Commission
d'accès à l'information
du Québec

Applications de traçage ou de notification des contacts et vie privée

Mémoire de la Commission d'accès à l'information présenté à la Commission des institutions de l'Assemblée nationale dans le cadre des consultations particulières et auditions publiques au sujet d'outils technologiques de notification des contacts

Québec, 13 août 2020

TABLE DES MATIÈRES

APPLICATIONS DE TRAÇAGE OU DE NOTIFICATION DES CONTACTS ET VIE PRIVÉE
Mémoire de la Commission d'accès à l'information

SOMMAIRE EXÉCUTIF

Dans le présent mémoire, la Commission d'accès à l'information du Québec s'attarde, de manière générale, aux enjeux et aux conditions de conformité légale du déploiement d'outils technologiques de notification des contacts, plus spécifiquement aux chapitres de la protection des renseignements personnels et du respect de la vie privée.

Les principes minimaux à respecter dans l'éventualité de la mise en place d'une telle mesure exceptionnelle sont les suivants :

1. *Établir la nécessité et la proportionnalité du recours à l'outil technologique de notification des contacts*
2. *Minimiser l'atteinte aux droits dès la conception*
3. *Garantir le caractère volontaire et assurer un consentement valide*
4. *Adopter une démarche transparente en amont et en aval*
5. *Limiter la collecte de renseignements personnels*
6. *Limiter l'utilisation et la communication des renseignements personnels*
7. *Mettre en place une infrastructure technologique et un écosystème sécuritaires*
8. *Déterminer les conditions de mise hors service de cette mesure temporaire et détruire les renseignements recueillis*
9. *Permettre l'exercice de ses droits par la personne concernée*
10. *Assumer la responsabilité par une évaluation continue, une reddition de compte et un contrôle externe indépendant*
11. *Adopter un cadre juridique spécifique au déploiement et à l'utilisation de l'application au Québec*

La Commission recommande des mesures concrètes afin de respecter chacun de ces principes dans l'éventualité où le gouvernement du Québec déciderait de recourir à ce genre d'outil technologique. Puisque la législation actuelle n'offre pas un degré de protection adapté au niveau de risque que comporte le recours à ce type d'application, la Commission identifie ensuite les principaux éléments qu'un encadrement spécifique devrait inclure.

Malgré ces recommandations générales, la Commission souligne qu'un examen et une analyse plus poussée d'une éventuelle solution qui serait retenue par le gouvernement seront requis afin d'émettre un avis et de formuler des recommandations spécifiques à cette solution et, possiblement, à l'écosystème qui sera mis en place pour assurer son fonctionnement.

A. CONTEXTE

De nombreuses initiatives technologiques voient le jour afin d'atténuer les effets causés par la crise sanitaire qui sévit partout dans le monde. Des entreprises, des chercheuses et des chercheurs mettent à profit leurs connaissances et leur ingéniosité en proposant des solutions technologiques innovantes ayant pour objectif de favoriser un déconfinement sécuritaire et un retour à une certaine normalité pour les citoyens.

Parmi les technologies envisagées, les applications de traçage ou de notification des contacts (ou notification d'exposition) sur téléphones intelligents retiennent l'attention de plusieurs gouvernements. Depuis mars 2020, ces outils technologiques alimentent de nombreuses discussions et analyses de par le monde. Des débats entourant leur développement et leur déploiement soulèvent divers enjeux, dont leur efficacité et leur caractère non inclusif, surtout par rapport aux groupes les plus vulnérables de la société. Leur impact sur certains droits et libertés fondamentaux, dont le respect du droit à la vie privée, fait évidemment aussi partie de ces discussions.

Interpellée dès le début de la crise sanitaire par les enjeux qu'elle percevait autour de ces initiatives, la Commission d'accès à l'information du Québec (la Commission) a publié le 14 avril un document de réflexion[1] dans lequel elle rappelle les éléments importants à considérer dans l'évaluation de la légalité du déploiement d'une solution technologique dans le contexte de la présente crise sanitaire. Parallèlement à la publication de son document de réflexion, la Commission a joint sa voix à celles de ses homologues fédéral, provinciaux et territoriaux le 7 mai 2020 pour émettre une déclaration commune portant spécifiquement sur les applications de traçage des contacts et de notification d'exposition[2]. Dans cette déclaration, les commissaires canadiens énoncent les principes minimaux à respecter pour le déploiement éventuel d'une telle application par leurs gouvernements respectifs.

Des applications de traçage ou de notification des contacts ont rapidement émergé un peu partout dans le monde[3]. Au Canada, l'Alberta a adopté une telle

---

[1] COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *Pandémie, vie privée et protection des renseignements personnels*, Commission d'accès à l'information, 14 avril 2020 (mis à jour le 4 mai 2020), en ligne : <https://www.cai.gouv.qc.ca/documents/CAI_document-reflexion_PRP_COVID-19_FR.pdf> (consulté le 4 mai 2020) (ci-après le « document de réflexion »)

[2] « Appuyer la santé publique et bâtir la confiance des Canadiens : principes de protection de la vie privée et des renseignements personnels pour les applications de traçage des contacts et autres applications similaires » (7 mai 2020), en ligne : <https://www.cai.gouv.qc.ca/documents/CAI_D%C3%A9claration_commune_FRA_vf.pdf> (consulté le 9 juillet 2020) (ci-après la « déclaration commune »)

[3] Le *MIT Technology Review Covid Tracing Tracker* recensait 47 applications différentes en date du 1er août 2020, alors que l'Observatoire international sur les impacts sociétaux de l'IA et du numérique (OBVIA) dit en avoir dénombré de plus de 70. RYAN-MOSLEY, T., « Contact Tracing Tracker », *MIT Technology Review*, en ligne :

application dès le début mai[4]. Le 18 juin 2020, le gouvernement du Canada a exprimé son intention de rendre disponible une application de notification d'exposition pour l'ensemble des citoyens canadiens : COVID Shield. Le même jour, l'Ontario a annoncé qu'elle prendrait part au déploiement initial de cette application. L'application a été rendue disponible pour téléchargement le 31 juillet 2020 sous le nom Alerte COVID[5].

Le 8 juillet 2020, le Secrétariat du Conseil du trésor du Québec a lancé une consultation publique visant à sonder l'opinion de la population et à connaître ses

---

<https://public.flourish.studio/visualisation/2241702/> (consulté le 3 août 2020); OBSERVATOIRE INTERNATIONAL SUR LES IMPACTS SOCIÉTAUX DE L'IA ET DU NUMÉRIQUE, « Avis sur l'application de notification de contacts proposée par Mila », *Observatoire international sur les impacts sociétaux de l'IA et du numérique* (4 juin 2020), en ligne : <https://observatoire-ia.ulaval.ca/avis-obvia-covi/> (consulté le 4 juin 2020).

[4] L'application ABTraceTogether a été lancée le 1er mai 2020. Elle supporte des activités de traçage manuel effectuées par Alberta Health Services en automatisant le suivi des contacts significatifs entre ses utilisateurs. Basée sur la technologie Bluetooth, l'application collecte les « poignées de main » numérique entre téléphones via l'échange d'identifiants dépersonnalisés. En cas de diagnostic positif, l'utilisateur peut fournir la liste de ces « poignées de main » aux autorités de santé publique. À l'aide de cette liste, ces dernières peuvent contacter les personnes qui auront été croisées par la personne déclarée positive, car elles ont accès à un registre permettant de faire le lien entre les identifiants dépersonnalisés et les données identificatoires des utilisateurs. Le 9 juillet, l'homologue albertain de la Commission publiait un avis favorable portant sur l'évaluation des facteurs relatifs à la vie privée réalisée par les promoteurs de l'application et formulait plusieurs recommandations. GOUVERNEMENT DE L'ALBERTA, « ABTraceTogether », *Alberta.ca*, en ligne : <https://www.alberta.ca/ab-trace-together.aspx> (consulté le 20 juillet 2020); BUREAU DU COMMISSAIRE À L'INFORMATION ET À LA VIE PRIVÉE DE L'ALBERTA, *ABTraceTogether Privacy Impact Assessment Review Report*, Bureau du commissaire à l'information et à la vie privée de l'Aberta, 2020, en ligne : <https://www.oipc.ab.ca/media/1089098/Report_ABTraceTogether_PIA_Review_Jun2020.pdf> (consulté le 13 juillet 2020).

[5] L'application Alerte COVID, développée principalement par le Service numérique canadien en collaboration avec Santé Canada et plusieurs autres intervenants, a été lancée à l'échelle fédérale. Elle a pour but la notification d'exposition. Grâce à elle, les téléphones des utilisateurs s'échangent des identifiants dépersonnalisés aléatoires par l'entremise de la technologie Bluetooth. Les identifiants des personnes croisées (selon certains paramètres de durée et de distance) par un utilisateur sont stockés dans son propre téléphone, tout comme la liste de ses propres identifiants. En cas de diagnostic positif, l'utilisateur peut obtenir une clé à usage unique de la part de l'autorité sanitaire de sa province ou de son territoire. Grâce à cette clé, il peut confirmer son diagnostic dans l'application. Il peut ensuite consentir à transmettre les identifiants dépersonnalisés aléatoires qui sont stockés dans son téléphone vers un serveur de clés. Sur une base quotidienne, ce serveur transmet ensuite les données aux téléphones des autres utilisateurs. Leur application détermine alors si ceux-ci ont été en contact avec une personne infectée en vérifiant la présence de l'un ou l'autre des identifiants de cette dernière dans la liste stockée sur leur téléphone. S'il y a eu contact, les utilisateurs reçoivent une notification d'exposition qui leur donne des informations (façon de joindre les autorités de santé publique, endroits où passer un test de dépistage, etc.).

Le jour du lancement, soit le 31 juillet, le Commissaire à la protection de la vie privée du Canada et le Commissaire à l'information et à la protection de la vie privée de l'Ontario ont indiqué par communiqué qu'ils avaient conclu leur examen de l'application et soutenaient son utilisation. Notons que bien qu'Alerte COVID puisse être téléchargée dans l'ensemble des provinces et territoires, la confirmation d'un diagnostic positif n'est actuellement possible qu'en Ontario en date du 10 août. Voir notamment SANTÉ CANADA, « Alerte COVID : Évaluation de la protection des renseignements personnels de l'application de notification d'exposition », *Canada.ca*, en ligne : <https://www.canada.ca/fr/sante-publique/services/maladies/maladie-coronavirus-covid-19/alerte-covid/politique-confidentialite/evaluation.html> (consulté le 10 août 2020); COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, « Communiqué - Les commissaires fédéral et ontarien à la vie privée soutiennent l'utilisation de l'appli Alerte COVID sous réserve d'une surveillance continue de ses mesures de protection et de son efficacité », *Commissariat à la protection de la vie privée du Canada* (31 juillet 2020), en ligne : <https://www.priv.gc.ca/fr/nouvelles-du-commissariat/nouvelles-et-annonces/2020/nr-c_200731/> (consulté le 4 août 2020).

préoccupations quant à l'utilisation volontaire d'une application mobile de notification des contacts à la COVID-19. Le gouvernement du Québec a aussi annoncé la présente consultation particulière et audition publique auprès de la Commission des institutions sur les outils technologiques de notification des contacts, leur pertinence, leur utilité et, le cas échéant, les conditions de leur acceptabilité sociale.

Selon le document de consultation, l'objectif visé par la Commission des institutions est triple :

- Recueillir l'avis des représentants de la société civile sur les applications de notification d'exposition au coronavirus;
- Soupeser leurs risques et leurs avantages;
- Déterminer si l'encadrement en place est adéquat.[6]

La Commission s'attarde principalement au troisième point de la consultation dans ce mémoire.

B. PORTÉE DU PRÉSENT MÉMOIRE

Les enjeux relatifs au recours à ces applications dépassent la protection des renseignements personnels. Une réflexion plus globale s'impose et doit considérer les autres enjeux éthiques et juridiques potentiels associés au recours à ces outils[7]. D'autres droits fondamentaux sont susceptibles d'être en cause. Il faut évidemment aussi considérer les enjeux de santé publique et socio-économiques causés par la crise sanitaire et évaluer l'effet bénéfique potentiel de ces outils en cas de deuxième vague.

---

[6] SECRÉTARIAT DU CONSEIL DU TRÉSOR, *Document de consultation — Consultations particulières et auditions publiques au sujet d'outils technologiques de notification des contacts ainsi que sur la pertinence de ce type d'outils, leur utilité et le cas échéant, les conditions de leur acceptabilité sociale dans le cadre de la lutte contre la COVID-19*, Québec, Secrétariat du Conseil du Trésor, p. 2, en ligne : <http://www.assnat.qc.ca/Media/Process.aspx?MediaId=ANQ.Vigie.Bll.DocumentGenerique_159911&process=Default&token=ZyMoxNwUn8ikQ+TRKYwPCjWrKwg+vIv9rjij7p3xLGTZDmLVSmJLoqe/vG7/YWzz>.

[7] À ce titre, voir : COMMISSION DE L'ÉTHIQUE EN SCIENCE ET TECHNOLOGIE, *Rapport d'étape : conditions d'acceptabilité éthique*, Commission de l'éthique en science et technologie, 2020, en ligne : https://www.ethique.gouv.qc.ca/media/1329/cest-conditions-acceptabilite-ethique_v7.pdf (consulté le 13 juillet 2020); ORGANISATION MONDIALE DE LA SANTÉ, *Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing*, Organisation mondiale de la santé, 2020, en ligne : <https://www.who.int/publications-detail-redirect/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1> (consulté le 10 juillet 2020); CIFAR, *Société, technologie et éthique en cas de pandémie*, Canadian Institute For Advanced Research (CIFAR), 2020, en ligne : <https://www.cifar.ca/docs/default-source/all-reports/ai-step-report-fr-4-f.pdf> (consulté le 10 juillet 2020); Michel DÉSY, Julie ST-PIERRE, BRUNO LECLERC, Marie-Ève COUTURE-MÉNARD, Dominic CLICHE et Jocelyn MACLURE, *Cadre de réflexion sur les enjeux éthiques liés à la pandémie de COVID-19*, Québec, Institut nationale de santé publique du Québec, 2020, en ligne : <https://www.inspq.qc.ca/publications/2958> (consulté le 6 juillet 2020).

Toutefois, la Commission limite ses commentaires aux enjeux qui sont en lien avec ses attributions et son expertise, soit la transparence et la protection des renseignements personnels.

Elle souligne également le caractère général du présent avis. Un examen et une analyse plus poussée d'une éventuelle solution retenue par le gouvernement seront requis pour émettre un avis et formuler des recommandations spécifiques à cette solution et, possiblement, à l'écosystème qui sera mis en place pour assurer son fonctionnement (ex. : échanges requis pour l'interopérabilité avec les applications utilisées dans d'autres provinces ou territoires canadiens).

Les objectifs de santé publique visés par le recours à une application et divers paramètres relatifs à sa conception et à son fonctionnement influencent les enjeux de vie privée et de protection des renseignements personnels liés à son déploiement et à son utilisation.

C. DES OBJECTIFS ET DES PARAMÈTRES À PRÉCISER

Il existe un nombre important de paramètres qui peuvent avoir une incidence sur l'évaluation qui sera faite d'une technologie donnée et sa conformité avec la législation actuelle et les principes mis de l'avant par la déclaration commune des commissaires à la protection de la vie privée du Canada. Le document de consultation élaboré par le Secrétariat du Conseil du trésor en présente quelques-uns.

Ainsi, la nature et la quantité des renseignements recueillis, le lieu de leur stockage (incluant une centralisation ou non), leur utilisation et leur communication, le cas échéant, les mesures de sécurité mises en place, le ou les objectifs spécifiques de santé publique poursuivis et la nature de la ou des technologie(s) utilisée(s) sont autant d'éléments susceptibles d'influencer l'évaluation de l'application et les recommandations spécifiques que pourrait formuler la Commission.

Pour les fins de la présente consultation, il est pertinent de souligner trois éléments des divers outils développés dans différents pays et qui ont une incidence certaine sur les enjeux de protection des renseignements personnels.

TRAÇAGE DES CONTACTS ET NOTIFICATION D'EXPOSITION

Les **applications de « traçage des contacts »** sont déployées pour assister les activités de traçage manuel effectuées par les autorités de santé publique et requièrent

généralement la collecte de renseignements personnels identificatoires afin de pouvoir entrer en contact avec les personnes concernées. C'est l'approche retenue par l'Alberta.

Pour leur part, les **applications de « notification d'exposition » ou de « notification des contacts »** visent à informer leurs utilisateurs qu'ils ont peut-être été en contact avec une personne testée positive à la COVID-19 et à les inviter à prendre des mesures appropriées (ex. : contacter le personnel de la santé publique, s'isoler, subir un test de dépistage). Il existe différents modèles de ces applications dont certains misent sur un fonctionnement à partir de données ne permettant pas d'identifier une personne ni de recueillir de manière centralisée des renseignements personnels. Alerte COVID, l'application lancée par le gouvernement fédéral, vise la notification d'exposition.

Bien que ces deux catégories d'applications s'appuient sur des mécanismes similaires pour la détection des contacts physiques significatifs (géolocalisation, Bluetooth ou les deux), la différence entre ces deux approches est importante, notamment en termes d'enjeux de protection des renseignements personnels.

STOCKAGE DES DONNÉES CENTRALISÉ OU NON

Un autre élément de variation concerne l'approche retenue pour le stockage des renseignements nécessaires au fonctionnement de l'application : centralisée ou décentralisée. Le document de consultation en fait également état.

Les données peuvent être stockées dans une unique base de données sous le contrôle d'une organisation (approche centralisée). Elles peuvent aussi être stockées directement sur les téléphones des utilisateurs de l'application pour être échangées seulement au besoin, dans l'éventualité d'un diagnostic positif (approche décentralisée). L'approche décentralisée est reconnue comme offrant généralement un meilleur contrôle sur les renseignements personnels[8].

Des modèles hybrides peuvent également être envisagés. Par exemple, les données concernant les contacts sont conservées sur les téléphones des utilisateurs dans l'application déployée en Alberta. Elles sont transférées aux autorités de santé publique en cas de diagnostic positif, avec le consentement de l'utilisateur, afin que celles-ci puissent effectuer le contact avec les personnes qui ont été croisées.

---

[8] OBSERVATOIRE INTERNATIONAL SUR LES IMPACTS SOCIÉTAUX DE L'IA ET DU NUMÉRIQUE, « Petit guide sur les enjeux et opportunités des applications de notifications d'exposition à la COVID-19 », *Observatoire international sur les impacts sociétaux de l'IA et du numérique*, en ligne : <https://observatoire-ia.ulaval.ca/qa_covid/> (consulté le 9 juillet 2020).

FONCTIONNALITÉS SECONDAIRES

Des fonctionnalités secondaires ont parfois été évoquées, en plus de la fonctionnalité de base de traçage ou de notification des contacts. Ainsi, des applications pourraient inclure des fonctionnalités comme : le suivi des symptômes, des questionnaires d'auto-évaluation du niveau de risque, la collecte de renseignements pour des fins d'études épidémiologiques, la vérification du respect des consignes sanitaires (quarantaine, distanciation sociale, etc.) ou même l'utilisation de renseignements de santé pour l'évaluation d'un niveau de risque, notamment à l'aide d'un algorithme.

Chaque fonctionnalité ajoutée influence l'analyse de la solution et la détermination des enjeux particuliers qu'elle soulève, notamment en matière de protection des renseignements personnels.

Dans ces circonstances, la Commission insiste sur le fait que des recommandations spécifiques ne pourront être formulées qu'après un examen et une analyse approfondis d'une éventuelle solution retenue par le gouvernement.

D. PRINCIPES DE PROTECTION DES RENSEIGNEMENTS PERSONNELS À RESPECTER

En complément des éléments à considérer contenus dans le document de réflexion de la Commission, la déclaration commune qu'elle a coélaborée avec ses homologues canadiens pose les principes minimaux à respecter en matière de vie privée et de transparence dans l'éventualité où le gouvernement déciderait de déployer un outil de traçage des contacts ou de notification d'exposition à la COVID-19.

S'inspirant de ces documents, de ces principes et du cadre légal applicable au Québec, la Commission formule les recommandations générales suivantes dans l'éventualité où le gouvernement choisirait de déployer un tel outil, qu'il s'agisse de celui rendu disponible par le gouvernement du Canada (Alerte COVID) ou d'une autre application.

Enfin, puisque la législation actuelle n'offre pas un degré de protection adapté au niveau de risque que comporte le recours à ce type d'application, la Commission recommande la mise en place d'un encadrement juridique spécifique. Étant donné l'importance de cette recommandation, une section lui est dédiée après la présentation du principe qui la sous-tend. Dans celle-ci, la Commission identifie les principaux éléments qu'un tel encadrement devrait inclure.

1. ÉTABLIR LA NÉCESSITÉ ET LA PROPORTIONNALITÉ DU RECOURS À L'OUTIL TECHNOLOGIQUE DE NOTIFICATION DES CONTACTS

Le recours à une application de traçage ou de notification des contacts n'est pas sans conséquences potentielles sur les droits fondamentaux, dont le droit au respect de la vie privée et la protection des renseignements personnels.

Toutefois, le droit à la vie privée, comme tout droit fondamental, n'est pas absolu. Il s'exerce notamment dans le respect des valeurs démocratiques, de l'ordre public et du bien-être général des citoyens du Québec.

Il est donc prévu qu'on puisse y porter atteinte, en certaines circonstances et à certaines conditions, afin d'assurer un équilibre et une pondération entre les besoins de la société et les droits des individus.

Entre autres, cette atteinte sera justifiée s'il est démontré que la mesure poursuit un objectif légitime, important et réel et que l'atteinte au droit fondamental qu'elle constitue est proportionnelle à cet objectif. La *Charte québécoise des droits de la personne*[9] prévoit que la loi peut alors en fixer la portée et en aménager l'exercice. La Cour suprême du Canada[10] a précisé le test à appliquer dans ces circonstances.

Ce test s'effectue en deux temps. Il vise à évaluer si la mesure envisagée est :

- nécessaire pour répondre à un objectif légitime et suffisamment important et réel et
- proportionnelle à l'atteinte au droit fondamental qu'elle constitue.

NÉCESSITÉ

Il s'agit d'abord de s'assurer que les objectifs poursuivis sont légitimes, importants et réels, de manière à justifier la nécessité de la mesure pour la société et son atteinte aux droits fondamentaux.

---

[9] RLRQ, c. C-12, en ligne : <http://legisquebec.gouv.qc.ca/fr/showDoc/cs/C-12?& digest=> (consulté le 15 juillet 2020).

[10] Cour suprême du Canada, 28 février 1986, *R. c. Oakes*, [1986] 1 RCS 103, en ligne : <https://scc-csc.lexum.com/scc-csc/scc-csc/fr/item/117/index.do> (consulté le 15 juillet 2020).

Dans le document de consultation, il est fait mention que l'objectif principal de l'application serait de faciliter la recherche des contacts[11]. Le document énumère d'autres objectifs de santé publique potentiels du recours à une application, selon le modèle choisi. Si le gouvernement décide d'aller de l'avant avec une application de traçage ou de notification des contacts, ces objectifs devront être précisés.

Les objectifs de santé publique doivent être fondés sur la science, selon des données probantes, et libellés avec un certain niveau de précision.

Ils doivent aussi s'inscrire dans la stratégie de lutte contre la transmission de la COVID-19 des autorités de santé publique. Il importe donc de s'assurer que les autres éléments de cette stratégie en lien avec l'utilisation de l'application sont disponibles.

À titre d'exemple, dans le cas des applications de notification d'exposition, plusieurs pays ont souligné l'importance de pouvoir compter sur des tests de dépistage suffisamment nombreux et accessibles, afin de vérifier si le contact « à risque » se traduit ou non par une transmission du virus.

Dans le cas des applications de traçage des contacts, il importe que les ressources pour effectuer le suivi approprié de ces contacts soient disponibles et en nombre suffisant pour agir en temps opportun.

PROPORTIONNALITÉ

Une solution sera proportionnelle si elle respecte les conditions suivantes :

- Il existe un lien rationnel entre l'objectif poursuivi et la solution envisagée;
- L'intrusion à la vie privée des individus est minimale;
- La solution s'impose en l'absence d'autres solutions moins intrusives pour la vie privée;
- Les avantages surpassent les conséquences préjudiciables pour les personnes concernées[12].

Pour établir la proportionnalité de manière adéquate et complète, une application spécifique doit avoir été identifiée et les objectifs poursuivis doivent avoir été déterminés.

Par contre, les conditions énumérées ci-dessus peuvent aussi permettre d'orienter le choix d'une solution ou d'une technologie. Par exemple, le document de

---

[11] SECRÉTARIAT DU CONSEIL DU TRÉSOR, préc., note 6, p. 4.

[12] COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, préc., note 1, p. 4 à 6; note 2.

consultation identifie déjà, à juste titre, que l'intrusion dans la vie privée des individus est plus importante avec l'utilisation de certaines technologies (ex. : géolocalisation, biométrie) ou du mécanisme centralisé de stockage de l'information.

En outre, pour démontrer le lien rationnel entre l'objectif poursuivi et la solution envisagée, celle-ci doit être efficace ou du moins, susceptible de l'être. Or, l'efficacité des applications de traçage ou de notification des contacts demeure inconnue actuellement. Les limites de ces applications pour effectuer le suivi des contacts ont été soulevées à plusieurs reprises[13].

Selon l'Organisation mondiale de la santé (OMS), il n'existe actuellement aucune méthodologie permettant d'évaluer directement l'impact d'une telle solution sur la gestion de la crise[14]. Toujours selon l'OMS, un outil de notification des contacts ne peut être pleinement effectif que s'il s'intègre à l'intérieur d'un système préexistant de santé publique et dans une réponse nationale à la pandémie qui prévoit l'affectation de personnel de santé publique dédié aux tests à la COVID-19 et au suivi manuel des contacts[15].

Du point de vue technologique, des lacunes ont été évoquées dans la précision des mesures de distance réalisées grâce à la technologie Bluetooth ou à l'utilisation de données de géolocalisation. De plus, ces technologies ne permettent pas de rendre compte des éléments liés au contexte dans lesquels ont lieu les différents contacts et qui pourraient influencer les risques de transmission de la maladie (ex. : port du couvre-visage ou de visières, présence de cloisons, etc.)[16].

Au-delà des considérations purement techniques, l'efficacité véritable d'une application de traçage ou de notification des contacts demeure théorique à ce stade-ci.

---

[13] Notamment, voir ORGANISATION MONDIALE DE LA SANTÉ, préc., note 7; ADA LOVELACE INSTITUTE, « COVID-19 Rapid Evidence Review: Exit through the App Store? », *Ada Lovelace Institute* (18 avril 2020), p. 26 à 34, en ligne : <https://www.adalovelaceinstitute.org/our-work/covid-19/covid-19-exit-through-the-app-store/> (consulté le 20 avril 2020); Robert A. KLEINMAN et Colin MERKEL, « Digital contact tracing for COVID-19 », (2020) 192-24, *Canadian Medical Association Journal* E653- E656, DOI : 10.1503/cmaj.200922.

[14] « "Currently, there are no established methods for assessing the effectiveness of digital proximity tracking. More research to evaluate their effectiveness is needed and, ultimately, robust methodologies need to be developed for this purpose. », ORGANISATION MONDIALE DE LA SANTÉ, préc., note 7, p. 2.

[15] « Digital proximity tracking applications can only be effective in terms of providing data to help with the COVID-19 response when they are fully integrated into an existing public health system and national pandemic response » *Id.*

[16] OBSERVATOIRE INTERNATIONAL SUR LES IMPACTS SOCIÉTAUX DE L'IA ET DU NUMÉRIQUE, préc., note 3, p. 14; ORGANISATION MONDIALE DE LA SANTÉ, préc., note 7, p. 2.

Les applications déployées actuellement dans le monde semblent avoir des effets plutôt mitigés[17].

L'efficacité est aussi corrélée au taux d'adoption de la solution par la population[18]. Or, les taux d'adoption sont généralement faibles actuellement[19]. Ils dépendent beaucoup de la confiance que les citoyens accordent à cet outil, des craintes qu'il suscite, notamment en matière de vie privée et de sécurité, mais aussi du nombre d'utilisateurs de téléphones intelligents suffisamment récents pour soutenir la technologie mise en place[20]. Ce dernier élément soulève l'inefficacité de ces applications pour une partie importante de la population, mais aussi pour ceux qui l'utilisent et entrent en contact avec une personne qui ne dispose pas de la technologie requise.

---

[17] Voir par exemple, pour l'Islande : « COVID-19 : l'application de traçage n'aurait pas beaucoup aidé en Islande », *Radio-Canada* (12 mai 2020), en ligne : < https://ici.radio-canada.ca/nouvelle/1702196/application-coronavirus-efficace-efficacite-islande-depistage-modele-technique-islandais> (consulté le 10 juillet 2020); pour la Suisse : SEYDTAGHIA, A.*,* « Pourquoi SwissCovid recule : des pistes pour comprendre », *Le Temps* (12 juillet 2020), en ligne : <https://www.letemps.ch/economie/swisscovid-recule-pistes-comprendre> (consulté le 4 août 2020); pour la France : UNTERSINGER, M.*,* « Après trois semaines, l'application StopCovid n'a averti que 14 personnes », *Le Monde* (23 juin 2020), en ligne : <https://www.lemonde.fr/pixels/article/2020/06/23/application-stopcovid-14-personnes-averties-en-trois-semaines_6043915_4408996.html> (consulté le 4 août 2020); pour l'Australie : GLADSTONE, N.*,* « COVIDSafe app yet to trace useful number of unique cases despite second wave », *The Sydney Morning Herald* (26 juillet 2020), en ligne : <https://www.smh.com.au/national/covidsafe-app-yet-to-trace-useful-number-of-unique-cases-despite-second-wave-20200725-p55fd7.html> (consulté le 4 août 2020).

[18] Les médias ont beaucoup fait état des résultats d'une étude de l'Université d'Oxford. Dans cette étude, un taux d'adoption de 60 % était mentionné pour que l'utilisation d'une application soit efficace. Or, bien que l'étude fasse mention de ce taux, les chercheurs estimaient qu'il était requis si l'application était le seul moyen déployé pour réduire et, éventuellement, éliminer le virus. Il ne tenait pas compte des autres moyens déployés (ex. distanciation sociale, mesures prophylactiques, etc.). L'application pourrait avoir, selon certains, une certaine efficacité peu importe le taux d'adoption. FERRETTI, L., WYMANT, C., KENDALL, M., ZHAO, L., NURTAY, A., ABELER-DÖRNER, L., PARKER, M., BONSALL, D. et FRASER, C., « Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing », *Science* (2020) 368-6491, DOI : 10.1126/science.abb6936; O'NEILL, P.H. « No, coronavirus apps don't need 60% adoption to be effective », *MIT Technology Review* (5 juin 2020), en ligne : <https://www.technologyreview.com/2020/06/05/1002775/covid-apps-effective-at-less-than-60-percent-download/> (consulté le 5 juin 2020).

[19] CHAN, S. « COVID-19 Contact Tracing Apps Reach 9% Adoption In Most Populous Countries », *Sensor Tower Blog* (14 juillet 2020), p. 9, en ligne : <https://sensortower.com/blog/contact-tracing-app-adoption> (consulté le 17 juillet 2020).

[20] Quelques jours après sa mise en service, l'application du gouvernement fédéral, Alerte COVID, est critiquée sur cet aspect, puisqu'elle ne fonctionnerait pas avec des téléphones moins récents. Par ailleurs, le CEFRIO mentionnait que 77 % des Québécoises et Québécois détenaient un téléphone intelligent en 2020. WELLS, N., « Les problèmes d'accessibilité de l'application Alerte COVID critiqués », *La Presse* (3 août 2020), en ligne : <https://www.lapresse.ca/covid-19/2020-08-03/les-problemes-d-accessibilite-de-l-application-alerte-covid-critiques.php> (consulté le 4 août 2020); CEFRIO, *NETendances 2019 : Services gouvernementaux en ligne*, CEFRIO, 29 avril 2020, p. 5, en ligne : https://cefrio.qc.ca/fr/enquetes-et-donnees/netendances2019-services-gouvernementaux-en-ligne/ (consulté le 13 juillet 2020).

Recommandation 1 : Pour évaluer la nécessité et la proportionnalité du recours à un outil technologique de traçage ou de notification des contacts, la Commission recommande, préalablement à son déploiement, de :

- **Déterminer les finalités spécifiques de santé publique poursuivies. Celles-ci doivent être fondées sur la science selon des données probantes et libellées avec un certain niveau de précision;**
- **S'assurer que l'outil s'inscrit à l'intérieur de la stratégie de lutte contre la transmission de la COVID-19 des autorités de santé publique et que les autres éléments de cette stratégie en lien avec l'utilisation de l'outil sont disponibles (ex. : ressources pour le dépistage, pour un traçage plus poussé des contacts, pour les informations aux personnes recevant une notification de contact à risque, etc.);**
- **Déterminer les critères permettant d'évaluer l'efficacité de l'outil et démontrer qu'il est susceptible d'être efficace pour atteindre les objectifs spécifiques de santé publique identifiés;**
- **Mettre sur pied un mécanisme d'évaluation en continu de l'efficacité de l'outil.**

2. *MINIMISER L'ATTEINTE AUX DROITS DÈS LA CONCEPTION*

La minimisation de l'atteinte aux droits des citoyens doit être prioritaire dès le départ et être réévaluée tout au long de la durée de vie de l'application.

EFFECTUER ET RENDRE PUBLIQUE UNE ÉVALUATION DES FACTEURS RELATIFS À LA VIE PRIVÉE

Un projet d'application devrait être précédé d'une évaluation des facteurs relatifs à la vie privée (EFVP)[21], exigence légale dans un grand nombre de pays et de provinces canadiennes – et, par ailleurs, prévue dans le projet de loi nº 64, qui vise la refonte des lois québécoises sur la protection des renseignements personnels. Cet exercice permet d'évaluer les enjeux de protection des renseignements personnels propres à la solution technologique envisagée. Son analyse permet aux autorités de surveillance et de contrôle, comme la Commission, d'examiner la solution envisagée et de formuler des recommandations.

---

[21] COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *Guide d'accompagnement : Réaliser une évaluation des facteurs relatifs à la vie privé*, Commission d'accès à l'information du Québec, mai 2020, en ligne : https://www.cai.gouv.qc.ca/documents/Guide_EFVP_FR.pdf (consulté le 27 mai 2020); COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *Évaluation des facteurs relatifs à la vie privée : savoir détecter et atténuer les risques d'atteinte aux renseignements personnels*, Québec, Commission d'accès à l'information du Québec, 2018, en ligne : https://www.cai.gouv.qc.ca/documents/CAI_FI_efvp.pdf (consulté le 27 mai 2020).

Pour assurer la transparence de la démarche, la publication de l'EFVP a été exigée dans plusieurs pays ayant choisi de déployer une application de traçage des contacts ou de notification d'exposition. L'analyse éventuelle de la Commission et ses recommandations concernant l'EFVP devraient aussi être publics.

APPLIQUER LES PRINCIPES DE PROTECTION DE LA VIE PRIVÉE DÈS LA CONCEPTION

L'application des principes de protection de la vie privée et de protection des renseignements personnels dès la conception et par défaut[22] dans toutes les étapes de planification, de développement et de déploiement maximise les chances de respecter la vie privée des utilisateurs. Les choix technologiques doivent favoriser la vie privée[23].

PORTER UNE ATTENTION PARTICULIÈRE À LA TECHNOLOGIE ET AUX RENSEIGNEMENTS UTILISÉS

Le choix d'une technologie émergente (comme le recours à un système d'intelligence artificielle ou à la biométrie) et l'utilisation de renseignements sensibles, assujettis à des obligations particulières (comme des renseignements médicaux, de géolocalisation ou biométriques) doivent faire l'objet d'une attention particulière compte tenu des enjeux spécifiques qu'ils soulèvent.

Recommandation 2 : Afin de minimiser l'atteinte aux droits dès la conception, la Commission recommande de :

- **Réaliser une évaluation des facteurs relatifs à la vie privée concernant la solution retenue et la soumettre pour analyse et commentaires à la Commission, avant le déploiement de l'application;**

---

[22] Ces principes sont désignés en anglais par les noms *privacy by design* et *privacy by default*. Le premier met de l'avant 7 principes qui permettent de prendre en compte la protection des renseignements personnels dès la phase de conception d'un projet impliquant de tels renseignements. Le second implique d'accorder la meilleure protection possible aux renseignements personnels, et ce, par défaut : par exemple, les paramètres liés à la vie privée dans un logiciel devraient être fixés au niveau le plus protecteur, dès le départ. Ces deux principes sont notamment intégrés au Règlement général sur la protection des données (RGPD) européen, une législation souvent citée comme référence internationale en matière de protection des renseignements personnels. Voir COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *Rapport quinquennal 2011 : Technologies et vie privée à l'heure des choix de société*, Commission d'accès à l'information (2011), p. 28, en ligne : <https://www.cai.gouv.qc.ca/documents/CAI_RQ_2011.pdf> (consulté le 3 juillet 2020); COMMISSION EUROPÉENNE, *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) (Texte présentant de l'intérêt pour l'EEE)*, OJ 2016 L 119/1 (avril 2016), article 25 et considérant 78, en ligne : <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016R0679> (consulté le 3 juillet 2020).

[23] Par exemple, l'approche décentralisée pour le stockage des données est un choix technologique qui pourrait favoriser la vie privée par défaut.

- **Diffuser publiquement cette évaluation et l'avis de la Commission (voir la recommandation 4 au sujet de la transparence);**
- **Mettre en œuvre les principes de protection de la vie privée dès la conception;**
- **Porter une attention particulière à la technologie et aux renseignements utilisés.**

3. *GARANTIR LE CARACTÈRE VOLONTAIRE ET ASSURER UN CONSENTEMENT VALIDE*

Le caractère volontaire de l'utilisation d'une technologie de traçage ou de notification des contacts est une condition déterminante pour l'analyse du caractère proportionnel de l'atteinte aux droits fondamentaux qu'elle est susceptible d'entraîner.

En matière de respect de la vie privée et de protection des renseignements personnels, il permet le respect de l'essence de ces droits, soit le contrôle des citoyens sur leurs propres renseignements.

Enfin, il est de nature à favoriser la confiance envers une telle application.

L'importance du caractère volontaire a d'ailleurs été maintes fois soulignée par différentes instances s'étant attardées à la légalité et aux enjeux éthiques de ces applications[24].

Le caractère volontaire doit être garanti par des moyens concrets, notamment en s'assurant que l'utilisateur puisse fournir un consentement valide[25]. Il implique aussi d'interdire que l'accès à un lieu (y compris de travail), à un bien, à un service ou à un emploi soit conditionné par quiconque (employeur, commerçant, propriétaire, etc.) à

---

[24] Voir note 2; ORGANISATION MONDIALE DE LA SANTÉ, préc., note 7, p. 3; COMMISSION DE L'ÉTHIQUE EN SCIENCE ET TECHNOLOGIE, préc., note 7, p. 3-4; ADA LOVELACE INSTITUTE, préc., note 13, p. 33; COMMISSION EUROPÉENNE, *Orientations sur les applications soutenant la lutte contre la pandémie de COVID-19 en ce qui concerne la protection des données*, Commission européenne, 16 avril 2020, p. 4, en ligne : https://ec.europa.eu/info/sites/info/files/5_fr_act_part1_v3.pdf (consulté le 13 juillet 2020); COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES, *Lignes directrices 4/2020 relatives à l'utilisation de données de localisation et d'outils de recherche de contacts dans le cadre de la pandémie de COVID-19*, Comité Européen de la Protection des Données, 2020, en ligne : <https://edpb.europa.eu/our-work-tools/our-documents/linee-guida/guidelines-042020-use-location-data-and-contact-tracing_en> (consulté le 20 juillet 2020).

[25] Voir note 2; COMMISSION DE L'ÉTHIQUE EN SCIENCE ET TECHNOLOGIE, préc., note 7; 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 »*, CNIL, 26 avril 2020, p. 5, en ligne : <https://www.cnil.fr/sites/default/files/atoms/files/deliberation_du_24_avril_2020_portant_avis_sur_un_projet_dapplication_mobile_stopcovid.pdf> (consulté le 6 juillet 2020).

l'utilisation de l'application ou à la consultation de son contenu par une personne autre que l'utilisateur.

CONSENTEMENT LIBRE, ÉCLAIRÉ, SPÉCIFIQUE, LIMITÉ DANS SA DURÉE ET EXPLICITE

Une attention particulière devrait donc être portée à la question du consentement. La Commission rappelle que pour que ce consentement soit valide, il doit être libre[26], éclairé[27], spécifique[28] et limité dans le temps[29]. Compte tenu des enjeux que soulèvent ces applications, il devrait être explicite.

Un consentement distinct pour chaque élément ou étape significative de l'utilisation de l'application devrait être demandé. Par exemple, un consentement initial doit être obtenu avant la première utilisation, puis un consentement pour chaque finalité de santé publique pour laquelle les renseignements personnels peuvent être recueillis, utilisés ou communiqués, le cas échéant. Autre exemple : dans plusieurs applications, un nouveau consentement est requis avant la communication des « contacts » à la suite d'un diagnostic positif à la COVID-19. C'est notamment le cas pour l'application déployée par le gouvernement fédéral, Alerte COVID.

Avant l'obtention du consentement initial à l'utilisation de l'application, il importe de bien expliquer ses objectifs, son fonctionnement et ses limites (par exemple, que l'enregistrement des « contacts à risque » par l'appareil ne tient pas compte de certains éléments comme le port du couvre-visage ou la présence de cloisons et peut donc générer de « faux positifs »).

Cette notification de départ devrait également indiquer les risques liés à son utilisation, les droits de l'utilisateur et la portée de son consentement.

Considérant que tout risque de réidentification ne peut être écarté[30], il est préférable d'éviter de donner des garanties d'anonymat aux utilisateurs lorsque

---

26 Un consentement est libre s'il est exprimé sans conditions, contraintes, menaces ou promesses.

27 Un consentement est éclairé s'il est donné en pleine conscience de sa portée, en toute connaissance de cause, d'où l'importance de la transparence.

28 Un consentement est spécifique s'il autorise l'utilisation ou la communication d'un ou des renseignement(s) personnel(s) identifié(s), à des personnes ou organisations identifiées, à des fins déterminées et à un moment précisé.

29 Un consentement est valide pour la durée requise à la réalisation des objectifs pour lesquels le consentement est demandé.

30 À titre d'exemple, dans une communauté où vivent peu de personnes, la réception d'une notification d'exposition pourrait permettre aux utilisateurs de l'application d'identifier, par déduction, la personne ayant confirmé son infection à la COVID-19.

l'application utilise ou génère des renseignements dépersonnalisés ou pseudonymisés. En effet, pour qualifier des renseignements d'anonymes, il doit être démontré que l'on ne peut réidentifier directement ou indirectement la personne à laquelle ils étaient liés à l'origine, et ce, de manière irréversible.

Le consentement doit aussi pouvoir être retiré en tout temps. Les personnes ne désirant plus utiliser l'application doivent pouvoir la désinstaller facilement et tous les renseignements, personnels ou non, à leur sujet doivent être détruits. Une confirmation de cette destruction devrait être transmise aux utilisateurs.

De manière plus générale, le déploiement doit se faire à l'intérieur d'un contexte exempt de pression sociale ou extérieure qui viendrait miner le caractère volontaire de l'utilisation de l'application.

INTERDIRE D'EXIGER L'INSTALLATION DE L'APPLICATION OU LA CONSULTATION DE SON CONTENU

Une affirmation ou un engagement des développeurs ou des autorités gouvernementales ne suffisent pas, à eux seuls, à garantir le caractère libre et volontaire du recours à l'application. En effet, employeurs, propriétaires et commerçants pourraient décider d'exiger son utilisation pour accéder à un lieu, incluant un lieu de travail, un commerce, ou pour obtenir un bien, un service ou un emploi. Ils pourraient aussi exiger de voir son contenu.

Ces pratiques doivent être interdites spécifiquement afin de garantir le caractère volontaire de l'utilisation de l'application[31].

Recommandation 3 : Afin de garantir le caractère volontaire de l'utilisation de l'application et d'assurer un consentement valide, la Commission recommande de :

- **Fournir une information claire, simple et complète aux utilisateurs afin de permettre un consentement éclairé. Cette information devrait inclure minimalement : les objectifs de santé publique poursuivis, la description du fonctionnement de l'application, les limites de l'application, la liste des**

[31] CIFAR, préc., note 7, p. 14; ORGANISATION MONDIALE DE LA SANTÉ, préc., note 7, p. 3; COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, « Examen des répercussions sur la vie privée de l'application Alerte COVID », *Commissariat à la protection de la vie privée du Canada* (31 juillet 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/rev_covid-app/> (consulté le 4 août 2020)

renseignements collectés et les raisons pour lesquelles ils le sont, le détail concernant le stockage des données, l'ensemble des utilisations et des communications prévues, les modalités de destruction des renseignements, les risques liés à l'utilisation de l'application, les droits des utilisateurs quant à leurs renseignements personnels et leurs recours;

- **Éviter de donner des garanties d'anonymat aux utilisateurs si les renseignements sont dépersonnalisés ou pseudonymisés;**
- **Obtenir un consentement distinct, spécifique et explicite :**
  - **Demander un premier consentement à l'installation de l'application, préalablement à sa mise en fonction;**
  - **Demander un consentement distinct pour chaque finalité de santé publique pour laquelle les renseignements personnels sont recueillis, utilisés ou communiqués, de même que pour tout autre événement significatif lié à l'utilisation de l'application;**
- **Permettre en tout temps à un utilisateur de retirer son consentement et de cesser d'utiliser l'application ou de la désinstaller;**
- **Détruire sans délai tout renseignement concernant cet utilisateur;**
- **Mettre en place toutes les conditions permettant de conserver le caractère volontaire de l'utilisation de l'application, notamment en interdisant à quiconque d'exiger l'installation de l'application ou la consultation de son contenu.**

4. ADOPTER UNE DÉMARCHE TRANSPARENTE EN AMONT ET EN AVAL

La transparence est intimement liée au caractère éclairé du consentement et à la confiance envers l'application : les citoyens doivent être informés des motifs justifiant une éventuelle décision de recourir à une telle mesure exceptionnelle et des modalités de son déploiement.

Une condition importante de transparence, mise de l'avant dans plusieurs travaux examinant les applications de traçage ou de notification des contacts[32], est la publication du code source de l'application et des autres composantes qui y sont liées et qui peuvent avoir un impact sur les risques liés à son utilisation (ex. API)[33]. Celle-ci

---

[32] Voir par exemple CIFAR, préc., note 7, p. 4; ADA LOVELACE INSTITUTE, préc., note 13, p. 29; COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, préc., note 25, p. 11.

[33] *Application programming interface*, ou interface de programmation. Selon l'Office québécois de la langue française, il s'agit d'un « [e]nsemble de routines standards, accessibles et documentées, qui sont destinées à faciliter au programmeur le développement d'applications ». OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, « interface de programmation », *Grand dictionnaire terminologique* (2005), en ligne : <http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8394269> (consulté le 10 juillet 2020).

permet un audit externe et indépendant par la société civile, des experts et des scientifiques, qui peuvent vérifier que l'application fonctionne bel et bien comme annoncé et que le code ne renferme pas de failles potentielles.

Faire montre de transparence, c'est également tenir la population informée de l'efficacité de l'application à atteindre ses objectifs, des décisions qui sont prises à partir des informations recueillies par cette application, le cas échéant, et des incidents de sécurité qui découleraient de son utilisation.

La Commission tient d'ailleurs à saluer la double démarche consultative tenue au Québec. En plus de la démarche de consultation de la Commission des institutions, la consultation générale en ligne du gouvernement permet d'inclure la société civile dans la décision de recourir ou non à ces outils. Selon l'avis de la Commission, ces actions favorisent la transparence et la confiance des citoyens.

Recommandation 4 : Afin d'adopter une démarche transparente en aval et en amont, la Commission recommande de :

- **Diffuser les motifs justifiant une éventuelle décision de recourir à une telle mesure exceptionnelle et les modalités de son déploiement;**
- **Diffuser le code source de l'application et de toute autre composante susceptible d'avoir un impact sur les risques liés à son utilisation (ex. : API) afin de faciliter un audit externe indépendant;**
- **Informer les citoyens et la Commission de tout incident ou de toute faille de sécurité ou risque identifié et des mesures prises pour y remédier;**
- **Diffuser l'évaluation des facteurs relatifs à la vie privée au sujet de l'application[34];**
- **Rendre public tout rapport concernant l'évaluation de l'efficacité de l'application pour atteindre le ou les objectif(s) de santé publique identifié(s).**

5. LIMITER LA COLLECTE DE RENSEIGNEMENTS PERSONNELS

De manière à limiter l'intrusion dans la vie privée des citoyens et en respect du principe de nécessité et de minimisation de la collecte des renseignements personnels, la solution retenue devrait limiter la quantité de renseignements personnels recueillis. Elle devrait éviter de recueillir des renseignements sensibles.

[34] La Commission rendra public son avis au sujet de cette évaluation.

Recommandation 5 : Afin de limiter la collecte de renseignements personnels, la Commission recommande de :

- **Privilégier l'utilisation de renseignements anonymisés, dépersonnalisés ou pseudonymisés.**
- **Privilégier une application fonctionnant en mode décentralisé et recueillant le moins possible de renseignements liés aux individus. Éviter la collecte de renseignements sensibles (biométrie, géolocalisation, santé).**
- **Démontrer la nécessité de recueillir chaque renseignement personnel.**

6. *Limiter l'utilisation et la communication des renseignements personnels*

Les renseignements collectés par une application de traçage ou de notification des contacts ne devraient servir qu'aux fins de santé publique spécifiques identifiées lors de son déploiement, que ces renseignements soient identificatoires, anonymisés, dépersonnalisés ou pseudonymisés.

La communication de ces renseignements devrait être limitée aux seuls situations et intervenants nécessaires au fonctionnement de l'application et à l'atteinte de ces fins.

Recommandation 6 : Afin de limiter l'utilisation et la communication des renseignements personnels, que ceux-ci soient identificatoires, anonymisés, dépersonnalisés ou pseudonymisés, la Commission recommande de :

- **Ne les utiliser qu'aux fins de santé publique spécifiques identifiées lors du déploiement de l'application et nécessaire à son utilisation;**
- **Limiter leur communication aux seuls situations et intervenants nécessaires au fonctionnement de l'application et à l'atteinte de ces fins.**

7. *Mettre en place une infrastructure technologique et un écosystème sécuritaires*

Les applications de traçage ou de notification des contacts sont des outils reposant largement sur une infrastructure technologique : celle-ci doit être conforme aux plus hauts standards disponibles en matière de confidentialité et de sécurité. Des audits de sécurité indépendants devraient être faits afin de valider les éléments de sécurité. Toute faille ou incident de sécurité détecté après la mise en service d'une éventuelle application de traçage ou de notification des contacts doit être résolu et rendu public.

D'autres aspects doivent aussi faire l'objet d'une attention particulière. Par exemple, des applications tierces pourraient également interagir avec l'application

déployée ou pourraient exploiter d'éventuelles failles dans sa sécurité. De même, certaines tentatives d'hameçonnage ont été rapportées par les médias et de fausses applications circulent déjà[35].

Enfin, l'écosystème dans lequel évoluera une éventuelle application doit être entièrement sécurisé. Des informations sont susceptibles d'être échangées entre les différents organismes, peut-être même hors du Québec (ex. : avec Santé Canada). Si des fournisseurs tiers interviennent dans le fonctionnement de l'application, des ententes visant à assurer la protection des renseignements doivent être conclues et l'ensemble de ces communications doit respecter le cadre juridique actuel.

Recommandation 7 : Afin de prévenir les incidents de sécurité et les accès, l'utilisation ou la communication non autorisés des renseignements personnels, la Commission recommande la mise en place d'une infrastructure technologique et d'un écosystème sécuritaires. Elle recommande aussi de :

- **Mettre en œuvre des mesures de protection techniques et juridiques répondant aux plus hauts standards en la matière;**
- **Mener une veille constante des menaces inhérentes à l'utilisation de l'éventuelle technologie retenue;**
- **Tenir les utilisateurs informés des risques et des incidents de sécurité, le cas échéant.**

8. DÉTERMINER LES CONDITIONS DE MISE HORS SERVICE DE CETTE MESURE TEMPORAIRE ET DÉTRUIRE LES RENSEIGNEMENTS RECUEILLIS

La plupart des observateurs ont souligné l'importance de circonscrire dans le temps l'utilisation d'une application de traçage ou de notification des contacts et d'indiquer les modalités de sa mise hors service, étant donné qu'il s'agit d'une mesure exceptionnelle. Comme elle l'a indiqué dans la déclaration commune avec ses homologues canadiens, la Commission partage cet avis. Il en va de la nécessité et surtout, de la proportionnalité de cette mesure.

Il est difficile de cibler une date précise de mise hors service, vu l'évolution constante de la situation sanitaire. Par conséquent, un terme prédéfini devrait être déterminé avant le déploiement d'une telle application. À son expiration, ce terme

---

[35] Voir par exemple HUMPHREYS, A., « Hackers target Canadians with fake COVID-19 contact-tracing app disguised as official government software », *The National Post* (24 juin 2020), en ligne: <https://nationalpost.com/news/canada/hackers-target-canadians-with-fake-covid-19-contact-tracing-app-disguised-as-official-government-software> (consulté le 18 juillet 2020).

pourrait être renouvelé périodiquement si la situation en cours à ce moment justifie la pertinence de poursuivre l'utilisation de l'application. Il faut éviter qu'une mesure initialement temporaire devienne permanente sans la tenue d'un débat public sur la question.

Comme indiqué précédemment, si son efficacité n'est pas concluante, une application de traçage ou de notification des contacts devrait aussi être mise hors service.

Dans un cas comme dans l'autre, tous les renseignements personnels recueillis pendant sa période d'utilisation devraient être détruits et l'utilisateur devrait en recevoir la confirmation. L'utilisateur doit pouvoir être assuré que ses renseignements ne seront pas conservés ni réutilisés une fois la crise sanitaire passée.

Recommandation 8 : Afin d'affirmer le caractère temporaire d'une application de traçage ou de notification des contacts, la Commission recommande de :

- **Déterminer le terme et les conditions de la mise hors service de l'application, incluant si son efficacité n'est pas démontrée;**
- **Détruire tous les renseignements lors de la mise hors service de l'application et confirmer cette destruction aux utilisateurs.**

9. PERMETTRE L'EXERCICE DE SES DROITS PAR LA PERSONNE CONCERNÉE

Les responsables de la mise en œuvre de l'application doivent s'assurer que les droits des personnes concernées puissent être respectés et que des recours appropriés puissent être exercés, le cas échéant. Ces droits doivent être connus des utilisateurs.

Le nom et les coordonnées d'une personne contact à joindre en cas de questions au sujet de l'application ou pour l'exercice de leurs droits doivent être facilement accessibles aux utilisateurs.

Recommandation 9 : Afin de permettre à la personne concernée d'exercer ses droits en matière d'accès et de protection des renseignements personnels, la Commission recommande :

- **D'informer l'utilisateur de ses droits et recours lors de la mise en service de l'application et de rendre facilement disponible, par la suite, ces informations pour qu'il puisse s'y référer au besoin;**
- **De rendre disponible le nom et les coordonnées d'une personne contact à joindre en cas de questions au sujet de l'application ou pour l'exercice de ses droits.**

10. Assumer la responsabilité par une évaluation continue, une reddition de compte et un contrôle externe indépendant

Dans l'état actuel des connaissances sur l'utilisation et l'efficacité des applications de traçage ou de notification des contacts à la COVID-19, le choix d'y recourir implique une certaine part d'incertitude. Ces inconnues et les enjeux soulevés par le recours à ces applications requièrent la mise en place de mesures d'évaluation continue, assorties d'une reddition de compte transparente.

Ces mesures doivent permettre de détecter rapidement et de régler tout problème résultant de l'utilisation de l'application. Les évaluations peuvent être réalisées par les promoteurs de l'application (ex. : le gouvernement ou les autorités de santé publique), mais aussi par des tiers indépendants.

Comme indiqué précédemment, ces évaluations devraient porter notamment sur l'efficacité de l'application et les mesures de protection mises en place, par exemple en matière de sécurité ou de respect de la vie privée.

Le résultat de ces évaluations devrait être diffusé de manière proactive.

Enfin, un organisme indépendant doit pouvoir assurer une surveillance des mesures de protection des renseignements personnels mises en place et de la conformité de l'application avec le cadre juridique québécois. À cet égard, la Commission dispose déjà de l'expertise et des pouvoirs d'enquête et d'inspection lui permettant de jouer ce rôle.

Recommandation 10 : Dans un objectif de responsabilité et d'imputabilité, la Commission recommande :

- **D'évaluer de façon continue l'efficacité d'une éventuelle application de traçage ou de notification des contacts et des mesures de protection mises en place;**
- **De rendre compte de manière transparente du résultat de ces évaluations;**
- **De s'assurer de la surveillance par une autorité indépendante du respect des principes, de la suffisance des mesures de protection en place et de la conformité avec la législation applicable.**

11. Adopter un cadre juridique spécifique au déploiement et à l'utilisation de l'application au Québec

Au même titre que plusieurs homologues et experts, la Commission considère que le déploiement d'outils technologiques de traçage ou de notification des contacts

doit être soumis à un encadrement juridique spécifique pour garantir aux citoyens le respect des principes énoncés précédemment.

Ainsi, bien que l'analyse du respect de la législation québécoise actuelle dans la conception et l'utilisation de ces applications soit essentielle, elle ne saurait suffire. Les lois existantes ne permettent pas d'encadrer adéquatement tous les enjeux soulevés précédemment. Par exemple, le respect du caractère volontaire de l'application, les restrictions quant à l'utilisation et à la communication des renseignements personnels et la durée déterminée de cette mesure exceptionnelle ne sont pas des obligations incluses dans le cadre juridique actuel.

L'autorégulation n'est pas une avenue qui nous apparaît acceptable dans les circonstances, compte tenu des enjeux en cause et de la confiance nécessaire au déploiement de ce type d'outil technologique. Le déploiement d'une éventuelle application de cette nature devrait être accompagné de l'adoption d'un encadrement juridique spécifique, comme d'autres pays l'ont fait, par loi ou par décret, dont la France[36], la Suisse[37] et l'Australie[38].

Il s'agit d'ailleurs d'une recommandation de l'OMS, ainsi que du Comité consultatif d'experts sur la société, la technologie et l'éthique en cas de pandémie du CIFAR, organisation de recherche mondiale basée au Canada[39].

Recommandation 11 : La Commission recommande d'adopter un cadre juridique spécifique applicable au déploiement, le cas échéant, et à l'utilisation d'une application de traçage ou de notification des contacts au Québec.

---

[36] *Décret n° 2020-650 du 29 mai 2020 relatif au traitement de données dénommé « StopCovid »*, (29 mai 2020), 2020-650, en ligne : <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000041936881&categorieLien=id> (consulté le 15 juillet 2020).

[37] CONSEIL FÉDÉRAL SUISSE, *Ordonnance du 24 juin 2020 sur le système de traçage de proximité pour le coronavirus SARS-CoV-2 (OSTP)*, (24 juin 2020), RS 818.101.25, en ligne : <https://www.admin.ch/opc/fr/classified-compilation/20201730/index.html> (consulté le 5 août 2020).

[38] PARLEMENT AUSTRALIEN, *Privacy Amendment (Public Health Contact Information) Bill 2020*, 13 mai 2020, en ligne : <https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22legislation/bills/r6556_aspassed/0000%22> (consulté le 14 mai 2020). Voir également BUREAU DU COMMISSAIRE À L'INFORMATION AUSTRALIEN, « The COVIDSafe app and my privacy rights », *Bureau du Commissaire à l'information australien* (28 mai 2020), en ligne : <https://www.oaic.gov.au/privacy/covid-19/the-covidsafe-app-and-my-privacy-rights/> (consulté le 28 mai 2020).

[39] ORGANISATION MONDIALE DE LA SANTÉ, préc., note 7; CIFAR, préc., note 7.

E. CADRE JURIDIQUE SPÉCIFIQUE ACCOMPAGNANT LE DÉPLOIEMENT ET L'UTILISATION D'UNE APPLICATION DE TRAÇAGE OU DE NOTIFICATION DES CONTACTS AU QUÉBEC

Étant donné l'importance de la recommandation 11, la Commission souhaite détailler davantage les éléments minimaux que devrait contenir ce cadre juridique.

Particulièrement dans le contexte où l'application choisie pourrait s'inscrire à l'intérieur d'un projet pancanadien, ce cadre devrait notamment tenir compte de la spécificité des lois québécoises en matière de protection des renseignements personnels. Conséquemment, les obligations déjà prévues dans la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*[40] ne sont pas incluses dans l'énumération suivante.

CIRCONSCRIRE LES RENSEIGNEMENTS PERSONNELS QUI PEUVENT ÊTRE RECUEILLIS

- Identifier les renseignements qui peuvent être recueillis et par quelles personnes ils peuvent l'être. Dans l'éventualité d'une application impliquant divers paliers de gouvernement, préciser le partage des responsabilités.
- Interdire toute autre collecte de renseignements personnels.
- Interdire la réidentification de renseignements dépersonnalisés ou pseudonymisés.

RESTREINDRE LES FINALITÉS ET LES UTILISATIONS PERMISES DES RENSEIGNEMENTS PERSONNELS RECUEILLIS

- Circonscrire de façon précise les objectifs de santé publique visés par l'application.
- Interdire l'utilisation des renseignements pour d'autres finalités que celles déterminées initialement.
- Prévoir les personnes qui auront accès aux renseignements, l'étendue de cet accès (c'est-à-dire quels renseignements leur seront accessibles) et les motifs le justifiant.

---

[40] RLRQ, c. A-2.1.

Mesurer en continu l'efficacité et la protection accordée aux renseignements personnels

- Prévoir l'évaluation de l'efficacité de l'application de manière périodique et la diffusion du rapport d'évaluation.
- Exiger, avant son déploiement, la réalisation d'une évaluation des facteurs relatifs à la vie privée et sa transmission à la Commission, pour analyse et recommandations. Prévoir qu'une mise à jour de cette évaluation doit également être réalisée et transmise à la Commission pour toute modification significative.
- Prévoir la diffusion de cette évaluation.

Affirmer et maintenir le caractère volontaire de l'application

- Affirmer clairement le caractère volontaire de l'application.
- Interdire à quiconque d'exiger l'utilisation de l'application ou le partage de son contenu (consultation par une personne tierce, communication ou autre) à quelque fin que ce soit (ex. accès à un lieu, à un bien, à un service, à un emploi, etc.)
- Prévoir des sanctions sévères en cas d'infraction.
- Exiger qu'une information détaillée en des termes clairs soit accessible à l'utilisateur avant toute utilisation de l'application.
- Requérir l'obtention d'un consentement distinct pour chacune des finalités de santé publique poursuivies et pour tout événement significatif par la suite (ex. : entrée d'une clé de diagnostic positif et communication des informations de « contact »).
- Prévoir la possibilité pour un utilisateur de retirer son consentement en tout temps ou de désinstaller l'application, ces deux actions impliquant la destruction des renseignements le concernant.

Assurer la transparence

- Obliger la diffusion du code source de l'application avant sa mise en service afin de permettre à des tiers compétents de l'évaluer du point de vue de la technologie et de la cybersécurité.
- Diffuser les modalités concernant la collecte, la conservation et la disposition des renseignements collectés.
- Diffuser de manière proactive tout autre rapport portant notamment sur l'efficacité de l'application pour atteindre l'objectif visé et aviser les utilisateurs et la Commission en cas d'incident ou de vulnérabilités susceptibles d'affecter la protection des renseignements personnels.

GARANTIR LE CARACTÈRE TEMPORAIRE DE LA MESURE

- Préciser la durée d'utilisation de l'application et les conditions de sa mise hors service
- Inclure des modalités de mise hors service dans le cas où l'application n'atteint pas un niveau d'efficacité suffisant à l'intérieur d'un délai raisonnable, ou si elle s'avère nuisible aux fins qui ont été fixées avant son déploiement.
- Prévoir les modalités de destruction des renseignements recueillis par l'application; ceux-ci devraient être détruits lorsque le terme sera atteint, ou au plus tard, lorsque la crise sanitaire sera terminée.

F. CONCLUSION

La Commission réitère que les présentes recommandations sont d'ordre général. Seule l'analyse d'une application spécifique pourrait lui permettre d'émettre un avis précis sur sa conformité et sur les enjeux propres à son utilisation.

Dans l'éventualité où le gouvernement déciderait d'aller de l'avant avec le déploiement d'un outil technologique de traçage ou de notification des contacts, la Commission analysera l'évaluation des facteurs relatifs à la vie privée qui sera produite afin de formuler des recommandations plus spécifiques.

La Commission demeure disponible pour répondre à toute question que pourrait soulever le présent mémoire.

RÉCAPITULATIF DES RECOMMANDATIONS

Recommandation 1 : Pour évaluer la nécessité et la proportionnalité du recours à un outil technologique de traçage ou de notification des contacts, la Commission recommande, préalablement à son déploiement, de :

- **Déterminer les finalités spécifiques de santé publique poursuivies. Celles-ci doivent être fondées sur la science selon des données probantes et libellées avec un certain niveau de précision;**
- **S'assurer que l'outil s'inscrit à l'intérieur de la stratégie de lutte contre la transmission de la COVID-19 des autorités de santé publique et que les autres éléments de cette stratégie en lien avec l'utilisation de l'outil sont disponibles (ex. : ressources pour le dépistage, pour un traçage plus poussé des contacts, pour les informations aux personnes recevant une notification de contact à risque, etc.);**
- **Déterminer les critères permettant d'évaluer l'efficacité de l'outil et démontrer qu'il est susceptible d'être efficace pour atteindre les objectifs spécifiques de santé publique identifiés;**
- **Mettre sur pied un mécanisme d'évaluation en continu de l'efficacité de l'outil.**

Recommandation 2 : Afin de minimiser l'atteinte aux droits dès la conception, la Commission recommande de :

- **Réaliser une évaluation des facteurs relatifs à la vie privée concernant la solution retenue et la soumettre pour analyse et commentaires à la Commission, avant le déploiement de l'application;**
- **Diffuser publiquement cette évaluation et l'avis de la Commission (voir la recommandation 4 au sujet de la transparence);**
- **Mettre en œuvre les principes de protection de la vie privée dès la conception;**
- **Porter une attention particulière à la technologie et aux renseignements utilisés.**

Recommandation 3 : Afin de garantir le caractère volontaire de l'utilisation de l'application et d'assurer un consentement valide, la Commission recommande de :

- **Fournir une information claire, simple et complète aux utilisateurs afin de permettre un consentement éclairé. Cette information devrait inclure minimalement : les objectifs de santé publique poursuivis, la description**

du fonctionnement de l'application, les limites de l'application, la liste des renseignements collectés et les raisons pour lesquelles ils le sont, le détail concernant le stockage des données, l'ensemble des utilisations et des communications prévues, les modalités de destruction des renseignements, les risques liés à l'utilisation de l'application, les droits des utilisateurs quant à leurs renseignements personnels et leurs recours;

- **Éviter de donner des garanties d'anonymat aux utilisateurs si les renseignements sont dépersonnalisés ou pseudonymisés;**
- **Obtenir un consentement distinct, spécifique et explicite :**
    - **Demander un premier consentement à l'installation de l'application, préalablement à sa mise en fonction;**
    - **Demander un consentement distinct pour chaque finalité de santé publique pour laquelle les renseignements personnels sont recueillis, utilisés ou communiqués, de même que pour tout autre événement significatif lié à l'utilisation de l'application;**
- **Permettre en tout temps à un utilisateur de retirer son consentement et de cesser d'utiliser l'application ou de la désinstaller;**
- **Détruire sans délai tout renseignement concernant cet utilisateur;**
- **Mettre en place toutes les conditions permettant de conserver le caractère volontaire de l'utilisation de l'application, notamment en interdisant à quiconque d'exiger l'installation de l'application ou la consultation de son contenu.**

Recommandation 4 : Afin d'adopter une démarche transparente en aval et en amont, la Commission recommande de :

- **Diffuser les motifs justifiant une éventuelle décision de recourir à une telle mesure exceptionnelle et les modalités de son déploiement;**
- **Diffuser le code source de l'application et de toute autre composante susceptible d'avoir un impact sur les risques liés à son utilisation (ex. : API) afin de faciliter un audit externe indépendant;**
- **Informer les citoyens et la Commission de tout incident ou de toute faille de sécurité ou risque identifié et des mesures prises pour y remédier;**
- **Diffuser l'évaluation des facteurs relatifs à la vie privée au sujet de l'application[41];**

[41] La Commission rendra public son avis au sujet de cette évaluation.

- **Rendre public tout rapport concernant l'évaluation de l'efficacité de l'application pour atteindre le ou les objectif(s) de santé publique identifié(s).**

Recommandation 5 : Afin de limiter la collecte de renseignements personnels, la Commission recommande de :

- **Privilégier l'utilisation de renseignements anonymisés, dépersonnalisés ou pseudonymisés.**
- **Privilégier une application fonctionnant en mode décentralisé et recueillant le moins possible de renseignements liés aux individus. Éviter la collecte de renseignements sensibles (biométrie, géolocalisation, santé).**
- **Démontrer la nécessité de recueillir chaque renseignement personnel.**

Recommandation 6 : Afin de limiter l'utilisation et la communication des renseignements personnels, que ceux-ci soient identificatoires, anonymisés, dépersonnalisés ou pseudonymisés, la Commission recommande de :

- **Ne les utiliser qu'aux fins de santé publique spécifiques identifiées lors du déploiement de l'application et nécessaire à son utilisation;**
- **Limiter leur communication aux seuls situations et intervenants nécessaires au fonctionnement de l'application et à l'atteinte de ces fins.**

Recommandation 7 : Afin de prévenir les incidents de sécurité et les accès, l'utilisation ou la communication non autorisés aux renseignements personnels, la Commission recommande la mise en place d'une infrastructure technologique et d'un écosystème sécuritaires. Elle recommande aussi de :

- **Mettre en œuvre des mesures de protection techniques et juridiques répondant aux plus hauts standards en la matière;**
- **Mener une veille constante des menaces inhérentes à l'utilisation de l'éventuelle technologie retenue;**
- **Tenir les utilisateurs informés des risques et des incidents de sécurité, le cas échéant.**

Recommandation 8 : Afin d'affirmer le caractère temporaire d'une application de traçage ou de notification des contacts, la Commission recommande de :

- **Déterminer le terme et les conditions de la mise hors service de l'application, incluant si son efficacité n'est pas démontrée;**

- **Détruire tous les renseignements lors de la mise hors service de l'application et confirmer cette destruction aux utilisateurs.**

Recommandation 9 : Afin de permettre à la personne concernée d'exercer ses droits en matière d'accès et de protection des renseignements personnels, la Commission recommande :

- **D'informer l'utilisateur de ses droits et recours lors de la mise en service de l'application et de rendre facilement disponible, par la suite, ces informations pour qu'il puisse s'y référer au besoin;**
- **De rendre disponible le nom et les coordonnées d'une personne contact à joindre en cas de questions au sujet de l'application ou pour l'exercice de ses droits.**

Recommandation 10 : Dans un objectif de responsabilité et d'imputabilité, la Commission recommande :

- **D'évaluer de façon continue l'efficacité d'une éventuelle application de traçage ou de notification des contacts et des mesures de protection mises en place;**
- **De rendre compte de manière transparente du résultat de ces évaluations;**
- **De s'assurer de la surveillance par une autorité indépendante du respect des principes, de la suffisance des mesures de protection en place et de la conformité avec la législation applicable.**

Recommandation 11 : La Commission recommande d'adopter un cadre juridique spécifique applicable au déploiement, le cas échéant, et à l'utilisation d'une application de traçage ou de notification des contacts au Québec.

(Voir les détails dans la section *Cadre juridique spécifique accompagnant le déploiement et l'utilisation d'une application de traçage ou de notification des contacts au Québec.*)