Applications de traçage des contacts de la COVID-19

Réflexions du Groupe d'experts sur la protection des données personnelles du Barreau du Québec

Mai 2020

Barreau du Québec

Mission du Barreau du Québec

Afin d'assurer la protection du public, le Barreau du Québec surveille l'exercice de la profession, fait la promotion de la primauté du droit, valorise la profession et soutient ses membres dans l'exercice du droit.

Remerciements

Le Barreau du Québec remercie les membres de son Groupe d'experts sur la protection des données personnelles :

M^e^ Antoine Aylwin
M^e^ Sylvie Champagne
M^e^ Jean-François De Rico
M^e^ Raymond Doray
M^e^ Pierre Trudel

Le secrétariat de ce Comité est assuré par le Secrétariat de l'Ordre et Affaires juridiques du Barreau du Québec :

M^e^ Nicolas Le Grand Alary

Table des matières

INTRODUCTION

La recherche de contacts (en anglais le *contact tracing*) est une des méthodes efficaces afin de limiter la propagation d'infections, dont la COVID-19[1]. Ainsi, la plupart des États au monde ont mis sur pied des façons de rechercher et de contrôler les contacts physiques qu'une personne contaminée a pu avoir avec d'autres.

Ces mesures peuvent prendre la forme d'une enquête épidémiologique et de recherche des contacts qui passent par une entrevue où la personne infectée communique volontairement l'identité des personnes avec qui elle a eu des contacts rapprochés ainsi que les lieux qu'elle a fréquentés.

Dans une perspective où le déconfinement aura lieu dans un proche avenir et où les personnes auront de plus en plus de contacts entre elles, même en respectant les directives de distanciation physique, plusieurs acteurs privés et publics réfléchissent à la mise en œuvre de logiciels et d'applications mobiles destinées à être utilisées aux fins de la recherche de contacts potentiels de personnes avec des cas confirmés de la COVID-19.

Les gouvernements du Québec et du Canada réfléchissent à l'utilisation de ce type de solution afin d'aider les autorités de la santé publique dans leur travail[2]. La Commission d'accès à l'information[3] (ci-après « CAI ») et le Commissariat à la protection de la vie privée du Canada[4] (ci-après « CPVPC ») ont également publié des réflexions quant à certains enjeux identifiés en matière de protection des données personnelles et de la vie privée en ce temps de pandémie de COVID-19.

Au niveau mondial, des applications de ce type sont utilisées depuis mars 2020 en Chine, en Corée du Sud et à Singapour[5]. Aux États-Unis, des entreprises privées, comme Apple et Google se sont unies pour concevoir un protocole permettant le développement de solutions logicielles qui font appel à la technologie Bluetooth[6]. En France, le Conseil national du numérique s'est prononcé en faveur de l'application *StopCovid* en tant que partie d'une stratégie plus globale[7].

Le Groupe d'experts sur la protection des données personnelles du Barreau du Québec a pris connaissance avec intérêt de ces documents et des différentes initiatives et formule certains commentaires afin d'orienter la réflexion quant à ces applications et aux enjeux juridiques de leur utilisation, notamment sur la vie privée et la protection des données personnelles.

---

[1] Voir à ce sujet le site de l'ORGANISATION MONDIALE DE LA SANTÉ, *Flambée de maladie à coronavirus 2019 (COVID-19)*, en ligne : https://www.who.int/fr/emergencies/diseases/novel-coronavirus-2019.

[2] LA PRESSE, « Géolocaliser la pandémie, une fausse bonne idée? », 20 avril 2020, en ligne : https://www.lapresse.ca/covid-19/202004/19/01-5270071-geolocaliser-la-pandemie-une-fausse-bonne-idee.php

[3] COMMISSION D'ACCÈS À L'INFORMATION, *Pandémie, vie privée et protection des renseignements personnels*, avril 2020, en ligne : https://www.cai.gouv.qc.ca/documents/CAI_reflexionPRP-COVID-19_V2_2020-04-16.pdf.

[4] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Cadre pour l'évaluation par le gouvernement du Canada des initiatives en réponse à la COVID-19 ayant une incidence importante sur la vie privée*, avril 2020, en ligne : https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/renseignements-sur-la-sante-renseignements-genetiques-et-autres-renseignements-sur-le-corps/urgences-sanitaires/fw_covid/.

[5] CNBC, « Use of surveillance to fight coronavirus raises concerns about government power after pandemic ends », 26 mars 2020, en ligne : https://www.cnbc.com/2020/03/27/coronavirus-surveillance-used-by-governments-to-fight-pandemic-privacy-concerns.html.

[6] APPLE, *Apple and Google partner on COVID-19 contact tracing technology*, 10 avril 2020, en ligne : https://www.apple.com/ca/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/.

[7] CONSEIL NATIONAL DU NUMÉRIQUE, *StopCovid — Avis du Conseil national du numérique*, avril 2020, en ligne : https://cnnumerique.fr/files/uploads/2020/2020.04.23_COVID19_CNNUM.pdf.

1. APPLICATIONS DE TRAÇAGE ET LEURS USAGES

Le recours aux applications de traçage peut être envisagé afin d'identifier les personnes à risque et faciliter la mise en place de mesures pour ralentir la contagion. Ces applications sont généralement présentées comme un substitut ou comme un complément à des mesures de confinement physiques, celles-ci impliquant une restriction au droit des individus de se déplacer.

Plus on se rapproche de la possibilité de relâcher les mesures de confinement physique, plus il est prévisible que l'on préconise le recours à des dispositifs connectés afin de départager les personnes en fonction des risques qu'elles présentent. Les mécanismes qui cibleraient avec plus de précision les situations périlleuses sans prohiber les déplacements sont évidemment perçus comme des solutions intéressantes dès lors qu'elles permettent la reprise de plusieurs activités.

Selon une équipe de l'Université d'Oxford, dans une étude publiée dans la revue *Science*, l'application mobile de recherche des contacts doit toujours être combinée avec l'isolement des cas, le traçage et la mise en quarantaine des contacts, l'éloignement physique, les tests de diagnostic à plus grande échelle, la décontamination et les mesures d'hygiène[8].

Les chercheurs insistent cependant sur l'importance de normes rigoureuses accompagnant l'utilisation d'une telle technologie fondée sur des téléphones portables pour lutter contre la pandémie de COVID-19. De telles exigences éthiques permettent de renforcer la confiance du public et, par voie de conséquence, l'acceptabilité sociale des mesures et technologies utilisées[9].

1.1 Applications fondées sur la géolocalisation

Le traçage des contacts à l'aide de capacités de localisation pour lutter contre la COVID-19 a déjà été mis en œuvre dans des pays tels que la Corée du Sud et Taïwan. Il a également été déployé en Chine à l'aide d'une application « fichable » (*plugin*) pour les applications omniprésentes *WeChat* et *Alipay*. L'utilisation n'était pas obligatoire, mais elle était requise pour se déplacer entre certaines zones et les espaces publics. Une base de données centrale a collecté des données d'utilisateurs qui ont été analysées à l'aide d'outils d'intelligence artificielle (IA).

1.1.1 Corée du Sud

Depuis 2015, la Corée du Sud peut retracer le parcours d'individus testés positifs à différentes infections à contrôler et ainsi les isoler, tout comme ceux qui font partie de leur chaîne de contacts. On peut imposer aux individus l'installation dans leurs appareils portables d'une application de suivi de l'état de santé, l'accès aux données GPS des appareils de téléphone portables, l'utilisation de caméras de surveillance et une surveillance des informations bancaires.

Une alerte sur les téléphones portables est transmise pour détailler le parcours récent dans les lieux publics des personnes possiblement infectées. Ceux qui ont été en contact avec des individus

[8] Luca FERRETTI, Chris WYMANT, Michelle KENDALL, Lele ZHAO, Anel NURTAY, Lucie ABELER-DÖRNER, Michael PARKER, David BONSALL, Christophe FRASER, « Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing », *Science*, 31 mars 2020, en ligne : https://bit.ly/2xY8DGq.
[9] *Id.*

contaminés ont l'obligation de se faire tester dans les meilleurs délais. Le reste de la population est invité à limiter les sorties[10].

1.1.2 Chine

En Chine, dans une approche beaucoup plus intrusive, la société de paiement mobile *Alipay* a développé, sous la supervision du gouvernement chinois une application par laquelle les usagers sont invités à s'inscrire et fournir les informations demandées. Cela déclenche le processus de génération d'un code QR de couleur qui indique leur état potentiel de contagion.

La détention d'un code vert permet de circuler dans tous les lieux publics comme le métro ou les centres commerciaux, mais aussi les restaurants ou d'accéder à un simple taxi. Un code jaune contraint à une mise en quarantaine préventive de sept jours, alors que le code rouge indique que l'utilisateur doit rester chez lui durant 14 jours, correspondant à la période d'incubation du virus.

Une ligne de code intitulée « reportInfoAndLocationToPolice » témoigne du dessein de l'application qui transmet la localisation précise de la personne et un numéro de code d'identification à un serveur de la police[11].

1.2 Applications ayant recours à la technologie Bluetooth

L'application *StopCovid* développée dans certains pays européens permet un suivi des contacts, rendu possible lorsqu'elle est installée sur les téléphones portables des malades et des personnes qui sont susceptibles d'avoir été infectées.

Ce type d'application est l'équivalent numérique des démarches déjà effectuées manuellement par les équipes médicales lorsque celles-ci cherchent à identifier les rencontres, trajets et activités des personnes contaminées pour remonter à d'autres patients, mais aussi à identifier des chaînes de contamination afin de freiner la pandémie. En s'appuyant sur le parc de téléphones portables, on peut mener de telles opérations à plus grande échelle.

Lorsque deux personnes dont les téléphones portables sont munis de l'application se croisent pendant une certaine durée, et à une distance rapprochée, le téléphone portable de l'un enregistre les références de l'autre dans son historique. Lorsqu'un cas positif est déclaré, ceux qui auront été en contact avec la personne atteinte sont prévenus de manière automatique.

Tel qu'elle est envisagée, cette application n'enregistre que les appareils munis de la même application qui ont été dans son environnement immédiat pendant un temps à définir au-delà duquel il représente un risque d'infection au coronavirus si l'un des deux utilisateurs est lui-même contaminé. Dans ce modèle, il n'y a pas de recours à la géolocalisation[12].

---

[10] LE MONDE, « En Corée du Sud, des tests massifs pour endiguer le coronavirus », 20 mars 2020, en ligne : https://www.lemonde.fr/international/article/2020/03/20/en-coree-du-sud-des-tests-massifs-pour-endiguer-le-coronavirus_6033800_3210.html

[11] NEW YORK TIMES, « In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags », 1er mars 2020, en ligne : https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html.

[12] Julie JACOB, « Avec *StopCovid*, la France envisage aussi le tracking », *Décideurs magazine*, 9 avril 2020, en ligne : https://www.magazine-decideurs.com/news/demain-tous-trackes.

En France, la Commission nationale de l'informatique et des libertés a publié un avis[13] qui indique les conditions et garanties requises pour assurer la conformité du déploiement et de l'utilisation d'une telle application avec les dispositions du *Règlement général sur le protection des données*[14].

1.2.1 Apple et Google

Le projet de protocole conjoint d'Apple et Google s'appuie quant à lui sur la fonctionnalité *Bluetooth Low Energy* (BLE), un mode de communication sans fil conçu pour la communication à courte distance, utilisé ici pour détecter et journaliser des occurrences de proximité avec d'autres appareils munis d'une application utilisant le même protocole.

La documentation publiée à ce jour réfère notamment à l'utilisation d'identifiants multiples[15] afin de réduire le risque d'identification des personnes[16]. Lorsqu'un utilisateur constate qu'il est infecté, il peut téléverser les données générées par l'application vers un serveur contrôlé par l'exploitant qui génère quotidiennement un fichier regroupant sous forme agrégée les données téléversées par les personnes contaminées et qui le rend disponible pour téléchargement par tous les utilisateurs. La validation des occurrences de proximité par un utilisateur est effectuée localement sur l'appareil de chacun des utilisateurs.

1.2.2 Europe

La Commission européenne recommande de développer une approche commune pour l'utilisation des applications et des données mobiles dans la lutte contre la pandémie de la COVID-19, en mettant en place une approche coordonnée paneuropéenne permettant aux citoyens de prendre des mesures efficaces et plus ciblées de distanciation sociale, et servant à l'alerte, à la prévention et au traçage des contacts.

La Commission préconise aussi des outils permettant de modéliser et de prévoir l'évolution du virus au moyen de données de localisation mobile anonymisées et agrégées. Elle a également établi des principes clés pour l'utilisation de ces applications et de ces données en ce qui concerne la sécurité des données et le respect des droits fondamentaux de l'UE, tels que la protection de la vie privée et des données personnelles[17].

---

[13] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Délibération n° 2020-046 du 24 avril 2020 portant avis sur un projet d'application mobile dénommée « StopCovid »*, avril 2020, en ligne : https://bit.ly/3eX5Huh.

[14] *Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)*, en ligne : https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679.

[15] Désigné comme étant des *Rolling Proximity Identifiers* dans les spécifications relatives aux fonctions cryptographiques publiées par Apple et Google.

[16] L'application génère initialement une clé unique (*Tracing Key*) qui est générée et conservée sur l'appareil, et à partir de laquelle l'application génère des clés quotidiennes (*Daily Tracing Keys*), lesquelles sont associées aux occurrences de proximité et utilisées par l'exploitant pour constituer un fichier de données agrégées quotidien constitué des données que les utilisateurs infectés acceptent de téléverser.

[17] COMMISSION EUROPÉENNE, *Orientations sur les applications soutenant la lutte contre la pandémie de COVID-19 en ce qui concerne la protection des données*, avril 2020, en ligne : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52020XC0417(08).

1.2.3 Singapour

Singapour a déployé une application mobile intitulée *TraceTogether* pour permettre le suivi des contacts par la communauté où les appareils participants échangent des informations de proximité chaque fois qu'une application détecte un autre appareil avec l'application *TraceTogether* installée. Il utilise les lectures du Bluetooth *Relative Signal Strength Indicator* (RSSI) entre les appareils dans le temps pour évaluer la proximité et la durée d'une rencontre entre deux utilisateurs. Ces informations de proximité et de durée sont stockées sous forme cryptée sur le téléphone d'une personne pendant 21 jours sur une base continue. Aucune donnée de localisation n'est collectée[18].

1.2.4 Québec et Canada

Des chercheurs travaillent au développement d'applications en lien avec la lutte à l'épidémie, notamment en collaboration avec le Massachusetts Institute of Technology (MIT) pour développer une application qui utilisera les capacités Bluetooth et GPS des téléphones afin de dresser une liste des contacts que les individus ont eus entre eux[19].

Au Québec, des chercheurs montréalais travaillent sur une application de ce type. Il y a également une entreprise qui fait la promotion de l'application *MATAR-19* qui consigne pendant 20 jours les informations de déplacement du téléphone sur lequel elle est installée. D'autres équipes canadiennes développent aussi des applications de traçage de contacts[20].

Toutefois, à ce jour, il ne semble pas exister au Canada une application qui soit fonctionnelle et qui réponde aux critères énoncés précédemment.

2. ENJEUX DE SANTÉ PUBLIQUE ET ENJEUX DE PROTECTION DE LA VIE PRIVÉE

Le recours aux dispositifs de traçage est envisagé comme un substitut au confinement physique. Alors que le confinement physique se caractérise par l'imposition de limites significatives au droit de circuler, le recours aux dispositifs de traçage implique une limitation du droit à la vie privée par le partage de données plus ou moins sensibles.

2.1 Caractère raisonnable des mesures à appliquer

Pour apprécier le caractère raisonnable des limites aux droits découlant de l'utilisation de dispositifs numériques, il faut la considérer en tant qu'alternative aux mesures très lourdes de confinement systématiques qui sont mises en place afin d'assurer la distanciation sociale jugée nécessaire pour lutter contre la contagion.

En d'autres termes, entre deux maux, comme obliger presque tout le monde au confinement physique ou avoir recours à des dispositifs électroniques pour identifier les personnes infectées, il

[18] LE MONDE, « Coronavirus : à Singapour, *TraceTogether* permet de remonter les chaînes de contamination sans géolocalisation », 8 avril 2020, en ligne : https://www.lemonde.fr/planete/article/2020/04/08/coronavirus-a-singapour-tracetogether-permet-de-remonter-les-chaines-de-contamination-sans-geolocalisation_6035984_3244.html.
[19] LA PRESSE, « Traquer la pandémie grâce aux cellulaires », 31 mars 2020, en ligne : https://www.lapresse.ca/covid-19/202003/30/01-5267212-traquer-la-pandemie-grace-aux-cellulaires.php.
[20] *Id.*

faut choisir le moindre. Elle doit donc être vue comme une mesure complémentaire de la stratégie globale pour contrer la propagation du virus.

L'utilisation d'applications de traçage des contacts de la COVID-19 présente des avantages. Elle permet une plus grande mobilité des personnes et elle procure des possibilités de limiter les exigences de confinement physique à un nombre plus restreint d'individus. Cependant, elle peut se révéler extrêmement intrusive dans l'intimité de chacun et paver la voie à la discrimination de groupes ou d'individus. C'est pourquoi, elle ne doit être déployée que moyennant un ensemble de conditions strictes.

L'emploi de telles applications doit absolument être limité à des situations déterminées et son usage justifié par la nécessité de protéger la santé publique. Il doit nécessairement être temporaire. Les dispositifs utilisés doivent être conçus de manière à minimiser la collecte et la circulation d'informations sur les individus.

- ✓ **Constat nº 1 :** Le recours à une application de traçage des contacts doit être vu comme une mesure complémentaire de la stratégie globale pour contre la propagation de la COVID-19.
- ✓ **Constat nº 2 :** Toute application de traçage des contacts de la COVID-19 devra faire l'objet d'un encadrement serré, afin de s'assurer qu'elle ne porte qu'une atteinte minimale aux droits fondamentaux.
- ✓ **Constat nº 3 :** Une telle application devra faire l'objet d'une surveillance pendant sa conception, ainsi que pendant et après son utilisation, afin de s'assurer de la proportionnalité des mesures.

2.2 Impossibilité d'utiliser le consentement comme assise

D'aucuns insistent pour exiger que l'utilisation d'applications de traçage soit conditionnelle au consentement des individus à utiliser celles-ci ou autres dispositifs de collecte et de traitement des informations. Or, si l'on peut convenir que le consentement individuel est légitime dans des situations qui concernent uniquement l'individu, on a du mal à imaginer que les mesures de confinement soient tributaires du consentement des personnes.

Force est de reconnaître que l'utilisation de telles applications ne peut en toutes circonstances s'appuyer sur l'obtention d'un consentement manifeste, spécifique et éclairé des individus alors que le confinement physique qui prévaut actuellement dans plusieurs pays n'est pas sujet au consentement de chacun.

En effet, l'efficacité des mesures de traçage, en tant qu'alternative au confinement obligatoire, dépend souvent de sa généralisation à l'ensemble de la population. Dans ce contexte, l'obtention du consentement manifeste, spécifique et éclairé qui est au cœur de nos lois de protection des renseignements personnels est illusoire, pour ne pas dire contraire à l'objectif poursuivi.

C'est d'ailleurs de manière indirecte que les mesures de traçage sont généralement imposées par les juridictions qui y ont recours : transmission des données aux autorités de santé publique,

message d'alerte de celles-ci aux personnes susceptibles d'être infectées, partage obligatoire des données pour avoir accès à un lieu ou à un moyen de transport, exigences de l'employeur pour éviter de mettre à risque ses clients ou ses autres employés, etc. Les limitations au droit à la vie privée deviennent alors le prix à payer en échange d'une certaine liberté de mouvement, du droit de travailler, de fréquenter des lieux publics, etc.

Des limites aux mesures destinées à protéger la santé publique doivent dès lors être fixées de manière à ne limiter les droits des individus que dans la seule mesure où cela est nécessaire pour assurer la sécurité de l'ensemble des membres de la collectivité à protéger.

En revanche, le caractère obligatoire ou indirectement obligatoire d'applications de traçage des contacts de la COVID-19 doit être conditionnel à des règles strictes relatives à l'utilisation des données collectées et surtout aux processus décisionnels qui se fonderaient sur de telles données. C'est de cette façon qu'il devient possible de prévenir la stigmatisation des personnes à risque. Par exemple, une application qui permettrait d'identifier en direct le niveau de risque d'une personne que l'on croise publiquement risque de renforcer la stigmatisation.

- ✓ **Constat nº 4 :** Lorsque le consentement ne peut être utilisé comme assise de l'utilisation d'une application de traçage des contacts de la COVID-19, elle pourrait toutefois être exigée en contrepartie d'une plus grande liberté de mouvement, incluant le droit de retour au travail.

- ✓ **Constat nº 5 :** Le cadre juridique actuel prévu par les lois concernant la protection des données n'est pas adapté à la réalité particulière de la pandémie de la COVID-19.

3. RECOMMANDATIONS DE MESURES DEVANT ÊTRE MISES EN PLACE

Sans prendre position sur l'opportunité de mettre en place de telles applications, force est de constater que l'utilisation de toute application ou de tout logiciel de traçage des contacts de la COVID-19 devra ainsi faire l'objet de différentes mesures de contrôle, et ce, à chaque étape du processus.

Ainsi, des mesures devront être mises en place en amont, lors du développement de la solution technologique retenue. Des contrôles devront également être effectués en temps réel, lors de l'utilisation de l'application, ainsi qu'après, afin notamment de s'assurer que les informations recueillies ont été utilisées aux seules fins pour lesquelles elles l'ont été.

3.1 Élaboration d'un nouveau cadre normatif par le biais d'un comité d'experts

Comme nous l'avons énoncé précédemment, le cadre juridique actuel concernant la protection des données personnelles et de la vie privée n'est pas du tout adapté à la réalité de la pandémie de la COVID-19. En effet, la crise sanitaire actuelle nécessite une certaine agilité que les lois actuelles ne peuvent offrir.

3.1.1 Nouveau cadre législatif et réglementaire

Un nouveau cadre normatif juridique devra donc être mis en place afin d'encadrer les solutions de traçage retenues. Ce cadre pourrait être adopté par le gouvernement par décret. Il devra comporter différentes mesures afin de s'assurer de l'utilisation proportionnée des technologies, en contrôlant les règles de gouvernance encadrant les différents projets, le développement et l'exploitation des applications.

La CAI et la Commission des droits de la personne et des droits de la jeunesse (ci-après la « CDPDJ ») constituent les organismes de surveillance tout indiqués, à condition bien sûr qu'elles puissent effectuer cette surveillance en fonction de normes mieux adaptées que celles des lois actuelles en matière de protection des données.

En effet, plusieurs droits fondamentaux garantis par la *Charte des droits et libertés de la personne*[21] peuvent être affectés par le déploiement d'une application de traçage des contacts de la COVID-19. L'on peut penser à la liberté de mouvement, au droit à la vie et, de manière plus générale, au droit de ne pas être discriminé pour un motif interdit.

Ainsi, cette surveillance devrait s'effectuer conjointement par ces deux organismes, car la CAI possède l'expertise requise en matière de protection des renseignements personnels et la CDPDJ en matière de protection des droits fondamentaux.

3.1.2 Constitution d'un comité d'experts indépendants

Pour établir ce cadre normatif, le gouvernement devrait mettre sur pied un comité d'experts indépendants. Le mandat de ce comité n'y serait toutefois pas limité. Il devrait également :

- Préciser les objectifs poursuivis;
- Continuer de s'assurer que leurs mesures sont nécessaires et proportionnelles, « c'est-à-dire qu'elles sont essentiellement fondées sur des données probantes, qu'elles sont nécessaires pour la fin particulière déterminée et qu'elles n'ont pas une portée excessive »[22];
- Déterminer la temporalité réduite des mesures envisagées;
- Recommander les outils qui répondent mieux aux objectifs poursuivis en respectant les contraintes de la nécessité et la proportionnalité.

Tout en maintenant l'agilité requise, nous considérons qu'il est important que des représentants du public puissent siéger sur ce comité afin d'assurer un certain contrôle par la société civile. Bien que le gouvernement ne serait pas tenu à suivre les recommandations du comité, celles-ci seraient publiques.

[21] RLRQ, c. C-12.
[22] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, préc., note 4.

Ce comité serait nommé par le gouvernement, après consultation des chefs des partis d'opposition, comme c'est le cas en ce moment pour différents postes qui sont nommés par l'Assemblée nationale. De tels mécanismes ont été notamment mis en place dans la *Loi modifiant les règles encadrant la nomination et la destitution du commissaire à la lutte contre la corruption, du directeur général de la Sûreté du Québec et du directeur des poursuites criminelles et pénales*[23].

- ✓ **Recommandation nº 1 :** Un nouveau cadre normatif doit être mis en place, notamment parce que les lois actuelles ne sont pas adaptées à la présente pandémie de la COVID-19. La CAI et la CDPDJ auraient un rôle à jouer dans la surveillance du déploiement.
- ✓ **Recommandation nº 2 :** Un comité d'experts indépendants devrait être constitué par le gouvernement, afin de mettre en place ce nouveau cadre normatif et d'assurer un suivi du développement de toute application de traçage des contacts de la COVID-19.

3.2 Développement supervisé de l'application

En amont de l'utilisation de toute technologie de traçage, nous croyons qu'il est nécessaire de mettre en place des mesures encadrant le développement même de la technologie, comme des comités d'éthique, des évaluations des facteurs relatifs à la vie privée (EFVP) ou d'autres processus.

3.2.1 *Privacy by design*

La mise en place de mécanismes d'audit en amont a fait ses preuves, notamment en matière environnementale[24]. De plus, la mise en œuvre de mesures visant à protéger la vie privée dès la conception (*privacy by design*) constitue une excellente pratique qui doit être obligatoire dans la conception de toute application de traçage des contacts de la COVID-19.

L'utilisation de ressources de conformité interne telles que des audits et des vérifications permettent de responsabiliser les développeurs, les rendre imputables et les sensibiliser aux dérives potentielles des applications. Il s'agit d'un excellent mécanisme d'autoréglementation.

En outre, l'utilisation de l'EFVP, d'un processus de certification ou d'un comité d'éthique[25] constitue selon nous des façons permettant de remplir ces obligations. Ainsi, nous ne recommandons pas qu'un processus ou un autre soit obligatoire. Chacun possède ses avantages et ses inconvénients, qui dépendront des finalités du projet, des renseignements qui seront colligés ou inférés et les scénarios d'utilisation qui seront retenus.

[23] L.Q. 2019, c. 6 (anciennement le projet de loi nº 1).
[24] Voir les mécanismes prévus à la *Loi sur la qualité de l'environnement*, RLRQ, c. Q-2.
[25] Le Comité d'éthique de santé publique de l'Institut national de santé publique du Québec pourrait être mis à contribution en vertu de l'article 35 de la *Loi sur la santé publique*, RLRQ, c. S-2.2. Pour plus d'informations, voir en ligne : https://www.inspq.qc.ca/cesp.

D'ailleurs, nous croyons que ces applications de traçage devraient préférablement être développées par les autorités publiques ou à leur demande, afin d'éviter la multiplicité des plateformes ce qui pourrait augmenter la confusion de la population et les risques de dérapage.

3.2.2 Traitement localisé des données

Si possible, les données recueillies devraient être analysées et être conservées sur l'appareil de la personne qui l'utilise. Ainsi, des solutions préconisant un suivi macro des contacts potentiels et des infections à la COVID-19 est à privilégier. Si des données doivent être transmises sur des serveurs externes, notamment afin d'aviser certaines personnes d'un risque de contamination, cela devra être fait d'une façon à s'assurer que les identifiants personnalisés ne soient pas transmis sur ces serveurs.

De plus, il ne doit pas être possible de procéder à une réidentification de la personne contaminée, soit par l'application elle-même ou un acteur de mauvaise foi, mais également de la part des autres utilisateurs de l'application qui pourraient en déduire son identité sur la base des informations fournies par l'application.

3.2.3 Transparence des acteurs

En outre, nous sommes d'avis que la transparence doit être un élément essentiel de toute application de traçage de contacts de la COVID-19. Cela peut inclure le développement de logiciels *open source* de la part des autorités publiques ou bien assurer une transparence algorithmique aux systèmes qui feraient appel à l'IA. Ce n'est qu'en fournissant le plus d'informations sur la façon dont ces applications fonctionnent que le public sera rassuré que leur utilisation ne pose pas de risque particulier en ce qui a trait au respect de leur vie privée.

Le recours aux données générées par un appareil mobile et leur croisement avec d'autres sources de données peuvent être particulièrement intrusifs en raison de la quantité d'informations qu'elles sont susceptibles de révéler sur la vie privée d'une personne, notamment en regard de ses déplacements et de ses rencontres[26].

La publication des spécifications techniques par les promoteurs est conséquemment importante afin de permettre à des experts et à des professionnels de la protection de la vie privée de faire l'examen de la robustesse des processus sous-jacents, des mesures de sécurité destinées à préserver la confidentialité des renseignements personnels, dont les fonctions cryptographiques utilisées.

[26] Soulignons qu'un nombre significatif d'utilisateurs partagent en continu, consciemment ou inconsciemment, de telles données de localisation avec des exploitants de services publicitaires.

- ✓ **Recommandation nº 3 :** Afin d'être le plus soucieux du respect du droit à la vie privée et à la confidentialité des données personnelles, toute application de traçage des contacts de la COVID-19 devrait être développée en s'appuyant sur certains principes :
  - ✓ Emploi de la technique du *privacy by design*;
  - ✓ Ne permettre qu'un traitement localisé des données;
  - ✓ S'assurer de la transparence des acteurs.

3.3 Utilisation proportionnée des technologies de traçage

Lors du déploiement des applications de traçage des contacts de la COVID-19, nous sommes d'avis qu'il est primordial de mettre en place des processus qui permettront d'évaluer régulièrement l'application développée afin de s'assurer de l'opportunité de maintenir en place certaines mesures. Une évaluation en continu doit être mise sur pied.

3.3.1 Pouvoirs de surveillance de la CAI, du CPVPC et de la CDPDJ

Par le passé, nous avons souligné à plusieurs reprises que nous sommes favorables à l'octroi de nouveaux pouvoirs de surveillance à la CAI et au CPVPC. Le haut potentiel de dérapage des applications de la COVID-19 vient nous rappeler comment il est grandement venu le temps de conférer à la CAI au CPVPC et à la CDPDJ le pouvoir d'émettre des ordonnances et d'imposer des sanctions pécuniaires contre ceux qui refusent de se conformer à leurs lois respectives.

Nous ne pouvons toutefois cacher nos préoccupations réelles quant au niveau de financement requis pour s'assurer que cela puisse se réaliser sur le terrain. Il faut que les gouvernements, tant fédéral que provincial, octroient un budget suffisant pour permettre à la CAI, au CPVPC et à la CDPDJ de remplir leur mandat respectif.

Ainsi, malgré la mise en place d'un comité d'experts indépendants, la CAI, le CPVPC et la CDPDJ auront toujours un rôle à jouer, notamment en s'assurant du traitement des plaintes pendant le déploiement d'une application de traçage des contacts de la COVID-19.

3.3.2 Limitation de l'utilisation des données

Bien entendu, il est primordial que les données ne soient utilisées qu'aux fins pour lesquelles elles ont été recueillies, c'est-à-dire suivre l'évolution de la pandémie de la COVID-19. Il ne faut donc pas que ces renseignements soient utilisés à des fins commerciales comme du marketing ciblé envers les personnes infectées ou leurs proches.

Comme nous l'avons énoncé précédemment, ces applications devraient être développées par les autorités publiques ou pour elles par des entreprises privées. Ainsi, dans ces circonstances, et si le développeur de l'application n'a pas autrement accès aux données, il ne devrait raisonnablement pas avoir de risque d'une utilisation commerciale des données.

Cela ne veut toutefois pas dire que ces données ne pourraient pas être utilisées d'une façon autrement non conforme. Bien que nous reconnaissions que les autorités publiques pourraient avoir certaines utilisations légitimes de ces données, comme proposer la participation à des études cliniques aux personnes infectées, nous croyons que ces utilisations devraient être limitées.

Ainsi, pratiquement toute utilisation à d'autres fins devrait être interdite. Les données de géolocalisation et les inférences qui peuvent en être déduites ne devraient pas servir à des enquêtes pénales et criminelles ou à des vérifications du statut d'immigration, à moins qu'un mandat ait été obtenu en ce sens.

- ✓ **Recommandation nº 4 :** Lors du déploiement des applications de traçage des contacts de la COVID-19, celles-ci devraient faire l'objet d'une utilisation proportionnée, validée par le biais de différents mécanismes, comme :
  - ✓ Octroyer des pouvoirs de surveillance et d'enquêtes aux organismes de contrôle que sont la CAI, le CPVPC et la CDPDJ;
  - ✓ Limiter l'utilisation qui peut être faite des données aux seules fins appropriées en matière de traçage.

3.4 Sanctions et évaluations *a posteriori*

En parallèle, il est également primordial de mettre en place des mesures de contrôle *a posteriori*, c'est-à-dire après que l'application et que les données recueillies aient été utilisées et qu'il ne soit plus nécessaire de les garder.

3.4.1 Destruction des données et cycle de fin de vie de l'application

Ainsi, la destruction des données recueillies devrait être automatique, après la fin de la période d'utilisation de l'application (à la fin de la pandémie ou lorsqu'il ne sera plus nécessaire de l'utiliser, car de nouveaux outils auront été développés). Si cette période est trop étendue dans le temps, il est également possible de prévoir une date de destruction de certaines données plus anciennes conservées par l'application, s'il est clair qu'elles ne seront plus nécessaires.

Bien entendu, certaines métadonnées ou autres données dépersonnalisées devraient pouvoir être conservées, notamment à des fins de recherche et de développement. Il est important de reconnaître que ces applications peuvent grandement être utiles afin d'aider au développement de logiciels ultérieurs, si le besoin se réalise.

En outre, nous proposons que les organismes de contrôle, comme la CAI ou le CPVPC, effectuent des audits et des vérifications afin de s'assurer que les données ont également été détruites. Ces organismes devraient également mettre sur pied des comités ou effectuer des enquêtes afin de tirer des leçons sur (1) l'utilisation qui avait été prévue pour l'application, (2) l'utilisation qui a effectivement été faite et (3) les pistes d'amélioration qui devraient être mises en œuvre si des logiciels similaires doivent être utilisés dans le futur.

Un rapport de l'organisme de contrôle devrait être déposé à l'Assemblée nationale. Une consultation publique devrait obligatoirement suivre pour permettre aux citoyens et organismes de défense des droits fondamentaux de débattre publiquement de ces enjeux.

3.4.2 Sanctions à l'encontre des contrevenants

Comme nous l'avons énoncé précédemment, nous croyons qu'il est nécessaire de mettre en place des sanctions sévères envers ceux qui ne respecteraient pas les règles qui encadreront le développement de telles applications.

Si ces applications sont développées par ou pour les autorités publiques, le risque est plus faible, mais pas inexistant : il est important que les fournisseurs des gouvernements ne gardent pas d'accès caché au travers du logiciel (*back door*). De plus, des mesures suffisantes devront être mises en place afin d'éviter toute fuite de données ou toute utilisation non autorisée (par le biais d'un *hack* par exemple). Des sanctions sévères devront être mises en place pour dissuader de tels comportements.

- ✓ **Recommandation nº 5 :** Après que l'application et que les données recueillies aient été utilisées et qu'il ne soit plus nécessaire de les garder, des mesures de contrôle *a posteriori* devront être mises en place. La CAI et le CPVPC devront :
  - ✓ S'assurer de la destruction des données et du cycle de fin de vie de l'application de traçage des contacts de la COVID-19 par le biais d'audits et de vérifications;
  - ✓ Sanctionner sévèrement les contrevenants par le biais de leurs nouveaux pouvoirs.

CONCLUSION, CONSTATS ET RECOMMANDATIONS

La confidentialité des données est bien entendu encadrée par nos lois sur la protection des renseignements personnels, conformément aux principes de nécessité et de proportionnalité qui sous-tendent les lois sur la protection des renseignements personnels, lesquels ont été récemment réitérés par les autorités canadienne[27] et québécoise[28].

Il y a lieu de s'assurer que les mesures susceptibles d'être attentatoires soient nécessaires, proportionnelles et que leur portée ne soit pas excessive en regard de l'objectif qui consiste à réduire la propagation en notifiant les personnes ayant été en contact avec une personne infectée pendant la période de contagion. Cette analyse nous a permis de constater que :

- ✓ **Constat nº 1 :** Le recours à une application de traçage des contacts doit être vu comme une mesure complémentaire de la stratégie globale pour contre la propagation de la COVID-19;

- ✓ **Constat nº 2 :** Toute application de traçage des contacts de la COVID-19 devra faire l'objet d'un encadrement serré, afin de s'assurer qu'elle ne porte qu'une atteinte minimale aux droits fondamentaux;

- ✓ **Constat nº 3 :** Une telle application devra faire l'objet d'une surveillance pendant sa conception, ainsi que pendant et après son utilisation, afin de s'assurer de la proportionnalité des mesures;

- ✓ **Constat nº 4 :** Lorsque le consentement ne peut être utilisé comme assise de l'utilisation d'une application de traçage des contacts de la COVID-19, elle pourrait toutefois être exigée en contrepartie d'une plus grande liberté de mouvement, incluant le droit de retour au travail;

- ✓ **Constat nº 5 :** Le cadre juridique actuel prévu par les lois concernant la protection des données n'est pas adapté à la réalité particulière de la pandémie de la COVID-19.

De ces constats, certaines conclusions s'imposent. Ainsi, nous recommandons :

- ✓ **Recommandation nº 1 :** Un nouveau cadre normatif doit être mis en place, notamment parce que les lois actuelles ne sont pas adaptées à la présente pandémie de la COVID-19. La CAI et la CDPDJ auraient un rôle à jouer dans la surveillance du déploiement;

- ✓ **Recommandation nº 2 :** Un comité d'experts indépendants devrait être constitué par le gouvernement, afin de mettre en place ce nouveau cadre normatif et d'assurer un suivi du développement de toute application de traçage des contacts de la COVID-19;

[27] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, préc., note 4.
[28] COMMISSION D'ACCÈS À L'INFORMATION, préc., note 3.

- ✓ **Recommandation nº 3 :** Afin d'être le plus soucieux du respect du droit à la vie privée et à la confidentialité des données personnelles, toute application de traçage des contacts de la COVID-19 devrait être développée en s'appuyant sur certains principes :
    - ✓ Emploi de la technique du *privacy by design*;
    - ✓ Ne permettre qu'un traitement localisé des données;
    - ✓ S'assurer de la transparence des acteurs.
- ✓ **Recommandation nº 4 :** Lors du déploiement des applications de traçage des contacts de la COVID-19, celles-ci devraient faire l'objet d'une utilisation proportionnée, validée par le biais de différents mécanismes, comme :
    - ✓ Octroyer des pouvoirs de surveillance et d'enquêtes aux organismes de contrôle que sont la CAI, le CPVPC et la CDPDJ;
    - ✓ Limiter l'utilisation qui peut être faite des données aux seules fins appropriées en matière de traçage.
- ✓ **Recommandation nº 5 :** Après que l'application et que les données recueillies aient été utilisées et qu'il ne soit plus nécessaire de les garder, des mesures de contrôle *a posteriori* devront être mises en place. La CAI et le CPVPC devront :
    - ✓ S'assurer de la destruction des données et du cycle de fin de vie de l'application de traçage des contacts de la COVID-19 par le biais d'audits et de vérifications;
    - ✓ Sanctionner sévèrement les contrevenants par le biais de leurs nouveaux pouvoirs.