque mais aussi, une fois agrégées (et comme effet secondaire bénéfique) à informer la santé publique. En effet, pour pouvoir appliquer le prédicteur de risque dans chaque téléphone, il faut d'abord pouvoir l'entraîner sur des données centralisées et sécurisées.

De plus, les développeurs de COVI entendent recourir aux techniques d'apprentissage automatique pour notifier un individu plus tôt que les outils de notification de contacts plus classiques permettent de le faire. Cependant, ce dernier objectif conduit à la collecte de beaucoup plus de données sur l'utilisateur, telles que ses données sociodémographiques, des informations sur sa santé ou encore sur ses déplacements.

En conséquence, pour respecter les principes de nécessité, de proportionnalité, de finalité et de limitation des données collectées, il est important, comme le propose le livre blanc de COVI, qu'un consentement clairement différencié soit demandé pour la fonction de collecte des données d'une part et pour la fonction d'échange de niveaux de risques entre les téléphones, d'autre part. Le design et l'information éclairés sont nécessaires ici. Par exemple, il est loin d'être sûr que pour faire la notification de contacts, il soit nécessaire et proportionné de collecter les données relatives au sexe et à l'âge. Cela n'est utile que pour la finalité de recherche. Il devrait être possible et facile pour l'usager de choisir une seule des deux options de collecte offertes, ou les deux. Par ailleurs, afin de bien respecter le principe de limitation de la collecte des données, il serait nécessaire de bien distinguer les deux finalités de COVI et que les données collectées soient effectivement limitées à ce qui est nécessaire à chaque usage.

Yoshua Bengio relève que COVI ne fait pas de la simple notification de contacts mais est basé sur un prédicteur du risque (calculé pour envoyer les notifications au niveau approprié d'alerte), et que celui-ci pour être efficace dépend (en entrée) des réponses volontaires aux questionnaires médicaux (dont le sexe et l'âge, et surtout l'âge, sont connus comme des facteurs importants pour la COVID-19). Donc cette critique sur la nécessité et la proportionnalité de la collecte des données relatives au sexe et à l'âge ne s'applique pas à COVI. COVI n'est pas un système de notification plus un système de recherche épidémiologique mais bien une seule finalité, la prédiction du risque, qui peut servir à envoyer des alertes à différents niveaux et aussi fournir de l'information épidémiologique à la santé publique. Par contre, l'usager peut consentir à l'échange de notifications provenant du prédicteur de risque sans consentir au partage de ses réponses aux questionnaires médicaux. Il suffit qu'une fraction de la population donne son consentement au partage de ses réponses médicales pour que le prédicteur de risque (qui sert à tous) puisse être entraîné.

La loi prévoit en outre qu'un utilisateur puisse retirer son consentement et exiger que le fournisseur d'une application détruise les données qu'il a recueillies sur lui. Selon l'analyse du livre blanc, les données personnelles présentes dans l'appareil des Canadiens et dans les serveurs des promoteurs de COVI seraient effacées sur une base régulière. Lors de la rencontre du 8 mai avec les chercheurs du comité Covid-19 de l'OBVIA et les développeurs de COVI ont confirmé qu'au moment où un utilisateur supprimait l'application, le modèle était ré-entraîné pour permettre la destruction complète des renseignements personnels intégrés au modèle.

La pseudonymisation des données[13] est une autre question majeure soulevée dans le document. Il ressort de ce dernier que les données agrégées par les développeurs seront pseudonymisées. En particulier, si jamais un individu souhaite contribuer à la deuxième finalité (c'est-à-dire la collecte de données pour aider à comprendre l'épidémie), ses données seront envoyées de manière pseudonymisée à COVI Canada, l'organisme chargé de centraliser les données des participants. Il s'agit là d'une mesure de sécurité et de protection minimale des données personnelles, mais il importe de rappeler que la pseudonymisation n'est pas une solution miracle : les données pseudonymisées restent bien personnelles et des risques majeurs de réidentification existent, notamment en cas de fuite de données. Par conséquent, les développeurs de COVI devraient s'assurer d'informer les utilisateurs que les risques d'atteinte à la vie privée ne sont pas nuls, malgré que les données soient pseudonymisées et que des précautions soient prises.

Rien dans le document de Mila ne laisse en outre penser qu'il soit possible aux usagers de fermer complètement COVI, de mettre l'application à off sans que celle-ci ne s'en remette ensuite, à sa réouverture, à l'historique (ex. : au GPS intégré dans le téléphone) pour voir ce que les usagers ont fait pendant sa désactivation. Il serait intéressant, note une chercheuse de l'OBVIA, qu'une telle option soit envisagée par les développeurs, notamment « pour contribuer à nourrir le sentiment de coopération et de confiance des usagers, pour éviter de leur donner l'impression qu'une fois COVI installé, COVI suit tout ce qu'ils font en permanence ».

Au vu de ce qui précède, il faudrait que Mila réfléchisse à la manière dont l'architecture de COVI devrait être repensée pour mieux intégrer la limitation des données. Contrairement à d'autres contextes où il est parfois possible de concilier l'utilité des données avec un fort niveau de vie privée, dans le contexte de COVI il semble y avoir une tension forte entre la capacité d'estimer à un niveau très fin le risque d'exposition d'une personne et la limitation de la collecte et de la circulation des données sensibles sur les individus. Même s'il s'agit d'une question difficile à résoudre dans le contexte où la connaissance de la maladie se construit chaque jour, il convient de chercher à identifier les données qu'il est vraiment nécessaire de collecter pour que le prédicteur de risque fonctionne et celles qui, au contraire, ne sont pas indispensables.

Et les groupes dans tout cela ?

Fait à souligner dans le document, les développeurs de COVI entendent prendre des mesures poussées pour faire en sorte qu'il ne soit pas possible, en analysant les données recueillies par l'application, de retracer une personne atteinte du Covid-19 et son trajet. Toutefois, le livre blanc n'aborde pas les enjeux liés à la stigmatisation et la discrimination que COVI pourrait faire courir

[13] La pseudonymisation est « le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles garantissant que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable ».

à des communautés entières en permettant d'identifier certains quartiers comme quartiers chauds.

La question de l'emplacement des serveurs est importante lorsqu'on parle de protection de la vie privée des usagers d'une application informatique. On ne trouve cependant rien dans le livre blanc qui annonce clairement que les serveurs des promoteurs de COVI seront en sol canadien. « On peut s'en douter, mais il serait sans doute utile de voir cette précision dans le document ».

Le document reconnaît par ailleurs de manière implicite que l'OBNL qui sera mis sur pied pour gérer les données de COVI serait soumis à la *Loi sur la protection des renseignements personnels et les documents électroniques* et à la *Loi sur la protection des renseignements personnels dans le secteur privé* (ce qui ne va pas nécessairement de soi puisque ces lois ne s'imposent qu'aux entités qui conduisent des activités économiques). Mais il serait peut-être intéressant que les développeurs de COVI reconnaissent de manière plus explicite qu'ils accepteront de se soumettre à ces deux lois. Encore une fois, un engagement direct et sans équivoque nourrirait la confiance du public.

Finalement, le Commissariat à la protection de la vie privée du Canada et la Commission d'accès à l'information du Québec n'ont qu'un pouvoir de recommandation selon les lois actuelles. Toujours de manière à rassurer le public, il serait sans doute indiqué que les développeurs (1) s'engagent à respecter, le cas échéant, les recommandations que ces deux entités gouvernementales pourraient être invitées à formuler aux termes d'une enquête sur COVI ou, minimalement, (2) que les développeurs justifient publiquement les raisons qui pourraient justifier qu'ils s'écartent de ces recommandations dans certaines circonstances. Le Commissariat à la protection de la vie privée du Canada et la Commission d'accès à l'information du Québec ont rappelé les principes des lois sur la protection des renseignements personnels et la nécessité de les respecter. Un renvoi à ces déclarations officielles serait de nature à renforcer la confiance.

Assurer la sécurité des données

La protection des données des usagers contre les attaques de toutes sortes est un enjeu lors du lancement de toute application informatique. L'équipe de COVI démontre en matière de sécurité une volonté louable de protéger la vie privée et les informations personnelles des usagers. Des efforts conséquents ont ainsi été consentis afin d'anticiper et repousser plusieurs types d'attaques qui viseraient à dévoiler le statut médical des usagers de l'application ou leur historique de déplacements. Les développeurs proposent aussi des mesures d'atténuation reposant notamment sur des solutions techniques de cryptage des données.

Le document de Mila évoque aussi le point de vulnérabilité principal de COVI en matière de sécurité, lequel réside dans le stockage des données pseudonymisées de centaines de milliers, voire de

millions de Canadiens, sur un serveur d'apprentissage automatique (COVI ML Data Collection Server).

Le document reste cependant beaucoup plus discret sur les procédures de sécurité mises en œuvre pour protéger ce serveur. En effet, on sait que des campagnes d'espionnage via des cyberattaques ciblent des entreprises pharmaceutiques et des universités de recherche afin de recueillir des renseignements utiles à des gouvernements étrangers sur la Covid-19. On peut donc aisément imaginer que l'application COVI sera ciblée, surtout si elle rencontre un grand succès auprès de la population. Il est donc vital de s'assurer que la structure qui sera créée se dote des outils de cybersécurité les plus robustes (ce qui a un coût financier non négligeable), et que les chercheurs en IA qui vont travailler sur ces données soient aussi formés à cette réalité et aux bonnes pratiques d'hygiène numérique. En effet, ces chercheurs vont constituer des cibles de choix pour les attaquants en raison de leur accès privilégié au serveur sécurisé.

En tout état de cause, il convient de rappeler que certaines bases de données, comme celles des prescriptions pharmaceutiques, contiennent des informations – de surcroît non anonymisées – desquelles un agent malveillant pourrait extraire un renseignement privé de la plus haute importance. Notre société contemporaine a apprivoisé cette contrainte – et vit quotidiennement avec ce « danger nécessaire ».

Le livre blanc évoque en outre le fait que des attaques potentielles pourraient être mises en œuvre par des cybercriminels afin d'utiliser l'application comme prétexte ou amorce dans des campagnes d'hameçonnage (*phishing*) et de distribution de logiciels malveillants (*malware*). Les auteurs mentionnent que les développeurs comptent beaucoup sur Apple et Google pour prévenir ces attaques en exerçant un contrôle sur leurs boutiques de téléchargement d'applications (app stores). Il s'agit sans doute là d'un vœu pieux, car on sait que ces plateformes ont beaucoup de difficulté à empêcher la distribution de logiciels malveillants. Il serait donc utile qu'un mécanisme de veille soit mis en place afin d'identifier très rapidement les tentatives frauduleuses d'exploiter la popularité espérée de COVI sur les plateformes de téléchargement d'application. Il serait aussi important que Mila prévienne les usagers des dangers encourus lors de toute installation ou mise à jour de l'application.

L'un des problèmes de sécurité principaux qui n'est pas abordé dans le livre blanc est le risque accru d'infection numérique via les téléphones mobiles que COVI fait peser sur ses utilisateurs. En effet, le protocole Bluetooth, qui est déjà largement utilisé sur les téléphones intelligents et a été privilégié pour tracer les contacts – continue à poser de nombreux problèmes de sécurité. En demandant aux usagers de COVI de rendre leur téléphone accessible en tout temps par Bluetooth (l'accessibilité permanente étant directement corrélée à l'efficacité de l'application), on augmente la surface d'attaque de ces appareils, qui vont être exposés à des risques d'infection ou de vol de données, non pas liées à COVI, mais grâce à la porte d'entrée ouverte par COVI dans le système d'exploitation. On peut imaginer aisément que plus l'application COVI sera populaire, plus elle rendra attrayantes aux yeux des cybercriminels les vulnérabilités Bluetooth. Les solutions à ce problème sont d'ordre technique, et COVI n'est évidemment pas responsable de la sécurité de l'ensemble des

écosystèmes qui gravitent autour de Apple et Google, mais les développeurs devraient au minimum offrir des instructions claires et faciles à suivre pour inciter les usagers de COVI à mettre à jour leur système d'exploitation (quel qu'il soit) et les paramètres d'utilisation de Bluetooth.

De plus, l'architecture de COVI requiert que tous les contacts qu'un utilisateur a croisés envoient chaque jour à son application, pendant deux semaines, une estimation de l'évolution de leur propre score de risque. Normalement, cette information est cachée à l'utilisateur par l'application elle-même, qui lui montrera simplement un score de risque global ou encore les recommandations de santé associées à ce score. Cependant, cette mesure de protection pourrait être facilement contournée par un adversaire qui réécrirait l'application en lui demandant, pour chaque contact qu'il a eu, d'enregistrer l'heure et l'endroit où il a croisé ce contact ainsi que la distance à laquelle se trouvait ce contact. Il deviendrait possible avec cette version modifiée de l'application de recevoir une estimation de l'évolution du score de risque de toute personne avec qui on a été en contact proche et qui possède l'application. Ainsi, on pourrait recevoir un bulletin de santé quotidien pour son voisin, son collègue de bureau, le vendeur d'un magasin fréquenté ou un inconnu croisé dans le bus. On peut aussi imaginer qu'un journaliste intéressé par suivre l'état de santé d'une personnalité publique pourrait le faire très facilement s'il arrive à être dans son entourage proche (ex. : un journaliste assistant au point journalier du premier ministre pourrait par la suite recevoir une estimation de son score d'exposition pendant deux semaines). Contrairement à une fuite de données contre une base centralisée qui demande potentiellement un attaquant motivé et disposant de ressources importantes, cette attaque pourrait être réalisée beaucoup plus facilement et servir à détourner l'infrastructure de COVI en un «Little Brother »[14].

Dans une veine un peu différente, l'article 10.1 de la *Loi sur la protection des renseignements personnels et les documents électroniques* précise qu'une entité doit avertir le Commissaire à la vie privée lorsqu'il y a un bris de sécurité et qu'il « est raisonnable de croire, dans les circonstances, que l'atteinte présente un risque réel de préjudice grave à l'endroit d'un individu. » Aucune obligation de cette nature n'apparaît dans la *Loi sur la protection des renseignements personnels dans le secteur privé* du Québec. Il serait tout de même indiqué que les développeurs s'engagent à notifier les utilisateurs de tout bris de sécurité, même si on ne perçoit pas de risque de préjudice grave. En effet, on pourrait dire que c'est la personne qui sait si c'est grave pour elle ou non en fonction de sa tolérance au risque, un facteur sur lequel les auteurs insistent dans le document. Cela devrait se faire dans tous les cas (même ceux, peut-être rares d'ailleurs, où la *Loi sur la protection des renseignements personnels dans le secteur privé* serait applicable).

Le document de Mila insiste avec raison sur les mesures techniques qui seront prises pour assurer la protection des renseignements personnels. La jurisprudence canadienne et l'actualité

[14] Les risques que cela survienne sont reconnus dans le livre-blanc : « Unfortunately, someone who has built a cracked version of the app in advance could have it record all of the contacts and associated risk messages, along with exact time and location of contact. [...] Our technical protocol does not attempt to prevent this premeditated attack, though we should note for completeness that an attacker only needs a cracked copy of the COVI app in advance, rather than additional physical phones. As it is not possible to prevent this attack technologically, we must explore legal and economic solutions instead. »

québécoise nous montrent en effet que la grande majorité des incidents de sécurité n'ont pas uniquement une cause technique. Beaucoup ont surtout une cause humaine (que l'on pense à l'affaire Ashley Madison ou Desjardins). La *Loi sur la protection des renseignements personnels et les documents électroniques* parle à cet égard de l'importance pour les organisations de prendre des mesures « administratives » qui sont liées aux politiques institutionnelles de formation, de sensibilisation et de mise à jour des membres du personnel qui ont accès aux données. Il serait important que les développeurs développent un peu plus sur ce point dans leur document.

Finalement, comme les diagnostics sont autorapportés, il y a un risque important que des groupes anti-COVI, ou simplement des personnes mal intentionnées sabotent l'application en rapportant des cas d'infection fictifs. Avec un flux de mauvais diagnostics rapportés de cette façon, les problèmes mentionnés précédemment risquent d'être exacerbés et provoquer des vagues de quarantaines inutiles dans des quartiers ou des groupes sociaux particuliers. Par exemple, en se déclarant pour le fun « COVID-19 positifs » dans l'application, des groupes de jeunes pourraient entraîner le confinement d'écoles entières et de leurs familles. Des solutions permettraient cependant de pallier ce problème assez facilement. Il a été proposé par les développeurs de COVI que la santé publique du Québec fournisse un code secret unique à chaque personne dépistée pour qu'elle entre ce numéro dans l'application. Bien appliquée, une telle approche serait raisonnable.

Concluons cette section en soulignant qu'en raison des enjeux importants en termes de sécurité informatique et de protection de la vie privée, il est crucial d'inclure la communauté informatique travaillant sur ces sujets dès que s'amorce le développement d'une application comme COVI. En particulier, il est important que l'architecture d'une l'application ainsi que son code puissent être évalués par des experts externes indépendants, ou même mieux, que le code source de cette application soit vite rendu disponible pour qu'il puisse facilement être examiné. Cette proposition a été mise de l'avant, avec neuf autres principes, dans une déclaration signée par plus de 100 chercheurs canadiens en sécurité informatique et protection de la vie privée[15].

Éviter les dérapages

Même avec la meilleure des planifications, le lancement d'une application peut avoir des impacts négatifs inattendus. Par exemple, il peut mener à la discrimination de certaines personnes tandis que l'accès à certains lieux ou services (ex. : des commerces ou des moyens de transport) peut devenir conditionnel à son utilisation par les citoyens. Tout développeur doit être en mesure de prévenir les problèmes et d'assurer des ajustements rapides lorsqu'il s'avère que des usagers font face à des conséquences négatives ou des problèmes éthiques imputables à son application.

Le livre blanc de Mila témoigne d'une préoccupation pour les questions d'éthique. Toutefois, ce souci éthique devrait aller plus loin et être complété par la mise en place d'une infrastructure éthique rigoureuse et indépendante. Cela implique d'abord de créer un comité ou une instance d'évaluation

[15] Waterloo Cybersecurity and Privacy Institute, Déclaration sur les applications de traçage COVID-19 respectueuses de la vie privée et dignes de confiance, 2020.

éthique multidisciplinaire et indépendante, laquelle serait formée et agissante dès les premières étapes de conception. Son mandat se poursuivrait tout au long du développement et du déploiement de l'application.

Cette instance indépendante devrait évidemment veiller à s'assurer que la vie privée et les données sont adéquatement protégées, mais elle devrait aussi s'assurer du respect d'un ensemble beaucoup plus large de valeurs et de principes (comme l'équité et la justice sociale, la santé ou la capacitation). Cette instance indépendante pourrait superviser et évaluer les résultats de tests menés préalablement au lancement d'une application.

Cette instance indépendante devrait par ailleurs mettre en place un processus de déclarations d'intérêts et de communication transparente avec le public afin d'assurer la transparence quant aux objectifs poursuivis par le développeur, de même que ses liens et sources de financement.

Il s'avère par ailleurs intéressant que l'application COVI soit développée et gérée par un OBNL formé notamment de chercheurs au lieu d'être aux mains exclusives d'une entreprise privée. Mais un OBNL n'est pas nécessairement sans intérêts économiques ou particuliers. Pour qu'une telle structure soit jugée avantageuse, elle devra par conséquent faire preuve d'une transparence et d'indépendance quant aux intérêts qui la sous-tendent, à la composition du comité qui la dirige et aux mesures qui ont été mises en place pour assurer sa gestion adéquate et la protection des données qu'elle gère.

La surveillance indépendante du développement et du déploiement de l'application par un organisme de certification indépendant ou un autre organe du genre viendrait avantageusement complémenter et renforcer l'instance d'évaluation éthique. Dans un document intitulé *COVI Canada - Corporate Structure and Governance*, Mila confirme dans une section « Independent Third Party Audit of App » que la structure de gouvernance de COVI sera soumise à un examen indépendant.

Une instance neutre et indépendante (un gardien de l'éthique publique existant ou encore l'instance d'évaluation évoquée précédemment) devrait aussi être établie pour permettre le signalement et le dépôt de plaintes par les personnes ou les groupes qui se considèrent comme traités injustement à cause de leur utilisation ou non-utilisation de l'application, ou encore qui se sont vus imposer l'obligation d'utiliser l'application. La création d'une telle instance a été prévue par les développeurs de certaines applications de notification de contacts ailleurs dans le monde.

Les échanges entre Mila et les chercheurs de l'OBVIA ont montré que Mila serait sans doute ouvert à la mise en œuvre des mesures ci-dessus, qui contribueront hors de tout doute à une hausse de la confiance du public.

Tenir compte du guide de l'OMS

L'Organisation mondiale de la santé (OMS) a publié le 28 mai 2020 un ensemble de considérations éthiques pour guider l'utilisation d'applications de notification de contacts dans tous les pays du monde. Ce guide comporte une liste de 17 principes que les développeurs des applications, ainsi

que leurs utilisateurs, devraient suivre en vue de garantir un déploiement effectif et responsable de ces applications, dans le respect des droits et libertés individuelles et collectives.

Mila et ses partenaires devraient s'appuyer sur le guide de l'OMS pour vérifier si COVI répond bien à ces critères éthiques et proposer éventuellement des solutions concrètes dans le cas où des insuffisances viendraient à être identifiées.

Tout comme les chercheurs engagés dans la rédaction du présent document, l'OMS met l'accent sur les principes de confidentialité et de proportionnalité dans la collecte et l'usage des données collectées par les applications de notification de contacts. Mais aussi, l'organisation internationale insiste sur l'importance du principe d'imputabilité (*accountability*), en rappelant que les utilisateurs doivent pouvoir remettre en question, voire contester, les informations et les recommandations issues des applications. Enfin, la mise en œuvre d'un comité d'évaluation indépendant pour évaluer les impacts des applications semble une proposition phare du guide de l'OMS. Dans le cas de COVI, un comité d'évaluation multidisciplinaire et multisectoriel indépendant (avec des représentants des diverses parties prenantes, par exemple des universitaires, la santé publique, la Commission de l'éthique en science et en technologie, des groupes communautaires ou la société civile) pourrait s'assurer que l'application remplit non seulement ses objectifs de protection et de suivi sanitaire, mais respecte aussi les lois en vigueur, les principes de responsabilité énoncés plus haut ainsi que les droits de la personne fondamentaux. Finalement, le cadre de l'OMS nous rappelle la nécessité d'inscrire le développement et l'utilisation des applications de notification de contact dans une perspective inclusive et pluraliste qui favorise la participation effective de diverses communautés, dont celles qui sont les plus vulnérables.

Assurer la bonne gouvernance du projet

Le modèle de gouvernance mis en place par les développeurs de COVI pour assurer le fonctionnement efficace et éthique de COVI est décrit sommairement dans le livre blanc. Il a aussi été présenté aux chercheurs de l'OBVIA lors de rencontres.

Le modèle de gouvernance choisi repose en forte partie sur la fondation d'un OBNL qui serait basée au Québec et gérerait l'utilisation qui serait faite des données recueillies grâce à COVI. Cet OBNL serait piloté par un groupe d'administrateurs provenant de différents secteurs et représentant différents groupes de parties prenantes. Ni Mila ni l'État ne la contrôlerait. L'application COVI a visiblement été conçue dans un souci de responsabilité et de bien commun, mais l'idée de confier à un OBNL la responsabilité d'encadrer son déploiement ne fait pas l'unanimité.

Certains chercheurs disent ainsi comprendre, sans nécessairement les endosser, les principes qui ont amené Mila à suggérer de créer un OBNL pour gérer une base de données ne contenant apparemment aucune information sensible, tout en trouvant difficile de concevoir qu'un tel OBNL

en vienne à se substituer à l'État, « comme si, a relevé un chercheur, on ne pouvait pas faire confiance à cet État pour gérer le bien-être de la population dans un contexte de pandémie qui dépasse largement la démocratie participative ».

D'autres chercheurs de l'OBVIA trouvent de leur côté le choix de créer un OBNL éclairé et prometteur. En effet, il s'agirait là selon eux de la meilleure manière d'assurer que l'État ne se serve pas des données colligées afin de s'ériger en un « Big Brother » capable de suivre tous les mouvements de ses citoyens.

L'opposition entre les deux positions ci-dessus traduit sans doute des divergences fondamentales entre différentes perceptions de l'État.

En ce qui concerne la fiducie de données qui sera mise sur pied, il sera important qu'elle ne se place pas au service exclusif de ceux qui ont développé COVI et que des chercheurs provenant de l'extérieur du groupe de développeurs (par exemple des biostatisticiens du gouvernement du Québec ou du monde universitaire capables de faire de l'analyse de données et de valoriser celles-ci dans le but de combattre le coronavirus) puissent y accéder. Il sera important d'éviter de créer un problème de concurrence entre les acteurs qui pourrait mener à un abus de position dominante.

Le livre blanc contient peu d'information sur la question de l'accès des chercheurs aux données, mais un document intitulé *COVI Canada - Corporate Structure and Governance* indique qu'il est prévu de le favoriser. Ce document stipule en effet que « the Access Committee is an operation level committee composed of technical experts with delegated authority from the directors of the Not-for-Profit ». Il aura entre autres la mission suivante : « Receiving and processing access requests from public health authorities and researchers on case by case basis, in accordance with Charter principles and general direction set by the Data Ethics Advisory Council ».

Il semble clair, comme mentionné précédemment, que seule l'organisation d'une consultation publique large permettrait en fin de compte de discuter des principaux enjeux associés au développement et au déploiement de COVI (ou de toute autre application) et, aussi, de mettre sur pied une structure de gouvernance de l'application qui réponde aux attentes de la population québécoise ou canadienne.

Cela dit, il sera crucial, comme prévu dans le document *COVI Canada - Corporate Structure and Governance*, que tous les acteurs aient le droit d'accéder aux données recueillies grâce à COVI pour combattre la Covid-19 en mettant en place les garanties appropriées. Il faudrait en fait que, quelle que soit la structure de gouvernance retenue, des mécanismes permettant à d'autres groupes de recherche d'utiliser les données de COVI de manière éthique et responsable, dans le plein respect de la vie privée des usagers et d'autres critères, et dans le but de faire progresser la science, soient définis.

Conclusion

Le débat sur les applications de traçage et de notification de contacts est à peine amorcé au Québec et au Canada que déjà il soulève des passions chez certains groupes. Nous souhaitons qu'il soit plus équilibré et qu'il soit élargi à l'ensemble de la population. Cela suppose que les développeurs de COVI, conjointement avec les acteurs de la santé publique, y aillent d'un réel effort de sensibilisation et de clarification auprès de tous les groupes concernés par la conception et le déploiement d'outils numériques.

Il est essentiel de construire la confiance en offrant de solides garanties scientifiques tout en mettant en place des mécanismes de vérification qui assureront l'intégrité du processus de développement et de déploiement. Nous pensons essentiel, aussi, de lutter contre la pandémie en combinant le recours volontaire à des outils numériques avec des moyens qui ont déjà prouvé leur efficacité sur le plan humain.

Ne perdons jamais de vue que l'innovation numérique pourra rapporter aux sociétés québécoise et canadienne et être utile pour affronter une nouvelle vague de pandémie pourvu que son développement et son déploiement soient encadrés et alignés avec les valeurs et les lois de ces sociétés.

Recommandations

Les travaux des chercheurs de l'OBVIA les ont amenés à émettre différentes propositions à travers ce document. Quatre propositions méritent en fin de compte d'être élevées au rang de recommandations qu'il importerait fortement pour Mila et les pouvoirs publics de suivre.

1re recommandation

Avant d'approuver ou de rejeter COVI (ou quelque application de notification de contacts que ce soit) ou de suggérer au public d'utiliser COVI (ou quelque application de notification de contacts que ce soit), tout gouvernement devrait instaurer un débat public qui permette :

- de soulever les principaux enjeux associés au développement et au déploiement de COVI (ou de toute autre application) ;
- de discuter démocratiquement du modèle de gouvernance qui pourrait être mis en place pour encadrer l'utilisation qui serait faite des données recueillies grâce à COVI (ou toute autre application).

Ce débat public devrait être organisé en collaboration étroite avec les groupes de la société civile et les organisations communautaires. Il devrait servir, en fin de compte, à élaborer des stratégies de déploiement de l'application. De plus, pour que ce débat soit éclairé et éclairant, il faudra le nourrir avec l'ensemble des documents pertinents. Il faudra notamment divulguer les résultats de l'analyse des impacts de l'application sur la vie privée ou encore rendre accessible la publication du code source.

2ème recommandation

Les développeurs de COVI (ou de toute autre application conçue et déployée pour gérer la pandémie) devraient assurer la mise en place d'un mécanisme servant à l'auditer de manière indépendante.

Un protocole d'évaluation indépendant de l'application servirait à mesurer son utilité réelle aussi bien sur le plan individuel (ex. : prise de décision personnelle des usagers quant à leur exposition au risque et à leurs pratiques de protection) que sur le plan collectif (ex. : objectifs de santé publique de contrôle de la propagation ou d'éradication du virus).

3ème recommandation

En raison de l'incertitude relative à la capacité réelle de COVI ou des applications du genre à protéger la population de la pandémie, il serait important de précéder la diffusion à grande échelle de tout outil de la réalisation d'un projet pilote dont les critères de succès seraient définis et connus d'avance.

Ce projet pilote devrait servir à évaluer la robustesse de COVI ou de toute autre application semblable et à mesurer son efficacité dans une gamme d'environnements réels typiques. Comme cela s'est fait dans plusieurs pays (ex. : la Suisse), ce pilote pourrait se dérouler à l'échelle d'un quartier ou d'une petite municipalité.

4ème recommandation

Si une organisation comme l'OBNL devait se voir confier la mission d'encadrer l'utilisation qui sera faite des données de COVI, un comité indépendant détaché de Mila et des autres promoteurs de COVI devrait être créé pour éviter tout conflit d'intérêts. Ce comité aurait la charge de déterminer par lui-même la bonne structure de gouvernance de ladite OBNL ainsi que d'identifier les personnes les plus aptes à siéger au sein de cette instance décisionnelle et à assurer une évaluation indépendante des impacts à long terme.

Une telle mesure permettrait de garantir le fonctionnement intègre, transparent et imputable de l'OBNL.