ASSEMBLÉE NATIONALE DU QUÉBEC

PREMIÈRE SESSION QUARANTE-DEUXIÈME LÉGISLATURE

Journal des débats

de la Commission permanente des institutions

Le vendredi 14 août 2020 — Vol. 45 N° 79

Consultations particulières 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 (3)

Président de l'Assemblée nationale :
M. François Paradis

2020

Abonnement annuel (TPS et TVQ en sus):

Débats de l'Assemblée	145,00 $
Débats de toutes les commissions parlementaires	500,00 $
Pour une commission parlementaire en particulier	100,00 $
Index (une session, Assemblée et commissions)	30,00 $

Achat à l'unité: prix variable selon le nombre de pages.

Règlement par chèque à l'ordre du ministre des Finances et adressé comme suit:

Assemblée nationale du Québec
Direction de la gestion immobilière et des ressources matérielles
1020, rue des Parlementaires, bureau RC.85
Québec (Québec)
G1A 1A3

Téléphone: 418 643-2754
Télécopieur: 418 643-8826

Consultation des travaux parlementaires de l'Assemblée ou des commissions parlementaires dans Internet à l'adresse suivante:
www.assnat.qc.ca

Dépôt légal: Bibliothèque nationale du Québec
ISSN 0823-0102

Commission des institutions

Le vendredi 14 août 2020 — Vol. 45 N° 79

Table des matières

Autres intervenants

M. André Bachand, président

Mme Joëlle Boutin
M. Mathieu Lévesque
Mme Marwah Rizqy
M. Gabriel Nadeau-Dubois
M. Martin Ouellet
M. Guy Ouellette
Mme Lucie Lecours
Mme Marie-Claude Nichols
M. Luc Provençal

Le vendredi 14 août 2020 — Vol. 45 N° 79

Consultations particulières 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 (3)

(Neuf heures deux minutes)

Le Président (M. Bachand) : Bonjour. À l'ordre, s'il vous plaît! Ayant constaté le quorum, je déclare la séance de la Commission des institutions ouverte. Je vous souhaite la bienvenue et, comme vous le savez, je demande à toutes personnes présentes présentes dans la salle de bien vouloir éteindre la sonnerie de leurs appareils électroniques.

La commission est réunie afin de procéder aux consultations particulières 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.

Avant de débuter, Mme la secrétaire, y a-t-il des remplacements?

La Secrétaire : Oui, M. le Président. Mme Lachance (Bellechasse) est remplacée par M. Provençal (Beauce-Nord); M. Lamothe (Ungava) est remplacé par Mme Boutin (Jean-Talon); Mme Robitaille (Bourassa-Sauvé) est remplacée par Mme Nichols (Vaudreuil); M. Tanguay (LaFontaine) est remplacé par Mme Rizqy (Saint-Laurent); M. Fontecilla (Laurier-Dorion) est remplacé par M. Nadeau-Dubois (Gouin) et M. LeBel (Rimouski) est remplacé par M. Ouellet (René-Lévesque).

Auditions (suite)

Le Président (M. Bachand) : Merci beaucoup. Ce matin, nous entendrons les personnes suivantes : M. Stéphane Roche, professeur titulaire de sciences géomatiques de l'Université Laval; Mme Castets-Renard, professeure titulaire de la Faculté de droit civil de l'Université d'Ottawa; Mme Guliani, première conseillère législative de l'American Civil Liberties Union; et aussi M. Claude Sarrazin, qui sera notre premier intervenant, spécialiste en cybersécurité.

Je vous informe par ailleurs que les auditions de M. Sarrazin, Mme Castets-Renard et Mme Guliani se feront par visioconférence, et, pour cette dernière, il y aura interprétation simultanée.

Donc, M. Sarrazin, bienvenue. Bon matin. Merci d'être avec nous. Alors, je vous laisse la parole pour 10 minutes, et, après ça, nous aurons un échange avec les membres de la commission. Alors, la parole est à vous.

M. Claude A. Sarrazin

(Visioconférence)

M. Sarrazin (Claude A.) : Merci beaucoup. Bien, écoutez, je vous remercie de m'avoir invité pour cette analyse. Je suis fondamentalement un enquêteur. Depuis plus de 30 ans, je travaille dans le domaine des enquêtes et j'ai développé une spécialité au point de vue de ce qui s'appelle la cybercriminalité. Cette perspective-là m'a permis d'élaborer certaines façons de faire ou de développer une approche quant à la protection des informations par la suite. Je l'enseigne également à l'UQAM, à l'École des sciences de la gestion, au niveau de la maîtrise, dans un cours que je désigne, non officiellement, Cybercrime 201.

Donc, si vous me permettez, j'ai un court préambule sur l'analyse, un peu, de la situation. Un associé de recherche principal au Citizen Lab de l'Université de Toronto, Christopher Parsons, mentionne un seuil de 65 % à 80 % d'utilisation de l'application pour que celle-ci ait un impact majeur sur la propagation du virus. Cependant, il faut prendre en compte que ce n'est pas 100 % de la population qui possède un téléphone intelligent. Donc, afin d'obtenir un seuil d'utilisation de près de 60 % de la population, il faut qu'une grande majorité des utilisateurs de téléphones intelligents utilisent l'application de notification de contacts.

Le fait que l'application canadienne COVID Alert ne fonctionne que sur les appareils intelligents utilisant les systèmes Apple ou Android de fabrication récente, avec mise à jour du système d'exploitation, soulève une importante préoccupation. En effet, les communautés les plus à risque et qui bénéficieraient le plus de l'utilisation d'une telle application se trouveront donc à être celles qui n'y ont pas accès. Il s'agit des communautés les plus démunies, des personnes sans domicile fixe, des enfants et des personnes âgées. En effet, il n'y a aucune étude empirique indiquant qu'une application de suivi de contacts serait efficace pour lutter contre la pandémie si ce n'est pas la grande majorité de la population qui l'utilise. Et, si, de ce fait, la grande majorité le fait, ceci pourrait amener un intérêt renouvelé d'autres types d'utilisateurs, ce qui m'amène à ma propre spécialité, le cybercrime.

Il importe de souligner que le modus operandi des cybercriminels ne correspond pas à celui des criminels traditionnels. Ces derniers cherchent généralement une cible potentielle avant de définir leur plan. Les cybercriminels, dans bien des cas, identifient les vulnérabilités pour par la suite commettre un délit. Les cybercriminels collaborent généralement à distance avec un réseau, selon leur spécialité et leur capacité à exploiter les failles. Ils ne cherchent pas l'opportunité, ils la

créent. Comme démontré dans les dernières années, les nouvelles technologies comportent souvent d'importantes vulnérabilités. Par contre, les vulnérabilités Bluetooth sont rarement discutées, et c'est la base du système qui est mis de l'avant par le fédéral.

Bien qu'il soit vrai que l'utilisation du Bluetooth soit moins intrusive que la technologie de géolocalisation et ne collecte pas directement de données personnelles, elle comporte des vulnérabilités permettant à certains cybercriminels d'avoir accès à ces données. Il appert que le Bluetooth soit réputé pour n'être détectable que sur de courtes distances et qu'il soit difficile d'en extraire des informations. Cependant, il n'est pas impossible, pour des pirates informatiques, d'utiliser le «reverse engineering» pour obtenir l'accès aux données d'un tiers en utilisant les failles de sécurité.

Certains outils ont été développés afin d'obtenir accès aux échanges entre les appareils utilisant Bluetooth, tels qu'un téléphone et une paire d'écouteurs, permettant ainsi à une tierce personne d'écouter une conversation téléphonique. En effet, il est possible d'étendre la portée de détection d'un appareil Bluetooth en utilisant d'autres appareils ou des balises Bluetooth. Des vulnérabilités Bluetooth connues portent le nom de BlueBorne. Cette collection de failles permettait à des pirates informatiques d'installer des «malware» et d'effectuer des attaques sur les autres appareils en utilisant le Bluetooth.

Ce qu'on appelle le «Bluetooth Mesh Networking» rend cette vulnérabilité encore plus grave puisque les pirates pourraient sauter d'un appareil à l'autre facilement avec BlueBorne. L'attaquant commence par détecter un appareil Bluetooth à proximité avant d'identifier son adresse MAC. Cette dernière lui permet d'identifier le système d'exploitation de l'appareil et d'ajuster son attaque avant de la déployer.

Une autre vulnérabilité connue est BleedingBits, des puces électroniques installées dans plusieurs types d'appareils. Celles-ci permettaient des attaques sans même que l'attaquant ne soit jumelé avec l'appareil en question. Donc, on n'attaque pas directement la fonctionnalité Bluetooth, mais bien le hardware, si on veut, qui permet l'utilisation de Bluetooth.

Certaines vulnérabilités permettent d'obtenir la clé d'encryption utilisée par un appareil et de l'utiliser afin d'obtenir des données et de falsifier certaines informations. Des chercheurs en sécurité de l'Université de Boston, notamment, ont découvert qu'ils pouvaient identifier les appareils utilisés lors d'une connexion par technologie Bluetooth malgré que les identifiants étaient cryptés par l'appareil. De plus, lorsque le niveau de sécurité Bluetooth n'est pas maximal, certaines informations sont échangées sans encryption entre les différents appareils, ce qui accroît les risques puisque l'information n'a pas à être hackée, mais elle peut plutôt être déduite à partir de l'information interceptée par un tiers.

La sécurité standard de la technologie Bluetooth inclut deux étapes d'authentification, soit «legacy authentification procedure» et «secure authentication procedure». Celles-ci utilisent une clé d'encryption. Ces mesures sont supposées empêcher les attaques par usurpation, aussi appelées BIAS, «Bluetooth Impersonation Attacks». Une équipe de chercheurs européens provenant d'Oxford et de l'école polytechnique de Lausanne a démontré que même la technologie la plus récente de Bluetooth était vulnérable à ce type d'attaque. Cette équipe a attaqué différents types d'appareils possédant des puces électroniques des systèmes d'exploitation différents les uns des autres afin de démontrer que ceux-ci ne sont pas à l'abri des attaques par Bluetooth.

• (9 h 10) •

Bien que BlueBorne et Bleedingbits soient les vulnérabilités les plus connues et qu'elles aient été corrigées, elles ne sont pas les seules qui ont été détectées. Effectivement, en février dernier, BlueFrag, une nouvelle vulnérabilité critique, a été détectée. Celle-ci a également été corrigée peu de temps après sa détection, mais elle démontre que de nouvelles mises à jour des systèmes d'exploitation des appareils électroniques peuvent toujours introduire de nouvelles vulnérabilités. En effet, Niels Schweisshelm, directeur du programme HackerOne, estime que le Bluetooth et ses futures utilisations ne seront jamais à l'abri de nouvelles failles.

Pour le chercheur Jan Ruge, de la Technische Universität Darmstadt, le meilleur moyen de se protéger contre des attaques utilisant le Bluetooth est de désactiver celui-ci lorsqu'il n'est pas en utilisation. Cette méthode de sécurité, bien entendu, irait à l'encontre de toute utilisation d'un système de traçage.

Par contre, comme l'application Alerte COVID utilise le Bluetooth, il serait nécessaire de laisser le Bluetooth de l'appareil activé en tout temps, ce qui accroît les risques d'exploitation d'une faille. Et, à partir du moment que les fraudeurs potentiels démontrent un intérêt pour cette technologie-là et que le seuil d'utilisation dépasse le 60 %, on accroît considérablement le risque.

Il faut être d'autant plus vigilant avec les appareils mobiles fournis par l'employeur afin de ne pas mettre à risque le système également de l'employeur, parce qu'à travers ces différentes attaques là ce n'est pas nécessairement l'individu qui l'utilise qui peut être ciblé, mais bien l'employeur où il y a une connexion avec l'appareil de l'employé en question. Qu'en est-il également des outils utilisés par certains employeurs pour contrôler l'utilisation de leur matériel? De plus, est-ce que ceux-ci pourraient être tentés d'accéder aux informations personnelles à d'autres fins?

Il est important de noter que nous n'avons pas présentement accès à tous les détails concernant les protocoles de sécurité et le niveau d'encryption utilisé présentement par les outils proposés. De plus, Stas Protassov, cofondateur et président de la technologie d'Acronis, émet une mise en garde puisqu'il croit que certaines applications malveillantes imitant l'application officielle pourraient être mises en circulation.

Il est donc primordial que seule l'application officielle soit téléchargée afin d'assurer la confidentialité des données personnelles des utilisateurs. On l'a vu pendant le COVID, il y a beaucoup de fraudeurs qui ont profité, comme ils le font généralement, de cette situation-là pour leur permettre d'avoir un motif, justement, d'effectuer des attaques. On l'a vu notamment dans le cas du PCU.

En conclusion, le succès d'une application de notification des contacts ou de suivi de contacts dépend en grande partie de la confiance du public envers la fiabilité de l'outil et du gouvernement ou de l'organisme qui le met en oeuvre. Il est primordial de ne pas sacrifier le droit à la vie privée et la sécurité pour un outil technologique dont les bienfaits ne sont pas garantis.

Si, toutefois, une application est utilisée afin de protéger les données personnelles, celle-ci devrait être analysée localement dans le téléphone de l'usager et, idéalement, ne pas centraliser l'ensemble de ces données-là. Si une application plus intrusive était utilisée et que les données des usagers étaient stockées dans un serveur localisé, il est certain que plusieurs réseaux criminels seraient intéressés à accéder à ces informations-là. On l'a vu, on l'a su, la concentration d'une grande quantité de données attire de nombreuses attaques.

Et puis, puisque l'application proposée par le gouvernement canadien n'est pas accessible à tous, et si on la rend disponible aux versions antérieures des systèmes d'opération pour pouvoir aller chercher un maximum d'utilisateurs, nous courrons donc le risque de nous rendre collectivement vulnérables à une autre forme de virus qui est très intrusive et qui pourrait nous amener de Charybde en Scylla.

Le Président (M. Bachand) : Merci beaucoup pour votre présentation. On débute la période d'échange. Mme la députée de Jean-Talon, s'il vous plaît.

Mme Boutin : Bonjour, M. Sarrazin. Merci beaucoup de votre présence. C'est vraiment très apprécié, là. La cyberdéfense, ça m'intéresse particulièrement, là. Je dois vous avouer, je suis très au fait qu'il y a eu plusieurs... Bien, il y a plusieurs attaques en tout temps dans le monde... plusieurs institutions. Puis je ne veux pas faire peur aux gens qui nous écoutent, là. Il y a des mesures qui sont en place pour contrer ça. Même le gouvernement a renforcé ses mesures dans la dernière année, parce qu'on était assez conscients de ça.

Là, on parle de quelque chose de très différent, puis je trouve intéressant... parce que ça parle de nos appareils directement. Moi-même, j'ai quelques inquiétudes parce que je suis une utilisatrice de beaucoup d'applications. Mon Bluetooth est activé en tout temps, mon wifi. Je suis probablement une des personnes les plus à risque ici, dans la salle, pour vrai, puis, en le disant, bien, peut-être qu'il y a des pirates qui vont attaquer mon téléphone cellulaire.

Donc, ma première question tourne autour de la sécurité, puis j'aimerais savoir, tu sais, concrètement, comment ça se passe. Est-ce que des gens pourraient... Même, là, si jamais j'ai des applications, parce que j'en ai beaucoup, puis ça doit rouler en tout temps, est-ce qu'un pirate malveillant, tu sais, actuellement, qui m'entend pourrait décider de venir et saisir, admettons, mes données bancaires ou quelque chose comme ça, tu sais, des données très personnelles? Parce que je ne pense pas qu'il s'intéresserait aux données aléatoires ou si j'ai le COVID ou non. Je pense plutôt qu'il irait chercher des données qui seraient utiles, dont mes données bancaires, mes numéros, mon adresse, toutes les données que j'ai mises sur mon téléphone cellulaire, ainsi que ma reconnaissance faciale. J'ai tout mis ça, moi. Est-ce que moi, je peux me faire pirater, ou d'autres personnes?

M. Sarrazin (Claude A.) : Bien, la question est très large. La réponse l'est tout autant. Oui, tout le monde a le potentiel d'être victime d'un piratage de données.

Maintenant, ça dépend beaucoup des vulnérabilités individuelles, donc, les mises à jour qui sont sur votre téléphone. Comme je le mentionnais tout à l'heure, il y a beaucoup de menaces qu'on connaît par rapport à Bluetooth, par exemple, qui ont été corrigées, sauf que ce qu'on sait également, c'est que les hackeurs, eux, vont aller faire du «reverse engineering» pour aller voir comment que la patch a été corrigée et appliquée, et là ils vont trouver ou ils vont tenter de trouver de nouvelles vulnérabilités pour pouvoir les exploiter.

Donc, les mises à jour sont hyperimportantes. À partir de ce moment-là, on est à risque en tout temps par rapport à nos appareils de communication. On ne peut pas arrêter de penser à la sécurité, mais un des risques très importants... Et le plus grand risque est probablement l'utilisateur lui-même qui, par erreur... Et, on l'a vu, les attaques de «phishing» qui sont... Ça se fait maintenant par texto. Ça se fait maintenant par téléphone. Ça se fait par courriel, bien entendu. Il y a des méthodes spécifiques.

Et on connaît également des méthodes qui ciblent des gens particulièrement. On l'a vu notamment aux États-Unis. C'est ce qu'on appelle... Au lieu du «phishing», c'est le «whaling», où est-ce qu'on va cibler des gens par exemple, qui ont un poste important, qui sont impliqués au point de vue politique, et, ça, on va cibler ces gens-là de façon spécifique pour aller chercher leurs informations et non pas l'information de n'importe qui. Ça fait que, donc...

Mme Boutin : O.K. Donc, il faut que je clique sur des liens ou les gens peuvent carrément aller dans mon téléphone puis prendre contrôle de mon téléphone?

M. Sarrazin (Claude A.) : Bien, c'est sûr que les attaques, au point de vue du «phishing», le «whaling», tout ça, il y a généralement un lien ou une action à prendre. Ce n'est pas nécessairement un lien, mais ça peut être une action à prendre, qui permettra, à ce moment-là, à la personne d'accéder aux données de différentes façons. Et il y a une multitude de moyens par lesquels ça peut se faire. Et malheureusement la réalité, c'est que l'Internet, l'Internet des choses et l'Internet de façon générale, ce qu'on en connaît, c'est un peu le far west, parce que l'aspect législatif... Et j'ai travaillé... J'ai tenté de faire faire une modification au Code criminel, il y a cinq ou six ans maintenant, justement pour répondre à cette réalité-là. On n'a pas de loi qui couvre l'ensemble des actions qui sont posées justement par ces criminels-là.

Mme Boutin : Je suis d'accord avec vous, puis, bien, mon collègue va sûrement vous en parler après. C'est pour ça aussi qu'on a déposé le projet de loi n° 64. On est très au fait que plusieurs lois ont été écrites avant l'évolution du numérique puis, bon, il faut les revoir.

Moi, j'ai une question, puis c'est un scénario. Admettons qu'on est 60 % de la population, qu'on «downloade» une application sur un Bluetooth, outre l'efficacité qui n'a pas encore été vraiment démontrée, c'est quoi, le pire scénario

qui pourrait arriver au niveau de la sécurité, qu'il faut garder en tête, toujours voir quel est le pire scénario versus les bénéfices? Admettons, je vous dis le pire scénario, est-ce qu'il pourrait y avoir une fuite de données massive? Parce qu'on parle souvent des fuites de données qu'il y a eu chez Desjardins, Revenu Québec, mais, souvent, c'était la gestion des accès qui était peut-être désuète, puis c'est des gens, tu sais, mal intentionnés qui ont volé. C'est vraiment une erreur humaine, là, des gens qui sont allés par eux-mêmes chercher des données. Mais, sur des téléphones intelligents, admettons, parce que je ne sais pas si ça s'est fait ailleurs, dans les expériences, dans les autres pays, mais qu'est-ce qu'il faut garder en tête dans le pire scénario? Est-ce que c'est une fuite de données massive ou est-ce que ce serait plutôt que ça ne fonctionne pas finalement?

M. Sarrazin (Claude A.) : Bien, je crois qu'ici je ne parlerais pas nécessairement de fuite de données massive. C'est sûr que les gens qui feraient ces attaques-là sont malveillants. Ça fait que, donc, ce qui serait le pire cas, c'est qu'on se ramasse avec 60 % de la population qui a installé un outil de protection qui s'avère être une porte d'entrée pour des attaques sur les systèmes informatiques des gens. Ça fait que, donc, ça veut dire que, la personne, si on réussit à infecter son téléphone, on pourrait réussir à également infecter les ordinateurs. On peut cumuler des données informatiques. Et, pour vous donner une idée, là...

Mme Boutin : Un par un. Dans le fond, un individu par un et non tous ensemble.

M. Sarrazin (Claude A.) : Exact, exact. Si on utilise une technologie décentralisée, ça pourrait être ça. Le pire cauchemar, ça serait ça, et, à partir de ça...

• *(9 h 20)* •

Mme Boutin : Des pirates très motivés.

M. Sarrazin (Claude A.) : Pardon?

Mme Boutin : Des pirates très motivés.

M. Sarrazin (Claude A.) : Oui, exactement, mais, généralement, ils le sont parce que c'est excessivement payant. C'est inimaginable, les sommes d'argent que ces gens-là font avec... et de la façon qu'ils achètent des outils. C'est sûr qu'il y a des vulnérabilités partout, là, parce que la problématique en devient une à très long terme. Si quelqu'un se fait voler son identité et que l'identité est valide, donc est utilisable par les fraudeurs, nous, on calcule, en moyenne, que ça a une durée de vie, cette problématique-là, de cinq à 10 ans. Et, la semaine dernière, j'ai vu un cas qui durait depuis 17 ans. Et là on parle de gens qui ont des mandats d'arrestation pour des contraventions impayées, et ces personnes-là se sont fait complètement voler leur identité.

Mme Boutin : ...à quelqu'un que je connais bien. C'est ça, on se fait voler notre numéro d'assurance sociale ou des informations. Après ça, bon, tu sais, ça impacte beaucoup dans notre vie.

J'aimerais vous amener sur un autre point, puis je sais que mes collègues vont vouloir poser des questions, là, parce que moi, j'essaie de soupeser toujours le risque, le pire risque versus le bénéfice potentiel. C'est malheureux parce qu'il n'y a pas encore d'études qui ont sorti, qui ont été publiées sur l'impact réel. Plusieurs pays sont allés de l'avant souvent en se disant : Bon, bien, en prévision d'une deuxième vague, peut-être qu'on pourrait sauver quelques vies, peut-être qu'on pourrait désengorger les systèmes de collecte d'information manuelle.

Tu sais, la réflexion se fait beaucoup dans ce sens-là, je pense, par les responsables de la Santé publique également, de dire : Comment est-ce qu'on pourrait libérer quelques... Est-ce qu'on pourrait libérer quelques ressources qui font la collecte de contacts manuellement, avec des applications comme ça, puis mettre ces ressources humaines là, qui sont limitées, pour s'occuper, donc, des populations plus vulnérables qui n'ont pas nécessairement accès à des téléphones intelligents? Ils se posent cette question-là.

Est-ce que vous pensez que, si on mettait toutes les mesures... Parce qu'il n'y a pas de décision qui a été prise, là, encore, vraiment, là, mais, si on mettait toutes les mesures de sécurité, des audits de sécurité, de la surveillance, un stockage décentralisé, sur des téléphones, de données anonymisées — j'ai de la difficulté à dire ça — est-ce que vous pensez que ça pourrait potentiellement, parce qu'il n'y a rien de prouvé, libérer un peu des ressources, faciliter le travail de la Santé publique, lors de la collecte manuelle, ou non?

M. Sarrazin (Claude A.) : Bien, écoutez, je ne suis pas un spécialiste en santé publique. Bien humblement, je vous dirais que, si on fait une analyse logique, oui, ça devrait normalement libérer l'utilisation. S'il y a suffisamment d'utilisateurs, ça pourrait libérer des ressources pour être utilisées ailleurs. C'est la logique à laquelle on pourrait penser.

Maintenant, quel fardeau ça peut représenter, puis tout dépendant de la solution qui est... Il y a beaucoup d'éléments qu'il reste à déterminer là-dedans et qui sont difficiles à évaluer. Justement, c'est un peu la difficulté que j'ai eue quand j'ai analysé le projet. Il y a beaucoup d'éléments qu'il nous manque. Il y a beaucoup d'inconnues là-dedans, et c'est ce qui m'inquiète aussi, c'est de voir jusqu'à quel point on tombe dans des nuances de gris qui peuvent être problématiques. Est-ce que ça va être plus avantageux d'avoir cette ressource-là? Peut-être, malgré le risque. Est-ce que ça va être... Est-ce que ça ne sera pas efficace? C'est possible aussi. Puis est-ce que ça va nous aider? C'est également possible. À ce stade-ci, c'est difficile à dire.

Mme Boutin : Bien, je pense que tout le monde est d'accord. Puis c'est pour ça qu'on prend le temps de consulter, pour prendre une décision relativement éclairée. Malgré tout, tout n'est pas blanc ou noir.

Puis là ma dernière question, puis certains n'aimeront peut-être pas mon raisonnement, mais, tu sais, quand on soupèse le risque, le plus grand risque est peut-être d'avoir une augmentation du piratage, peut-être une efficacité qui forcerait le gouvernement à retirer l'application, donc, à, tu sais, admettre que, finalement, ça ne fonctionnait pas comme certains pays, versus un bénéfice potentiel qui n'est pas encore démontré, mais qui existe peut-être, de libérer certaines ressources pour éventuellement contribuer à contrer la pandémie.

Et, ultimement, l'objectif, c'est de sauver des vies humaines puis c'est de... Soupeser, là, tu sais, les risques, la valeur des risques versus la valeur des bénéfices, c'est une question qui est difficile à se poser, parce qu'on a, comme vous avez dit, des inconnues par rapport à ça. Mais vous, vous iriez quand même dire que les risques d'efficacité, c'est plus important qu'un bénéfice potentiel de sauver des vies?

M. Sarrazin (Claude A.) : Encore une fois, comme je vous dis, c'est le risque à long terme. Comme je vous disais tout à l'heure, le vol d'identité, là, ça a une durée de vie, là, de cinq à 10 ans. Ça fait que, donc, si les informations personnelles de ces gens-là sont dérobées et qu'ils se retrouvent dans des problématiques qui vont durer potentiellement, et ça non plus, on ne le sait pas, beaucoup plus longtemps que la durée du COVID, bien, il faut vraiment analyser cette perspective-là. Est-ce que c'est un outil qui est utile? Je pense que oui. S'il est bien fait et s'il protège l'information personnelle, c'est sûr que ça peut être intéressant. Et, sur papier, ça peut être miraculeux comme solution. Est-ce que ça va livrer ça en bout de ligne? Je ne suis pas certain.

Mme Boutin : Bien, merci.

Le Président (M. Bachand) : Merci beaucoup. M. le député de Chapleau, s'il vous plaît.

M. Lévesque (Chapleau) : Merci, M. le Président. Merci, M. Sarrazin. C'est un peu là-dessus que je voulais vous amener. D'ailleurs, on parle... Bien, vous parlez souvent, donc, de failles de sécurité, de vulnérabilité en lien avec certaines applications. Dans le fond, auriez-vous peut-être des pistes de solution, des améliorations qu'il faudrait mettre de l'avant sur ces applications-là? Si jamais le gouvernement décidait d'aller de l'avant, quelles étapes il y aurait et qu'est-ce que ce serait, les points à avoir de façon prioritaire?

M. Sarrazin (Claude A.) : Bien, c'est une très bonne question. Encore une fois, sans savoir les détails de ce qui a été mis en place en matière de sécurité, c'est un peu difficile... mais, toutefois, c'est sûr que la première condition, c'est que ça prend une capacité d'analyse presque en temps réel. Et ça, c'est un couteau à deux tranchants, parce que ça demanderait une centralisation au moins d'une partie des données pour permettre de répondre à d'éventuelles tentatives d'attaque, parce que c'est sûr que, s'il y a des attaques, les cybercriminels ne font pas ça d'un trait.

Généralement, ils y vont graduellement. Il y a des expériences, eux aussi, qu'ils font de leur côté pour prendre connaissance et apprendre l'utilisation de ces systèmes-là. Ça fait que ça, ça demande énormément de capacité de détection. Si on n'a pas de centralisation, c'est un peu difficile à faire. Ça fait que... Et, si on centralise, on sait qu'on se rend plus vulnérables. Ça fait que, donc, il y a un certain bémol à apporter à ce niveau-là.

Ceci étant dit, si on est capables de sécuriser l'application, si on est capables de trouver une façon de faire pour obtenir un niveau de sécurité qui permettrait d'avoir une certaine sûreté par rapport à ça, bien là, à partir de ce moment-là, O.K., là, on pourrait penser à aller de l'avant. Mais il faut absolument qu'on continue la surveillance de notre système pour permettre la détection des tentatives d'intrusion dans ces systèmes-là pour protéger le citoyen, parce que, trop souvent, on met en place des, et je ne parle pas nécessairement du gouvernement, mais de l'entreprise et de l'ensemble de l'oeuvre, là, de tous les utilisateurs, solutions, puis, vous l'avez tous vu, vous l'avez tous vécu, il y a un fournisseur qui met en place une solution, l'offre à tout le monde, c'est un miracle, et là, tout d'un coup, la solution, on se rend compte qu'il y a des vulnérabilités importantes quelques mois plus tard.

M. Lévesque (Chapleau) : Rapidement, là, on a entendu la solution des pirates informatiques à bonnet blanc, les fameux «white cap», «white hat hackers», est-ce que ça, ça pourrait être une option à envisager pour, dans le fond, améliorer ce type d'application là?

M. Sarrazin (Claude A.) : Oui, ça peut être une façon de faire. Il y en a plusieurs. Oui, l'utilisation des «white hat», ça peut être intéressant, mais non seulement les «white hat». Mais il y a des universités au Québec qui font de la recherche en matière de cybersécurité, l'Université de Montréal, l'UQAM. Ça peut être intéressant de les joindre, justement, à ce processus-là.

Maintenant, la réalité, c'est que, malgré tout ce travail-là... Et il y a des gens brillants qui travaillent chez Bluetooth. Il y a des gens brillants qui travaillent chez Apple. Il n'y a aucun doute là-dessus. Malgré ça, il y a une multitude de gens qui travaillent à défaire ce qu'ils font. Ça fait que, donc, il faut continuer la surveillance en temps réel. Il faut être proactif pour pouvoir détecter et réprimer les tentatives d'accession aux données des utilisateurs.

• *(9 h 30)* •

Le Président (M. Bachand) : Merci beaucoup. Alors, Mme la députée de Saint-Laurent, s'il vous plaît.

M. Lévesque (Chapleau) : Ah! merci, excusez-moi.

Le Président (M. Bachand) : Pardon, désolé, M. le député de Chapleau. Mme la députée, s'il vous plaît.

Mme Rizqy : Merci, M. le Président. Bonjour, M. Sarrazin. Bienvenue parmi nous. Dites-moi, au XXIe siècle, là, est-ce qu'il y a une donnée, un renseignement personnel qui ne vaut absolument rien ou est-ce qu'il y a toujours une valeur rattachée à chacune des données personnelles des gens?

M. Sarrazin (Claude A.) : Écoutez, il y a une valeur d'attachée à ça. Maintenant, la valeur n'est pas nécessairement celle qu'on pense. Et ce qu'il faut voir, c'est qu'en matière de cybercrime, souvent, ces gens-là vont être très créatifs sur la façon qu'ils peuvent utiliser ces données-là. Ça fait que, donc... Et on va voir... Il y a une multitude de types de crimes, qui sont vraiment ahurissants, sur la façon qu'ils vont développer justement... Comme je le disais, la grosse différence, puis le meilleur exemple, c'est que, traditionnellement, un voleur, il identifiait une banque, puis là il trouvait la façon par laquelle il était pour aller voler la banque. Il savait à quoi il s'attaquait.

Ici, on n'a pas la même... on n'a pas cette même façon de faire là. Ils vont innover. Ils sont très créatifs. Et, à partir du moment qu'ils voient apparaître une porte, en quelque part, ou une opportunité, ils vont, par la suite, trouver une façon d'utiliser cette information-là. Ça fait que j'ai vu des bases de données vendues pour 0,10 $ le nom comme j'ai vu des bases de données vendues pour des milliers de dollars par identifiant. Ça dépend d'une multitude de facteurs.

Mme Rizqy : Donc, à peu près tous les renseignements personnels peuvent avoir une valeur, que ce soit de 0,10 $ par nom jusqu'à... Par exemple, le numéro d'assurance sociale a une plus grande valeur, j'imagine. Dites-moi, vous avez plusieurs années d'expérience, des décennies d'expérience. Alors, à ce jour, lorsqu'il y a une fuite de données, c'est quoi, au niveau criminel... Je ne veux pas cibler d'entreprises. Je pense que, dans les dernières, il y en a eu qui ont eu leur lot, mais c'est quoi, au niveau criminel, aujourd'hui, là, pour une entreprise qui n'est pas capable... Prenons un géant tech qui a une fuite de données. Qu'est-ce qui arrive pour cette entreprise au Québec puis au Canada?

M. Sarrazin (Claude A.) : Bien, je vous dirais que la grosse problématique, c'est que ça dépend où le crime est commis, parce que les crimes virtuels ne sont pas nécessairement tous commis sur le territoire du Québec ou du Canada. Ça fait que, donc, ce qu'on va avoir et ce qu'on voit maintenant beaucoup plus comme problématique, c'est que les victimes sont ici, le criminel est à l'étranger, en quelque part, et là on doit définir où le crime a été commis, et le stockage des données n'est pas nécessairement local non plus. Les transactions qui ont été faites ou, en tout cas, toutes les différentes possibilités en matière de crime, ça peut avoir été commis n'importe où.

Et maintenant on va aller plus loin que ça. On peut se poser la question si, même dans ce pays-là où se trouve le cybercriminel, si ce qu'il a fait représente un crime, parce que, dans certains pays, il y a certains types de crimes qui n'existent pas. Ça fait que, donc, à partir de ce moment-là, on ouvre... Ça devient des situations excessivement complexes. On réussit à collaborer entre pays, mais, parfois, pour toutes sortes de raisons, il y en a un qui n'embarquera pas.

On l'a vu, dans le cas de l'Europe, dans le cas d'EncroChat, EncroChat qui était une méthode de communication que les criminels utilisaient, les criminels, les terroristes utilisaient. Pendant plusieurs années, ils ont utilisé cette méthode de communication là, encryptée, qui était totalement sécuritaire, jusqu'à tant qu'elle ne le soit plus, soit dit en passant. Et donc les policiers, pendant deux ans, ont réussi à intercepter les communications de ces gens-là en temps réel et d'avoir les communications entre criminels. Ça fait que, donc... Mais ça, ça a demandé une collaboration entre plusieurs pays qui ont collaboré pour pouvoir étendre leurs recherches et leurs analyses et ça a mené à des milliers et des milliers d'arrestations, là.

Mme Rizqy : ...dans cet autre pays, mais pas ici?

M. Sarrazin (Claude A.) : Mais pas ici, exactement, exactement, malgré le fait qu'EncroChat était au Canada aussi, soit dit en passant.

Mme Rizqy : Oui, mais eux... Ça n'a pas mené à d'arrestations ici, pas de condamnations ici et pas de pénalités non plus ici. Et le commissaire à la vie privée... Vous êtes bien au courant et au fait que ça fait quand même plusieurs années que le commissaire à la vie privée, au fédéral, se bat dans l'eau bénite pour avoir des lois avec du mordant, c'est-à-dire un vrai bâton pour courir. Ne trouvez-vous pas qu'on ne devrait pas mettre la charrue devant les boeufs puis plutôt avoir des lois avec plus de mordant? Parce qu'on a eu, hier, l'occasion d'entendre la Commission d'accès à l'information, donc, au niveau du Québec, qui, eux, nous réclament d'abord et avant tout un cadre juridique robuste. Est-ce que vous devriez... Pensez-vous qu'on devrait attendre, au Québec, d'abord, d'avoir cette vraie discussion sur un cadre juridique robuste avant d'aller de l'avant avec ce type de technologie qui... Même pour le secteur privé, là, en ce moment, eux autres aussi développent leurs propres technologies de traçage.

M. Sarrazin (Claude A.) : Oui, tout à fait. Bien, écoutez, c'est sûr qu'il y a un cadre juridique qui est existant. Il n'est pas... Au Québec, ça nous permet de faire un bout de chemin. Moi, je travaille plus au niveau du Code criminel. Donc, au point de vue du Code criminel, on est limités, quand même. Ça fait que, donc, justement, le p.l. n° 210, sur lequel j'avais travaillé, modifications au Code criminel, était justement pour établir le lieu où se commet une infraction. Ça fait que, donc, ça nous permettait un champ beaucoup plus large pour pouvoir accuser des gens ici, au Canada, en vertu du Code criminel, même si, physiquement, ils n'étaient pas là, un petit peu sur le modèle suisse.

Maintenant, oui, effectivement, ça prend des lois, mais ça prend des lois... Et là il faudrait le regarder dans un contexte peut-être autre que celui du COVID, mais ça nous prend des lois, des règlements en place pour pouvoir contrôler un peu ce qui se passe au point de vue du Web. Il faut toujours faire attention entre l'information et l'utilisation légitime de l'information. Il y a parfois des moments où est-ce qu'il peut y avoir une intrusion dans la vie privée des gens, pour toutes sortes de raisons, mais c'est l'utilisation illégale ou interdite dans le cadre de la commission d'un acte qui devient importante.

Ça fait que, donc, c'est vraiment là qu'il faut se pencher, pas juste sur la protection de la vie privée comme telle. Oui, effectivement, je suis entièrement d'accord, et ça peut paraître drôle venant d'un enquêteur, où est-ce que, quotidiennement, nous, on porte atteinte à la vie privée des gens, mais on est enchâssés par des règles qui ont été établies, des jugements de la Cour suprême notamment, qui viennent nous dire que, oui, vous avez droit à une vie privée. Toutefois, à partir du moment... selon les actes que vous commettez, bien, cette vie privée là peut être réduite en fonction de la nature des actes que vous avez commis. Et c'est juste à ça qu'il faut faire attention, là. Ça fait que, oui, effectivement, ça nécessite une loi. Allez-y, excusez-moi.

Mme Rizqy : Non, mais c'est parfait... parce que je sais que, des fois, le temps file...

Alors, si on revient à la technologie, la quasi-totalité des experts que nous avons entendus jusqu'à ce jour nous disent que l'application Alerte COVID lancée par le fédéral, ce n'est pas très efficace. Ils ont regardé ce qui se passe ailleurs dans le monde, que ce soit l'Islande, l'Australie, Singapour, Angleterre, la France, et plusieurs de ces pays ont même finalement mis ça au rancart. Et ils ont aussi mentionné que cette technologie n'était pas... En fait, le risque était beaucoup plus grand. Hier, même Steve Waterhouse nous mentionnait qu'on serait, en fait, exposés 24 heures par jour avec le... pour avoir le Bluetooth allumé pour que ça soit efficace.

Et là je sais que vous n'êtes pas un expert de santé publique, mais vous me semblez une personne qui fait preuve de gros bon sens. Lorsqu'on a d'autres exemples mondiaux qui ont déjà essayé cette technologie et qui sont arrivés, là, avec même à Singapour... avec plus de 1 million de personnes qui l'ont utilisé, puis, finalement, ça n'a pas marché, trouvez-vous qu'on devrait peut-être attendre voir ce qui se passe ailleurs dans le monde puis se dire : Bien, si ça n'a pas marché chez eux, peut-être que ça ne marchera pas plus chez nous?

M. Sarrazin (Claude A.) : Potentiellement. Et d'ailleurs, dans mon mémoire, ma conclusion personnelle n'est pas différente de celle de M. Waterhouse.

Mme Rizqy : ...pour les fins... Pour ceux qui n'ont peut-être pas suivi hier, c'était l'option c, qui était de ne pas aller de l'avant avec ce type d'application, et d'investir davantage dans un réseau de santé publique robuste, et de s'assurer de continuer à faire le testage que, présentement, la santé publique fait, c'est-à-dire manuel, on appelle les gens, ou même au niveau... par courriel. C'est bien ça, votre position?

M. Sarrazin (Claude A.) : Oui, sensiblement, c'est la conclusion à laquelle j'arrive aussi. Au point de vue du traçage, le traçage est quand même efficace. Si on avait une solution miracle qui serait excessivement sécuritaire, ça serait fantastique, mais ce n'est pas le cas. Ça n'existe pas, malheureusement, que sur papier.

• *(9 h 40)* •

Mme Rizqy : Merci beaucoup.

Le Président (M. Bachand) : Merci beaucoup. M. le député de Gouin, s'il vous plaît.

M. Nadeau-Dubois : Merci, M. le Président. Bonjour, M. Sarrazin. Merci de prendre du temps avec nous cet avant-midi. J'ai peu de temps. Je vais être direct. Est-ce que vous diriez que le risque d'attaque ou de piratage d'une application qui fonctionne par Bluetooth... est-ce que vous qualifieriez ce risque-là de réel?

M. Sarrazin (Claude A.) : Oui.

M. Nadeau-Dubois : Vous diriez qu'il est significatif?

M. Sarrazin (Claude A.) : Absolument.

M. Nadeau-Dubois : Est-ce que vous diriez que les bénéfices liés à l'utilisation d'une telle application sont assurés? Est-ce que l'efficacité de la...

M. Sarrazin (Claude A.) : Je ne peux pas me prononcer.

M. Nadeau-Dubois : Pardon, je... Peut-être plus pour être dans votre champ d'expertise, est-ce que vous diriez que, d'un point de vue technologique, ces applications-là, leur efficacité est démontrée?

M. Sarrazin (Claude A.) : De ce que j'ai pu lire ou de ce que j'ai pu consulter comme analyse jusqu'à date, il semblerait que non.

M. Nadeau-Dubois : Parfait. Donc, vous nous dites : Il y a des risques réels... En fait, non, vous dites : Des risques significatifs qu'il y ait piratage ou attaque. Et, de l'autre côté, vous nous dites : Les bénéfices, eux, ne sont... en fait, l'efficacité de tels outils, elle n'est pas démontrée. Si jamais il y avait piratage ou attaque, fuite de données, qui serait imputable, responsable de cette faille de sécurité? Vers qui les gens pourraient-ils se tourner?

M. Sarrazin (Claude A.) : Écoutez, ça dépend c'est qui qui promulgue et c'est qui qui fournit le service.

M. Nadeau-Dubois : Donc, ce n'est pas clair, à ce stade-ci, qui, exactement, serait responsable.

M. Sarrazin (Claude A.) : Tout dépendant de la solution choisie par le gouvernement, mais, à partir de ce moment-là, on pourra définir qui est responsable, ultimement.

M. Nadeau-Dubois : Dans le cas de l'application Alerte COVID, qu'on peut penser qui fait partie des choix du gouvernement du Québec, qui serait responsable?

M. Sarrazin (Claude A.) : Le gouvernement du Canada.

M. Nadeau-Dubois : Le gouvernement du Canada. Parfait. Si le Québec modifiait cette application un peu, est-ce que ça rendrait le gouvernement du Québec responsable?

M. Sarrazin (Claude A.) : Potentiellement. Il faut voir la nature de l'attaque. Ça peut être le fournisseur des logiciels qui sont utilisés ou des technologies qui sont utilisées également. Ça peut être une responsabilité partagée. Disons-le comme ça. On ajoute des joueurs.

M. Nadeau-Dubois : Vous avez fait une revue extensive de littérature. Dans la revue de littérature que vous avez faite, quelle est la proportion d'experts dans votre champ d'études, dans votre champ d'expertise qui juge que ces applications-là sont efficaces, sécuritaires, et qu'on devrait aller de l'avant?

M. Sarrazin (Claude A.) : Ce n'est pas énorme. Je ne pourrais pas vous sortir un chiffre.

M. Nadeau-Dubois : C'est minoritaire?

M. Sarrazin (Claude A.) : Pardon?

M. Nadeau-Dubois : Est-ce que vous diriez que c'est minoritaire?

M. Sarrazin (Claude A.) : Oui.

M. Nadeau-Dubois : C'est minoritaire. Donc, l'opinion majoritaire dans votre champ d'expertise est que le jeu n'en vaut pas la chandelle.

M. Sarrazin (Claude A.) : C'est qu'il n'y a pas de solution qui est suffisamment sécuritaire, à ce stade-ci, pour pouvoir répondre au besoin.

M. Nadeau-Dubois : Merci beaucoup, monsieur.

Le Président (M. Bachand) : Merci. M. le député de René-Lévesque, s'il vous plaît.

M. Ouellet : Bonjour. Merci à vous, M. Sarrazin, de prendre du temps ce matin avec votre expertise pour nous éclairer.

Je vais revenir sur des passages clés de votre mémoire. Vous avez dit, dans votre mémoire, après que vous avez consulté la littérature, qu'il n'existait aucune étude empirique sur l'efficacité de ces technologies Bluetooth quant à la capacité de traçabilité adéquate des cas. C'est bien ça?

M. Sarrazin (Claude A.) : Oui, exact.

M. Ouellet : Vous avez aussi, dans votre mémoire, dénoté d'importantes vulnérabilités sur la technologie Bluetooth. Vous avez fait état de vulnérabilités, par le passé, qui ont été réglées, mais vous indiquez aussi qu'il y aurait une vulnérabilité potentielle qu'on ne connaît pas, qui pourrait exister dans le futur.

M. Sarrazin (Claude A.) : Oui, exact.

M. Ouellet : Vous soulignez, dans votre mémoire, l'importance de ne pas prioriser la rapidité du lancement plutôt que la sécurité.

M. Sarrazin (Claude A.) : Tout à fait.

M. Ouellet : Donc, la prémisse de base à votre réflexion, c'est que, si on veut que ça fonctionne, il faut que ça repose sur la confiance.

M. Sarrazin (Claude A.) : Oui.

M. Ouellet : Donc, si aucune étude ne nous dit que c'est bon pour tracer les gens et obtenir des cas véridiques, donc ça a un impact sur la lutte à la pandémie. Si, deux, vous nous dites que, cette technologie, elle n'est pas fiable, mais surtout elle est vulnérable, comment peut-on donner confiance aux citoyens, aux citoyennes du Québec pour dire : Go, allez de l'avant, avec cette application, vous allez faire partie d'une chaîne humaine qui va nous permettre de se protéger devant cette pandémie?

M. Sarrazin (Claude A.) : C'est un gros contrat de vente. Et, là encore, on me sort de mon champ d'expertise. Mon objectif, moi, aujourd'hui, c'était de présenter la réalité telle que moi, je la perçois, et tel que j'ai pu analyser les résultats de différentes recherches qui ont été effectuées, et par rapport à ce que je connais du terrain, par rapport à ce que je connais de la part des cybercriminels.

Maintenant, le fait de donner confiance nécessite que ça ne soit pas quelque chose qui est intangible. Il faut que les gens aient confiance. Pour que les gens aient confiance, il faut que la sécurité de ces outils-là soit démontrée clairement et non pas une promesse faite dans le vide, finalement. Ça fait que, donc, c'est un élément essentiel. Et tout outil informatique qui est sorti rapidement, en utilisant des technologies déjà connues, reste un outil qui est vulnérable, et c'est mon inquiétude principale.

Le Président (M. Bachand) : Merci beaucoup. M. le député de Chomedey, s'il vous plaît.

M. Ouellette : M. Sarrazin, bonjour.

M. Sarrazin (Claude A.) : Bonjour, M. Ouellette.

M. Ouellette : Ça va bien?

M. Sarrazin (Claude A.) : Ça va très bien. Vous-même?

M. Ouellette : Bien oui. C'est très intéressant, ce que vous nous apportez comme réflexion ce matin. J'entends de la part du gouvernement que, dans le fond, ils n'ont rien à perdre. Si ça marche, ça marche. Si ça ne marche pas, bon, on l'enlèvera. Je pense qu'on doit pousser la réflexion un petit peu plus loin que ça, et le degré d'imputabilité est, je pense, majeur.

Vous avez parlé de confiance. Puis je sens, dans vos propos ce matin, que, si le gouvernement décidait quand même d'aller de l'avant, avant d'aller de l'avant, il faudrait que des experts comme vous, M. Waterhouse et d'autres, soyez consultés et soyez mis à contribution pour qu'on assure les citoyens du Québec, là, qu'on ne les met pas à risque. À moins que je sois complètement à côté de la track, là, c'est ce que j'ai senti dans vos propos.

M. Sarrazin (Claude A.) : Écoutez, que ça soit moi ou que ça soit n'importe qui, je le mentionnais tout à l'heure, il y a plusieurs chaires d'études en matière de cybersécurité au Québec qui existent. Ces gens-là pourraient travailler activement à tester ce genre de solution là, mais la portion... Et c'est toujours la problématique.

Il y a quelques années, il y a un gouvernement local, ici, au Québec, qui a sorti une solution technologique. J'avais participé à certaines discussions concernant ce projet-là. Et ce qu'on avait présenté aux élus à ce moment-là, c'était que la solution technologique serait sécuritaire pendant au moins cinq à 10 ans, ça fait que, donc, que ça serait... C'était une solution qui était inviolable. Nous, on a continué nos recherches et nos analyses. Deux semaines avant la mise en place de cette technologie-là, on savait déjà que les hackeurs avaient en main et vendaient les outils pour pouvoir hacker le système qui, je vous rappelle, était supposé être jugé inviolable pendant cinq à 10 ans. Ça fait que, donc, avant même sa mise en application, la vulnérabilité avait déjà été exploitée, et c'est ce qui m'inquiète dans cette situation-ci. Ça fait que, donc, votre analyse de mes propos est exacte.

M. Ouellette : Donc, effectivement, pour... Quand on parle... Quand on regarde la balance des inconvénients, présentement, là, il y a trop de zones grises. Et, un peu comme vous, vous n'avez pas toutes les données, on ne les a pas. On n'a même pas les données de la consultation en ligne même si on les a demandées. Je pense qu'on est à la même place. Merci de vos commentaires. C'est éclairant pour les membres de la commission.

Le Président (M. Bachand) : Merci, M. le député. Et à mon tour de vous remercier, M. Sarrazin, de votre participation à la commission. Ça a été fort intéressant, et puis on vous souhaite un super vendredi. Merci beaucoup et à bientôt.

M. Sarrazin (Claude A.) : Merci.

Le Président (M. Bachand) : Et je suspends les travaux quelques instants.

(Suspension de la séance à 9 h 49)

(Reprise à 9 h 52)

Le Président (M. Bachand) : À l'ordre, s'il vous plaît! Merci. La commission reprend ses travaux. Alors, nous souhaitons la bienvenue à M. Stéphane Roche, professeur titulaire de sciences géomatiques de l'Université Laval.

Alors, comme vous savez, vous avez 10 minutes de présentation, après ça, un échange avec les membres de la commission. Alors, encore une fois, bienvenue et la parole est à vous.

M. Stéphane Roche

M. Roche (Stéphane) : Merci beaucoup. Mmes et MM. les députés, merci. Merci pour l'invitation. Merci pour l'organisation de cette consultation et de ces auditions qu'on était un certain nombre à appeler de nos voeux depuis un certain nombre de semaines, voire de mois. Je ne vais pas être très long parce que je vais essentiellement redire les trois choses qui me semblent être les plus importantes au regard des questions qu'on se pose ici.

La première, c'est qu'il y a une seule étude, pour l'instant, hein, qui a été réalisée de façon sérieuse et qui montre un peu quelles seraient les conditions dans lesquelles ce type d'application pourrait avoir des effets positifs. C'est une étude qui a été publiée au courant du mois d'avril, dans la revue Science, par une équipe de l'Université d'Oxford, vous devez la connaître, et qui dit, grosso modo, que ça peut être efficace à certaines conditions, sinon il y a des risques de faux positifs et faux négatifs très nombreux... à condition que 60 % à 70 %, vous le savez, de la population adopte ce genre de technologie, ce qui pose, au Québec, et au Canada en général, un problème, parce qu'on sait que c'est à peu près ce pourcentage-là de la population qui possède un téléphone cellulaire. Donc, il faudrait que la totalité des gens qui utilisent un téléphone cellulaire acceptent d'utiliser l'application.

Le deuxième, c'est qu'il faudrait que des tests, de façon massive, soient faits de façon beaucoup plus importante qu'ils ne le sont faits aujourd'hui, de façon, évidemment, à ce que les cas puissent apparaître et rentrer dans la chaîne de contacts. Il faudrait que les recommandations... que les notifications ne ciblent que les personnes qui sont vraiment concernées pour éviter d'alerter une part importante de la population sans raison. Il faudrait que, dans les chaînes de contacts, les gens utilisent évidemment... enfin, non seulement téléchargent cette application, mais l'utilisent de façon... jouent le jeu, je dirais, de façon très active en s'engageant. Et, dans ces conditions-là, et pour peu que les verrous technologiques, et je vais y revenir rapidement, soient levés, alors, éventuellement, ce genre d'application pourrait constituer non pas la solution, mais une solution parmi un ensemble, une boîte à outils que l'on pourrait utiliser, et dont certains outils sont déjà utilisés.

Donc, pour moi, ça soulève deux enjeux qui sont en lien avec mon expertise. Le premier, c'est celui de... Comment est-ce qu'on qualifie un contact de façon pertinente? Comment on est capables d'identifier le contact qui va être virosensible de celui qui ne l'est pas? Et aujourd'hui les applications qui fonctionnent sur la base du protocole Bluetooth, qui est une onde radio en réalité, n'ont pas la capacité à déterminer précisément si un contact vaut la peine d'être notifié ou s'il ne vaut pas la peine d'être notifié.

Pour ça, il faudrait que le contexte dans lequel le contact a été... s'est produit soit évalué et quelle est la distance réelle — ça, le Bluetooth n'est pas capable de le faire — dans quel contact, y avait-il un masque, y a-t-il une visière de protection, combien de temps a duré le contact, etc. Et, ça, il n'y a aucune application basée sur le protocole Bluetooth. Et, si on écoute même, d'ailleurs, les deux créateurs de ce protocole-là, ils sont assez clairs en disant qu'ils ne voient pas comment leur... cette onde radio pourrait renvoyer un signal suffisamment précis.

Donc, ça ne veut pas dire qu'il n'y a pas d'utilité possible, mais ça veut dire qu'une application comme celle que le Canada a choisie, par exemple, à mon avis, ne sera pas utile. Ça ne sera pas utile même si elle était utilisée par 70 % de la population, ce qui semble assez improbable. Et puis toutes les autres applications qui ont été développées sur ce modèle-là dans le monde ont montré... Il n'y a aucune preuve probante que ça ait fonctionné nulle part ailleurs.

Ça ne veut pas dire que je suis contre ce genre d'application. Ça veut dire que, si on veut que ce genre d'application soit utile, il va falloir rajouter des fonctionnalités.Il va falloir les rendre, donc, beaucoup plus intrusives. Il va falloir faire en sorte qu'on mixe beaucoup plus de données. Il va falloir éventuellement utiliser la géolocalisation. Il va falloir utiliser, pourquoi pas, l'intelligence artificielle. Mais là on rentre dans un autre type d'application qui nécessite beaucoup plus de précautions. Et, si jamais le Québec allait dans cette direction-là, alors il faudrait, à mon avis, deux choses.

La première, c'est que ça se fasse main dans la main avec les utilisateurs. Et on a les moyens de le faire. Je l'ai écrit dans mon rapport. On a les moyens de le faire, parce qu'il y a beaucoup d'expériences qui sont menées dans d'autres domaines, dans le domaine des sciences citoyennes, des initiatives qui permettent d'engager les utilisateurs comme producteurs actifs. Et là on pourrait imaginer que les utilisateurs soient engagés dans une vraie stratégie pour produire des traces, qu'ils soient conscients de ce qu'ils fassent, qu'ils le fassent de manière explicite, et qu'on les accompagne pour le faire. Et, pour ça, ça veut dire que le Québec doit s'engager lui aussi avec un certain nombre de garanties qui doivent être données à ces utilisateurs-là.

Évidemment, personne ne peut garantir l'anonymisation complète des données si jamais on mixe un certain nombre de données, personne. Il n'y a aucune garantie. Vous avez eu des spécialistes comme... le premier jour, je crois, sur les enjeux de l'intelligence artificielle ou les enjeux tout simplement d'analyse de données. Personne ne peut garantir l'anonymisation complète des données, surtout quand on utilise la géolocalisation, qui est un des meilleurs moyens pour rematérialiser des données qui ont été dématérialisées.

Mais il reste que des engagements peuvent être pris. Tu sais, des engagements peuvent être pris, comme dans beaucoup d'autres domaines, et, en particulier, il y a un engagement qui me semble essentiel, c'est celui de l'obsolescence programmée de ce genre d'application et de la destruction des données une fois qu'on serait sortis de cette période de pandémie. Il n'y a pas eu à peu près aucun exemple jusqu'à présent de technologies qui ont été déployées pour répondre à des crises et qu'on n'a pas vues perdurer au-delà de la crise. Moi, c'est ma préoccupation principale.

Alors, je vais terminer là-dessus. Oui, pour des applications de traçage. Inutile, à mon avis, si elles sont ne sont basées que sur le Bluetooth. Donc, nécessité d'intégrer d'autres technologies, mais là grand risque, et donc engagement

nécessaire non seulement de la population, pour qu'elle soit consciente de ce qu'elle va faire et de ce qu'on attend d'elle... et engagement de l'État pour garantir que ces technologies, ces données ne seront pas utilisées à d'autres fins et mettre tout en oeuvre pour protéger au mieux l'anonymisation et l'anonymat des utilisateurs. Merci beaucoup.

Le Président (M. Bachand) : Merci beaucoup pour votre présentation. Alors, période d'échange maintenant avec la députée de Les Plaines, s'il vous plaît.

Mme Lecours (Les Plaines) : Merci beaucoup, M. le Président. Merci, M. Roche, de votre présence aujourd'hui. Merci d'avoir pris le temps de regarder l'ensemble du défi, hein? Moi, j'aime mieux dire «défi» que «problématique», parce qu'effectivement il n'y a aucune solution parfaite. On l'a vu en cours de route. La grande majorité des experts ont parlé de la technologie Bluetooth. Vous l'expliquez très bien aussi.

Par contre, c'est la technologie qui, à l'heure actuelle, est la moins intrusive. Il n'y a pas... Comme on l'a dit, ce n'est pas parfait, mais c'est celle qui pourrait s'apparenter à la moins intrusive actuellement. Vous parlez d'une nécessité d'un taux d'adoption de 60 % à... Vous avez dit 60 %, il me semble. Actuellement, il n'y a pas... On a tenté... On a posé la question à plusieurs personnes qui n'ont pas pu l'évaluer à ce point. Vous le dites, vous vous basez sur...

• *(10 heures)* •

M. Roche (Stéphane) : Je me base sur la seule étude qui a été publiée dans la revue *Science* par une équipe de l'Université d'Oxford, une équipe pluridisciplinaire d'informaticiens, de spécialistes d'analyse de données, d'épidémiologistes. Elle a été publiée quelque part en avril, et eux annoncent ce chiffre-là. Je sais qu'il est très discuté, et puis il est certainement discutable, parce que c'est une étude, mais c'est la seule dont on dispose aujourd'hui. Il est assez clair que... Tu sais, je ne veux pas m'avancer dans des chiffres parce que je ne peux pas dire autre chose que ça, mais je ne vois pas comment on pourrait obtenir des résultats probants avec un taux d'adoption qui ne serait pas un taux d'adoption majeur.

Après, le risque, à mon avis, et puis ça, c'est un autre risque qu'on n'a pas évoqué, c'est celui de l'exclusion, les enjeux d'inclusion sociale. C'est-à-dire qu'on risque de tracer, éventuellement, et d'avoir des résultats assez intéressants pour certaines catégories socioprofessionnelles, certaines catégories de population, certaines zones... D'ailleurs, on peut déjà les déterminer, à mon avis, hein, sur le plan géographique, là, mais certaines zones dans lesquelles l'adoption va être peut-être très importante et d'autres dans lesquelles on va avoir des déserts de données, ce qui... Ça existe déjà, les déserts de données. Donc, ça, c'est une autre préoccupation, c'est qu'on risque de protéger certaines catégories, certaines zones au détriment des autres, dans lesquelles il faudra, à ce moment-là, développer des stratégies autres que celle-là.

Mme Lecours (Les Plaines) : C'est ce qu'on appelle la fracture numérique.

M. Roche (Stéphane) : Oui, oui, absolument.

Mme Lecours (Les Plaines) : Là-dessus, en fait, on est pleinement conscients. Après tous les questionnements qu'on a eus et les réponses qu'on a eues, on est pleinement conscients qu'évidemment ce n'est pas tout le monde qui est doté d'un appareil numérique intelligent, et ce n'est pas tout le monde non plus qui utiliserait l'application.

Par ailleurs, si moi, j'utilise l'application et que j'ai une notification, c'est sûr que je vais faire attention. Je prends mon exemple à moi, mais c'est l'exemple de bien des gens. Je fréquente des gens âgés de par ma mère. Donc, c'est sûr qu'en ayant ça je peux décider, un, d'aller me faire tester ou je peux décider de me retirer aussi pendant deux semaines, le temps de voir si, les symptômes, je les ai vraiment, etc., bon.

Donc, c'est aussi... Puis je vous pose la question. Est-ce que vous considérez que c'est aussi... ce pourrait être également utile, dans un cas comme ça, même si les gens âgés que je fréquente, eux, n'en ont pas, là? On parle de ça ou des milieux moins bien nantis qui n'en ont pas aussi. Est-ce que ça pourrait quand même être utile? Parce que vous dites que ce n'est pas que c'est complètement inutile, donc, dans un cas comme ça.

M. Roche (Stéphane) : Oui. Je veux dire, tout ce qui peut nous donner éventuellement... Tout ce qui peut apporter un complément d'information sur la situation dans laquelle on se trouve est utile. Mais, après, ce qu'il faut comprendre, c'est que c'est l'espèce de balance, là, le prix à payer pour le résultat obtenu. Puis, tu sais, même avec le Bluetooth, là, qui est peu intrusif, peu invasif, tu sais, on pourrait discuter longtemps du type, comment dire, d'application ou du type de traçage que ça va mettre en place et que ça risque de laisser, ce type d'usage, ce type de technologie dont on sait qu'il y en a déjà beaucoup, des technologies très intrusives et qui collectent nos données. Donc, ce n'est, de toute façon, pas neutre complètement.

Donc, moi, ce que j'essaie de comprendre, c'est, comment dire, tu sais, la balance entre les deux. Est-ce que ça vaut la peine, alors que moi, je continue à être très sceptique sur la qualité de l'information et de la notification qui va vous être envoyée? Parce que peut-être... mais personne ne peut garantir que cette notification, elle sera pertinente. Peut-être que ça va être une notification qui va vous effrayer pour rien. Peut-être qu'elle va vous alerter pour rien. Il y a de grandes chances que ce soit un faux positif, puis on n'a pas les moyens de le mesurer. Est-ce qu'on est prêts à vivre ça pour le peu que ça apporte, l'énergie que ça prend, les moyens que ça demande de déployer, alors qu'on pourrait sans doute utiliser d'autres formes, ne serait-ce que le traçage manuel, qu'on pourrait développer davantage, ne serait-ce que de faire davantage de tests, beaucoup plus, alors qu'on n'a toujours pas la quantité de tests qu'on devrait avoir?

Il me semble qu'il y a d'autres solutions à développer que celle-là si on reste à une application de type Bluetooth, mais ça ne veut pas dire que c'est complètement inutile. Peut-être que, dans certains cas, ça va fonctionner, mais c'est un peu demander à la population de signer un chèque en blanc, là. C'est un peu lui demander... C'est un acte de foi qu'on lui demande sur la base de résultats dont l'efficience n'a jamais été prouvée encore. Donc, c'est ça qui me gêne un peu.

Mme Lecours (Les Plaines) : Mais ce serait — je dis bien «ce serait» — un outil complémentaire, parce que le traçage manuel va demeurer également, mais il fait appel à la mémoire des gens. Moi, si on me pose la question, cette semaine, je sais pas mal tout qu'est-ce que je fais. Je suis pas mal ici, là. Mais, tu sais, la semaine passée, qui t'as fréquenté... oui, les gens que j'ai fréquentés directement, je le sais, mais qui j'ai pu passer à côté pendant au moins cinq, 10 minutes, c'est ça, c'est... Est-ce que ce pourrait être, justement, dans cette utilisation, quelque chose de complémentaire? Parce que c'est comme ça qu'actuellement l'outil qui pourrait être appliqué serait vu.

M. Roche (Stéphane) : Bien oui, encore une fois, je le dis, c'est que, dans une boîte à outils globale, ça pourrait être... Je ne suis pas, comment dire, technophobe du tout, au contraire, mais c'est juste qu'encore une fois je... Tu sais, vous êtes quelqu'un de raisonné puis vous allez prendre la notification avec le recul nécessaire, ce qui n'est pas forcément le cas de tout le monde, alors même que, cette notification, la probabilité qu'elle soit fausse est grande, est très grande. Ce n'est pas parce que vous êtes passé... Imaginez, là, imaginez que... La personne qui est derrière le guichet à l'IGA, derrière la caisse à l'IGA, elle va être notifiée combien de fois, cette personne-là? Tu sais, je veux dire, elle va être notifiée. Le risque qu'elle soit notifiée est grand, tu sais?

Donc, c'est pour ça que, dans la mesure où l'application ne va pas être capable de faire la différence, ne va pas être capable de déceler le contact ou la proximité qui fait sens par rapport, tu sais, à l'enjeu qu'elle est supposée adresser versus celle qui est complètement bénigne, bien, tu sais, il y a... Je veux dire, il n'y a pas beaucoup d'autres domaines dans lesquels on serait prêts à prendre ce risque-là. Il n'y a pas beaucoup de domaines dans lesquels on serait prêts à faire des tests massivement.

Si vous allez chez votre médecin et que vous lui dites : Ah! je voudrais que vous me testiez ça, ça, ça et ça, il va vous prendre pour un hypocondriaque. Il ne vous testera pas parce qu'il dira : Il n'y a pas de raison probante pour qu'on déploie, vous voyez, cette technique-là sur vous dans le contexte actuel. Donc, c'est ça qui me gêne un peu. C'est ça qui me gêne un peu, mais je ne peux pas vous dire non. C'est complémentaire, potentiellement, à ce qui existe.

Mme Lecours (Les Plaines) : Donc, dans la balance des inconvénients, vous, vous vous situez où?

M. Roche (Stéphane) : Bien, moi, dans la balance des inconvénients... parce qu'il y a d'autres choses qu'on n'a pas abordées, qui peuvent être des inconvénients assez graves. On voit déjà comment un certain nombre de mesures sont considérées ou pourraient être considérées, comme par exemple, je ne sais pas, nécessaires à l'autorisation d'accéder à tel service, se déplacer, ne pas se déplacer. Moi, ma crainte, c'est qu'à terme telle compagnie aérienne décide, et elle a le droit de le faire, une entreprise privée pourra le faire, de dire : Bien, si vous n'avez pas l'application, pas de service pour vous. Puis ça, vous ne serez... Personne ne sera en capacité réellement d'interdire une entreprise privée...

Mme Lecours (Les Plaines) : J'aurais une petite question, parce que je sais que mon collègue a des questions aussi à vous poser. Vous avez utilisé... Vous dites que ce serait... Bien, en tout cas, ça serait une des possibilités, d'utiliser l'obsolescence programmée pour mettre fin à... Donc, pour une fois, elle servirait à quelque chose, c'est ce que je comprends.

M. Roche (Stéphane) : Pour une fois quoi?

Mme Lecours (Les Plaines) : L'obsolescence programmée serait dans des bons termes, selon...

M. Roche (Stéphane) : Mais c'est toujours une bonne chose, l'obsolescence programmée.

• *(10 h 10)* •

Mme Lecours (Les Plaines) : Ça dépend comment c'est utilisé, là.

M. Roche (Stéphane) : Oui, oui, oui.

Mme Lecours (Les Plaines) : Donc, c'est ce que vous... Ça pourrait être une condition à...

M. Roche (Stéphane) : Oui, bien, moi, ça me semble être un élément important parce que... pour éviter que, si jamais la décision était prise de déployer une technologie de ce genre-là, elle survive à la situation pour laquelle elle aurait été déployée. Et puis c'est un genre de garantie ou d'assurance donnée aux utilisateurs qu'au-delà... Si c'est vraiment... Si la pandémie justifie que ce genre d'application soit déployée, à ce moment-là, ça doit être la seule justification.

Le Président (M. Bachand) : Merci. M. le député de Chapleau, s'il vous plaît.

M. Lévesque (Chapleau) : Oui, merci, M. le Président. Merci, Pr Roche, d'être ici avec nous, là. Vous semblez peut-être critiquer, là, dans ce que vous avez écrit, la façon, la manière dont le gouvernement du Canada, là, aurait choisi l'application COVID Shield. Bon, vous dites... Bon, il n'y a pas eu d'audits ouverts. Il n'est pas nécessairement transparent pour l'ensemble des solutions technologiques disponibles. Bon, vous dites : Ça crée un doute sur la pertinence des critères qui ont guidé leur décision. D'ailleurs, nous, on... Le gouvernement du Québec n'a pas pris la décision encore puis ne sait pas s'il va aller de l'avant avec ça. Qu'est-ce qu'il faudrait faire pour éviter de tomber dans, disons, les pièges, ces pièges-là que vous mentionnez dans votre mémoire?

M. Roche (Stéphane) : Bien, moi, je pense que, déjà, ce qui se passe, aujourd'hui, ici... Puis la consultation est quand même un préalable, à mon avis, nécessaire, peut-être pas suffisant. Ce qu'il faudrait faire ensuite, à mon avis, là, c'est que, si jamais... Tu sais, entre... Tu sais, il y a... Il faut être quand même clair. Dans les solutions technologies existantes, là, dans les familles, il y en a deux ou trois qui existent aujourd'hui, bien, on pourrait s'attendre à ce que le processus de choix, si choix il devait y avoir, soit documenté et transparent, et que les personnes à qui on va demander, c'est-à-dire la population, d'utiliser l'application, on puisse leur dire pourquoi on a choisi celle-là, pourquoi on a choisi cette... c'est quoi, les forces, c'est quoi, les faiblesses, c'est quoi, les risques, et qu'est-ce qu'on met en face des risques pour garantir, nous, aux utilisateurs qu'on a mis tout en oeuvre pour les protéger, d'une certaine manière. Donc, ça, ce serait, à mon avis, un élément, tu sais, important du dispositif général.

M. Lévesque (Chapleau) : Puis, avec ces éléments-là qu'on mettrait de l'avant, disons, qu'on retient vos recommandations, ça rendrait, donc, l'application déployable puis ce serait pertinent de le faire à ce moment-là?

M. Roche (Stéphane) : Bien, ça ne lève pas les enjeux technologiques que j'ai évoqués. C'est-à-dire, que, tu sais, je veux dire, on peut... C'est pour ça que j'insiste sur le fait qu'à mon avis les deux ou trois propositions que je fais ne sont pas totalement, mutuellement exclusives. C'est-à-dire que, pour qu'elles aient du sens, il faut qu'elles soient déployées ensemble. C'est-à-dire qu'il faut à la fois qu'on trouve le juste milieu de façon à faire en sorte que, la technologie, on améliore son efficacité, qu'on évite qu'elle envoie des notifications farfelues et massives dans la nature.

Il faut que les personnes à qui on demande de s'engager s'engagent et que ce ne soit pas juste des utilisateurs passifs à qui on dit : Allez, installez ça, et puis soyez des bons citoyens, et, si vous ne l'utilisez pas, vous serez des moins bons citoyens. C'est ce qu'on entend aussi par la bande. Donc, ça, ce serait assez, à mon avis...

Et puis, la troisième chose, c'est les engagements, effectivement, de transparence, d'ouverture que le gouvernement du Québec devrait prendre pour... C'est son rôle. C'est-à-dire que son rôle, c'est à la fois, effectivement, de mettre en place les mesures, les outils pour protéger la population d'un virus dont on connaît la dangerosité, mais aussi en s'engageant, dans la mise en oeuvre de mesures de protection, que ces mesures-là ne sortent pas d'un chapeau, et puis donc comme... c'est très critique, mais comme le gouvernement du Canada l'a fait.

Le Président (M. Bachand) : Merci beaucoup. Mme la députée de Saint-Laurent, s'il vous plaît.

Mme Rizqy : Ce serait à ma collègue...

Le Président (M. Bachand) : Parfait. Mme la députée de Vaudreuil, pardon.

Mme Nichols : Oui, merci, M. le Président. On avait oublié de vous faire un petit signe. Alors, merci beaucoup d'être parmi nous. Vos propos sont très enrichissants. En fait, ça va dans la ligne de ce qu'on a entendu, mais dans un vocabulaire très différent et quand même assez précis.

Quand vous nous parlez que ce genre d'application est inutile même quand elle est utilisée par 70 % de... quand il y a 70 % d'utilisateurs, pouvez-vous élaborer un peu? Parce que c'est sûr qu'il y a... Tu sais, cette application-là... Si, éventuellement, le gouvernement va de l'avant avec cette application-là, j'imagine, on va essayer de la vendre, cette application-là, aux gens, là, en disant : Il faut la télécharger, il faut aller de l'avant. Puis on est... Est-ce que ça peut sauver des vies? Pouvez-vous nous élaborer un peu là-dessus, sur le 70 %, là, que vous nous avez mentionné?

M. Roche (Stéphane) : Bien, ce n'est pas moi qui le mentionne.

Mme Nichols : Oui, en référence.

M. Roche (Stéphane) : Je ne fais que relater une étude, comme je le précisais au début, d'un groupe de chercheurs qui a mis en place une expérimentation statistiquement viable ou statistiquement... en tout cas, qui a du sens sur le plan statistique et qui évoque ce seuil-là. Je n'ai pas dit qu'elle n'était pas utile et efficace, même à 60 %, 70 %. Le Bluetooth reste une technologie qui n'a pas été faite... Bien, c'est une onde radio, et une onde radio qui n'a pas été faite pour mesurer des distances, ou évaluer la pertinence d'une proximité, ou quoi que ce soit. Tu sais, c'est juste une onde qui permet de transférer de l'information entre des technologies, tu sais, et de faire en sorte que mon casque d'écoute fonctionne avec mon téléphone, etc.

Donc, ça n'a pas été fait pour ça, mais c'est sûr qu'il est capable de déceler... Pour faire ça, la technologie Bluetooth doit repérer, dans son environnement, les autres technologies avec lesquelles elle va se mettre en interaction. Donc, c'est là-dessus que les spécialistes comptent en disant : Bien, on est capables de déceler la présence d'autres téléphones qui portent la... qui ont la même... avec la même technologie installée, la même application, de les détecter, mais on ne sait pas s'ils sont à 50 centimètres, à trois mètres, s'il y a quoi que ce soit entre... Bon, on ne le sait pas.

Pourquoi c'est plus efficace avec 60 % ou 70 %? Bien, c'est parce que plus on multiplie, comment dire, les utilisateurs et... C'est un peu comme dans le domaine de la statistique, hein? Plus l'échantillon est grand et plus on va éliminer aussi... C'est comme dans des mesures. Plus on fait des mesures, plus le nombre de mesures est grand et plus les erreurs systématiques, on peut les éliminer par calcul. Ce n'est pas forcément la meilleure métaphore, mais moi, je suis arpenteur-géomètre de formation, puis plus on mesure la même distance et meilleure la précision qu'on va obtenir sera grande, parce qu'on va éliminer un certain nombre d'erreurs liées à la mesure et à l'appareil, des erreurs systématiques. C'est un peu le même principe.

Mme Nichols : Encore, si 70 % des gens l'ont téléchargé, ça ne veut pas dire qu'ils l'utilisent puis...

M. Roche (Stéphane) : Non, ça ne veut pas dire...

Mme Nichols : Exactement.

M. Roche (Stéphane) : ...d'où l'importance de sensibiliser les gens pour que, s'ils la téléchargent et s'ils l'utilisent, ils l'utilisent de manière proactive, tu sais, qu'ils n'essaient pas de jouer... Je ne dis pas que les gens vont jouer avec, mais que, tu sais... puis ne pas la désactiver quand tu n'as pas envie qu'elle soit activée, tu sais, je veux dire, parce que, sinon...

Mme Nichols : Bien, vous avez aussi parlé que ça pourrait être un outil complémentaire. Quand vous parlez de complémentarité, comment ça peut être complémentaire si... C'est ça, comment ça peut être complémentaire, dans le fond, si ça ne fonctionne pas? Dans quel but ça pourrait être complémentaire si l'objectif n'est pas atteint? Ça veut dire qu'il y aurait un objectif de complémentarité?

M. Roche (Stéphane) : ...parce que je... La complémentarité, elle serait celle d'un outil qui dépasserait les limites techniques du Bluetooth. C'est ça que je dis. C'est-à-dire que je ne suis pas contre les technologies de traçage si elles peuvent sauver des vies. Personne ne peut être contre ça, évidemment. Mais je crois que, pour qu'elles puissent être efficaces, alors il va falloir qu'elles soient plus riches sur le plan technologique et sur le plan des données que ce que les applications de base fonctionnant selon le protocole Bluetooth permettent d'obtenir. Mais là, là, il y a un grand risque... Puis ce n'est pas à moi de prendre la décision... pas la prendre, mais ce que je veux dire, c'est que, si jamais on met de l'intelligence artificielle...

Je ne veux pas revenir sur l'application COVI, là, du Mila. Tu sais, j'ai eu des grandes discussions avec Yoshua Bengio puis avec les équipes là-bas, puis c'est un chercheur que j'apprécie beaucoup, puis une personne que j'apprécie beaucoup. Leur application, à mon avis, aurait... sur le plan de l'efficacité, serait certainement plus efficace. Mais là on met le bras dans un engrenage et dans un tordeur dont il faut qu'on soit conscients. C'est-à-dire que, tu sais, la fiducie de données, on ne sait pas trop comment ça fonctionne. C'est encore très en balbutiement, l'effet boîte noire de l'intelligence artificielle, son prédicteur, comment il fonctionne. On ne sait pas comment il fonctionne.

Alors, on sait que ça utilise beaucoup de données, incluant la géolocalisation. Personne ne peut garantir que tout ça, que l'anonymisation... que ça ne sera pas hacké. Tu sais, on l'a vu, là. Je veux dire, il y a... Desjardins a été hacké, tu sais. Donc, il n'y a aucune garantie, mais est-ce qu'on est prêts à prendre ce risque-là et est-ce que la situation le justifie? Je n'ai pas les compétences pour... mais ce que je dis, c'est que, si on veut que cette technologie-là, à mon avis, soit efficace, il faut qu'elle dépasse les limites techniques du Bluetooth.

• *(10 h 20)* •

Mme Nichols : Vous avez parlé... Bien, on a pris connaissance de votre mémoire, puis, entre autres, vous... c'est basé sur les enjeux techniques, les enjeux éthiques, l'enjeu humain en lien avec le traçage, puis évidemment avec votre formation, vos intérêts, le consentement. Puis j'aimerais bien vous entendre un peu sur votre position en lien avec le consentement, et cette application-là qui... Selon moi, avoir un consentement libre et éclairé... Il y a beaucoup de pédagogie qui doive accompagner le consentement, et j'aimerais vous entendre sur le consentement.

M. Roche (Stéphane) : Absolument. Bien, tu sais, oui, on est dans une situation dans laquelle il y a... comment dire, une situation de crise, une situation de pandémie. Il y a beaucoup de pression de toutes sortes. On le voit autour du port du masque. C'est une situation très anxiogène déjà. Et donc, là, si jamais on arrive avec une application comme le gouvernement du Canada l'a fait, qu'on rend disponible cette application-là, et qu'on part du principe qu'à partir du moment où les personnes vont la télécharger ils ont toutes les informations pour le faire, et que leur consentement sera libre et éclairé, à mon avis, on fait une erreur, parce que...

Puis je reviens sur les enjeux de pression sociale aussi qui ont été évoqués comme étant bénéfiques par certains, que moi, je trouve très dangereux. Dans bien d'autres domaines, on le voit, comment la pression sociale peut générer des clivages, peut générer des dissensions. On n'a pas besoin de ça dans une période de pandémie, au contraire. Donc, oui, je suis préoccupé par ces enjeux-là.

Je crois que, pour obtenir un consentement éclairé, ça prend de la pédagogie, ça prend de la transparence. Ça prend, du côté du gouvernement, vraiment une ouverture, ce qu'on évoquait tout à l'heure. S'il y a une application, il faut que les règles soient présentées, comment elle a été choisie, pourquoi celle-là a été choisie, c'est quoi, les risques que vous prenez en l'utilisant, mais c'est quoi, les gains que vous pouvez obtenir à la fois sur le plan individuel et plus sur le plan collectif, parce qu'on ne peut pas juste non plus partir du point de vue personnel dans cette affaire-là, et puis jusqu'à quand elle sera utilisée.

Est-ce qu'on peut garantir, contrairement à tout ce qui a été mis en place après les attentats du 11 septembre ou les attentats dans les aéroports en Europe il y a quelques années, où toutes ces technologies-là continuent à être utilisées, elles sont encore plus déployées... Donc, est-ce que c'est ça qu'on... Il y a une partie de la population qui risque, dont moi, de se dire : Non, là, si je n'ai pas de garantie, je ne vais pas aller là-dedans, compte tenu de...

Le Président (M. Bachand) : Merci beaucoup, M. Roche. Je dois céder la parole à Mme la députée de Saint-Laurent. Pardon.

Mme Rizqy : Merci. Bonjour. Vous êtes ingénieur et, en plus de ça, vous avez un doctorat. Et le gouvernement fédéral ainsi que le gouvernement du Québec nous disent toujours : Bien, le code source est public. Moi, là, je ne suis pas du tout ingénieure. Alors, pour moi, que le code source soit public ou pas, ça change quoi dans ma vie, qu'il soit public?

M. Roche (Stéphane) : Bien non, pour un utilisateur... Mais même moi, je ne suis pas un codeur chevronné. Donc, quand je le regarde, je comprends à peu près, mais...

Mme Rizqy : Donc, ce n'est pas une garantie de sécurité de dire : C'est un code source public?

M. Roche (Stéphane) : Non, ce n'est pas... Bien, c'est-à-dire que c'est une condition, à mon avis, nécessaire, mais pas suffisante. C'est nécessaire. Je crois que ça montre une ouverture, une transparence, que le code soit ouvert. Et puis on s'inscrit, tu sais, dans la tendance des données ouvertes, du code ouvert, etc. C'est une bonne chose, mais ce n'est certainement pas ça qui va permettre à l'utilisateur lambda de se faire une tête.

Mme Rizqy : Et est-ce que ça se peut aussi même que des développeurs de... des codeurs peuvent prendre ce code source que moi, je... D'ailleurs, je ne suis pas très favorable qu'il soit ouvert, mais, dans votre milieu, vous avez différents types d'ingénieurs, dont des architectes, qui, eux, vont créer ces pare-feux en cybersécurité, et c'est peut-être ça que, nous, il nous manque, ici, au gouvernement du Québec, d'avoir davantage d'architectes pour nous protéger davantage.

M. Roche (Stéphane) : Oui, bien, enfin, je ne sais pas s'il en manque au gouvernement du Québec.

Mme Rizqy : ...l'expertise interne.

M. Roche (Stéphane) : Mais, oui, il y a un enjeu. Je ne suis pas un spécialiste de cybersécurité. Vous en avez rencontré. C'est tellement mieux que moi. Ils ont pu vous expliquer les enjeux dans ces termes-là. Mais personne ne peut garantir... Une chose est certaine, là, c'est que personne ne peut garantir une protection absolue des données. Tu sais, ça n'existe pas, ça. Donc, il y a toujours un risque. Donc, il faut que ce risque soit géré d'une autre façon qu'en disant : Ah non! Mais ne vous inquiétez pas, sur le plan technique, tout est O.K. Ça ne marche pas comme ça. Donc, c'est une bonne chose que ce soit ouvert. Moi, ce qui me gêne là-dedans, c'est qu'effectivement c'est utilisé comme un argument suffisant, mais ce n'est pas suffisant. C'est nécessaire, mais ce n'est pas suffisant.

Mme Rizqy : Merci.

Le Président (M. Bachand) : Merci beaucoup. J'avais oublié de mentionner que notre collègue de Chomedey va être absent pour le témoignage de M. Roche et pour la personne suivante. Alors, si vous êtes d'accord, comme on a déjà fait, s'il y avait consentement pour répartir le temps du collègue de Chomedey entre les porte-parole du deuxième et du troisième groupe d'opposition... Consentement. M. le député de Gouin, s'il vous plaît.

M. Nadeau-Dubois : Merci, M. le Président. Bonjour, M. Roche. Merci d'être avec nous aujourd'hui. J'ai un peu plus de temps que d'habitude, mais pas tant que ça, ça fait que je vais procéder rapidement. M. Roche, vous êtes spécialiste des technologies géospatiales. J'aimerais qu'on parle de ça ensemble aujourd'hui. J'ai une série de questions pour vous. Est-ce que la technologie Bluetooth a été inventée pour mesurer des distances?

M. Roche (Stéphane) : Non.

M. Nadeau-Dubois : Est-ce que c'est une technologie qu'on peut caractériser de fiable pour mesurer des distances?

M. Roche (Stéphane) : Non.

M. Nadeau-Dubois : Est-ce que c'est une technologie qui nous permet de détecter la présence d'un masque ou d'une vitre, par exemple, entre deux personnes?

M. Roche (Stéphane) : Non.

M. Nadeau-Dubois : Est-ce que, donc, on peut conclure qu'il y a un risque élevé qu'une application basée sur cette technologie Bluetooth génère un nombre important de faux positifs?

M. Roche (Stéphane) : Oui, absolument.

M. Nadeau-Dubois : C'est un risque qui est élevé, vous diriez?

M. Roche (Stéphane) : Ah oui! Je le qualifierais de très élevé, oui.

M. Nadeau-Dubois : Est-ce que je peux même vous demander si vous pensez que c'est plutôt une assurance plutôt certaine que ça va générer des faux positifs?

M. Roche (Stéphane) : Ah oui! C'est certain que ça va générer des faux positifs.

M. Nadeau-Dubois : Parfait. Est-ce que, donc, on peut redouter raisonnablement que ça provoque un engorgement au niveau de notre capacité à tester des gens?

M. Roche (Stéphane) : C'est un risque, oui.

M. Nadeau-Dubois : Un risque réel et significatif?

M. Roche (Stéphane) : Je suppose que oui. Je ne connais pas la capacité de tests existante aujourd'hui, mais c'est sûr que si... Puis plus le nombre de personnes, ce qui serait une bonne chose... Plus le nombre d'utilisateurs sera grand, et donc plus le nombre de notifications sera important a priori, et donc plus le nombre de personnes qui souhaiteront être testées sera grand, et quelle sera la capacité à le faire? Je ne sais pas.

M. Nadeau-Dubois : Autrement dit, le succès de l'application, le trop grand succès de l'application pourrait nuire à notre capacité de tester en vue de la deuxième vague?

M. Roche (Stéphane) : Oui. D'ailleurs, c'est pour ça que l'étude que je mentionne toujours, publiée dans *Science,* là, met en parallèle le fait que, pour atteindre l'efficacité, il faut un nombre important d'utilisateurs, mais il faut aussi une capacité à tester qui soit... qui tienne le choc, qui soit capable de suivre, parce que, sinon, on va créer plus d'anxiété parce qu'on va devoir refuser à certaines personnes de les tester — sur quelle base, pourquoi plus une que l'autre? — alors que la notification ne nous donnera pas plus d'informations dans un cas de contact que dans un autre.

M. Nadeau-Dubois : Est-ce que ces effets pervers là qu'on vient de mentionner ensemble... est-ce que ces effets pervers là seraient également présents si on préférait à l'application une stratégie massive d'enquête épidémiologique manuelle?

M. Roche (Stéphane) : Je ne suis pas un spécialiste d'enquêtes épidémiologiques. Donc, je vais avoir du mal à répondre de façon aussi précise. Je suppose que, tu sais, dans le cas d'une enquête épidémiologique, on est capables de qualifier de façon plus précise la sensibilité des contacts, et donc on doit... a priori, on devrait générer moins de faux positifs, et donc, dans ces termes-là, vraisemblablement, moins d'engorgement, peut-être, oui.

M. Nadeau-Dubois : En posant la question à une personne, on est capables de savoir s'il y avait port du masque, par exemple, alors que la technologie Bluetooth, elle ne nous permet pas de le faire.

M. Roche (Stéphane) : Oui, absolument.

M. Nadeau-Dubois : Si je vous comprends bien, vous nous dites : En voulant choisir une technologie moins intrusive, le gouvernement du Québec, au fond, se retrouve avec un dispositif basé sur Bluetooth, qui est, en fait, inefficace. Et la seule autre option serait d'aller vers d'autres technologies, mais qui, elles, auraient comme défaut d'être beaucoup plus intrusives. Ce qui nous permet d'éviter ces deux écueils là, ce serait de miser avant tout sur du dépistage manuel massif.

M. Roche (Stéphane) : Oui, ça, c'est une alternative. C'est-à-dire que l'alternative, c'est soit d'aller vers du dépistage manuel massif, d'investir davantage là-dedans, soit, à mon avis, d'aller vers une technologie plus intrusive, avec les risques que ça pose et les engagements qui devraient être pris dans ce cas-là.

• *(10 h 30)* •

M. Nadeau-Dubois : Donc, de votre point de vue, l'option d'une application basée sur Bluetooth est la pire des trois options?

M. Roche (Stéphane) : Bien, moi, je pense que c'est une... oui, parce que je pense que c'est... Je le maintiens, ça ne veut pas dire qu'elle ne va pas être... Ça ne veut pas dire qu'à un moment donné ça ne va pas détecter un cas ou un autre, je le dis encore une fois, mais la probabilité... Tu sais, on n'a pas beaucoup de poignées pour s'assurer que les notifications vont avoir du sens.

M. Nadeau-Dubois : Donc, c'est la pire des trois options.

M. Roche (Stéphane) : D'une certaine manière, oui.

Le Président (M. Bachand) : Merci beaucoup. Je cède la parole maintenant au député de René-Lévesque.

M. Ouellet : Merci d'être avec nous aujourd'hui. Je vais aller... J'aimerais ça avoir votre opinion sur la question suivante. Comme la technologie, puis le collègue en a fait mention avec le dernier échange, n'est pas fiable, Bluetooth, comme on n'est pas certains que ceux qui vont la télécharger vont l'utiliser, donc, et même ne pas la désinstaller... Vous faites référence à l'étude publiée dans *Science*, qui nous amène à penser qu'un taux d'adoption de 60 % à 70 % serait la formule adéquate. La question que j'ai pour vous, c'est : Est-ce que le gouvernement du Québec, pour mettre en place la technologie, va devoir former des gens, va devoir former Info-Santé, va devoir former des gens qui vont devoir traiter cette

information-là? Est-ce que je suis positif ou pas? Tu sais, quand on va déployer, là, la technologie, là, grosso modo, il va y avoir des ressources qui seront attitrées à traiter cette nouvelle information là?

M. Roche (Stéphane) : Bien, c'est difficile de vous répondre. Je ne connais pas l'état des compétences qui sont présentes au gouvernement du Québec pour répondre à ça, donc, mais une chose est sûre, c'est qu'il va bien falloir qu'il y ait des ressources dédiées à ça. Est-ce qu'il va falloir les former parce qu'elles ne sont pas compétentes? Je ne sais pas, mais des ressources dédiées pour être capables... En fait, ça dépend comment vont fonctionner les notifications. Ça veut dire... Il y a différentes...

Je reprends au début. Il y a plusieurs manières de notifier. Il y a les notifications qui se passeraient entre les personnes sans même que ça aille directement... que ça soit centralisé et que la direction de la Santé publique, par exemple, reçoive l'information, puis, à ce moment-là, ce serait sur une base volontaire que les personnes ayant été notifiées diraient, un peu comme Mme la députée le disait tout à l'heure : Je devrais... ça serait plus prudent que j'aille me faire tester, et puis peut-être que je dois prendre du recul et moins voir les personnes avec qui je suis en contact régulier.

Puis, à ce moment-là, il n'y a pas de gestion, au niveau du gouvernement, à assurer, si ce n'est de recevoir la demande de certaines personnes qui vont vouloir être testées. Puis là on revient à ce qui a été évoqué par votre collègue, c'est : Si jamais les demandes sont massives, quelle sera la capacité à le faire? Et est-ce qu'on ne va pas gérer de la frustration et de la crainte si jamais on dit aux gens : Bien non, là, attendez, là, ne virez pas fous, on ne va pas tester tous ceux qui arrivent avec une notification positive?

M. Ouellet : Oui. Puis, par la suite, si jamais on est positif, il va falloir entrer un code pour notifier les autres. Donc, il y a quelqu'un qui va donner un code à quelque part...

M. Roche (Stéphane) : Bien, ça, ça pourrait être très simple. Ça pourrait être l'utilisateur qui, à partir du moment où il est notifié, ait juste à aller cocher : J'ai été notifié. Donc, tous ceux avec qui j'ai été en contact au cours des 15 derniers jours vont recevoir une notification comme quoi ils ont été en contact avec quelqu'un qui a été notifié puis... qui a été notifié, pas qui a été testé positif. Donc, tu sais, il y a aussi deux choses. Est-ce que le fait d'avoir été notifié comme ayant dans sa chaîne de contacts quelqu'un qui pourrait être porteur, ça... Tu sais, c'est très compliqué. Quel type de notification va être envoyé? Est-ce que c'est une notification qui dit : Dans votre chaîne de contacts, vous avez été en contact avec quelqu'un qui a été testé positif ou alors est-ce que vous êtes notifié parce que quelqu'un, dans votre chaîne de contacts, a été notifié?

M. Ouellet : C'est exponentiel.

M. Roche (Stéphane) : Bien, potentiellement, oui.

M. Ouellet : Donc, lorsque la collègue de Jean-Talon faisait référence, tout à l'heure, à... Si on peut... Si cette technologie nous permet de libérer des ressources attitrées au traçage manuel pour travailler à cette application... pas travailler, mais à répondre à cette demande d'application là, avec l'échange qu'on a, ce ne sera pas le cas. C'est-à-dire que les ressources devront quand même travailler sur le traçage manuel. Et on ne peut pas faire l'équation à savoir que, si on utilise cette technologie-là, moins de ressources seraient utilisées à faire du traçage manuel parce qu'on aura du traçage informatique qui va nous amener à être plus outillés pour identifier les gens.

M. Roche (Stéphane) : Je ne suis pas sûr d'avoir saisi votre question.

M. Ouellet : Bien, ce que je veux savoir, c'est que la technologie devrait, si elle est bien utilisée, avoir moins de manutention humaine, et donc nous permettrait de dédier les ressources à faire autre chose que de la manutention d'information manuelle.

M. Roche (Stéphane) : Bien, encore une fois, ça dépend. Est-ce que c'est une solution complètement décentralisée ou partiellement décentralisée? Si c'est complètement décentralisé, et qu'à la limite la Santé publique n'est même pas au courant de ce qui se passe dans les chaînes de traçage, et que, sur une base volontaire, les utilisateurs qui seraient notifiés vont, eux, demander à être testés, par exemple, là, il n'y a pas d'enjeu, si ce n'est que sur la capacité à tester.

Maintenant, si c'est centralisé, c'est-à-dire que l'information... Lorsqu'une personne, dans une chaîne, est testée positive et qu'elle l'indique, là, l'information est renvoyée au central, à la Santé publique, par exemple, qui, elle, redéploie ça à toutes les personnes de la chaîne de contacts. C'est une autre manière de procéder. C'est toujours sur la base de la technologie Bluetooth, mais c'est soit centralisé soit décentralisé. Puis là, évidemment, les enjeux de ressources nécessaires au niveau de l'État ne sont pas les mêmes.

Le Président (M. Bachand) : Merci beaucoup. C'est tout le temps qu'on a. Merci beaucoup, M. Roche, de votre participation.

M. Roche (Stéphane) : Merci à vous.

Le Président (M. Bachand) : Cela dit, je suspends les travaux quelques instants. Merci.

(Suspension de la séance à 10 h 36)

(Reprise à 10 h 47)

Le Président (M. Bachand) : Alors, à l'ordre, s'il vous plaît! La commission reprend ses travaux. Il nous fait plaisir d'accueillir Mme Castets-Renard, professeure titulaire de la Faculté de droit civil de l'Université d'Ottawa. Alors, bienvenue. Bon vendredi. Merci beaucoup d'être ici. Alors, on débute avec vous. Vous avez 10 minutes de présentation, après ça, un échange avec les membres de la commission. Alors, encore une fois, bienvenue. La parole est à vous.

Mme Céline Castets-Renard

(Visioconférence)

Mme Castets-Renard (Céline) : Merci beaucoup, M. le Président. Merci beaucoup, Mmes et MM. les députés. Il me fait plaisir... C'est un grand honneur d'être parmi vous. Et je vous remercie d'avoir accepté une visioconférence pendant ma quarantaine. Mon nom est Céline Castets-Renard. Je suis professeure à l'Université d'Ottawa, à la section de droit civil, et je suis titulaire d'une chaire de recherche sur l'intelligence artificielle, responsable à l'échelle mondiale.

J'ai écouté attentivement les auditions et les consultations particulières qui ont eu lieu jusqu'à présent — très passionnantes — et j'aimerais revenir sur trois enjeux principaux, un enjeu concernant la vie privée et les renseignements personnels, un enjeu social concernant l'acceptabilité, dont il a beaucoup été question. Et je me permettrais de parler aussi de la réforme du cadre légal puisqu'en tant que juriste je ne résiste pas à la tentation d'étendre la question posée au-delà du mandat de la commission.

Donc, pour le premier enjeu, concernant la vie privée et la protection des renseignements personnels, je rejoins parfaitement ce que le Pr Pierre-Luc Déziel a dit hier, s'agissant de la nécessité d'intégrer les débats et les analyses dans le cadre de la protection des renseignements personnels et de la vie privée. Même si l'interprétation même de la notion de renseignements personnels pourrait faire croire que l'on est en dehors du champ de cette protection puisqu'il s'agit... le renseignement personnel est un renseignement qui permet d'identifier la personne, et qu'on nous dit que les applications de notification de traçage qui pourraient être choisies ou l'application qui pourrait être choisie ne collecteraient pas de renseignements personnels, il y a toujours un risque de réidentification que nous a rappelé le Commissariat à la protection de la vie privée du Canada et, également, le commissariat à l'information et à la protection de la vie privée de l'Ontario, et, même si ce risque est minime, il n'est pas nul, et il me semble que le gouvernement du Québec doit en tenir compte, qu'il faut effectivement considérer la protection des renseignements personnels et les lois québécoises en la matière.

Et, au-delà de cette interprétation extensive, hein, il faut le dire, je pense qu'il s'agit aussi de l'occasion de réfléchir à la définition même de ces renseignements personnels, en particulier dans le cas du projet de réforme du projet de loi n° 64. Simplement, à titre d'exemple, je voudrais signaler qu'en droit de l'Union européenne, depuis 1995, depuis la directive de 1995, et ça a été réitéré par le règlement général de protection des données en 2018, la notion de données personnelles intègre les données qui permettent d'identifier, mais qui rendent aussi identifiable directement ou indirectement, si bien que, si on a une réidentification plus tardive dans le temps, par croisement de fichiers, par exemple, on peut tomber sous le coup de la loi sur la protection des données personnelles. Donc, je pense que c'est l'occasion d'avoir une réflexion sur cette notion au-delà de la question des applications de traçage ou de notification des contacts.

• *(10 h 50)* •

Et il en est de même aussi des notions de pseudonymisation et anonymisation, parce qu'effectivement le commissariat à la vie privée l'a signalé, il ne s'agirait pas de données anonymisées, mais pseudonymisées. Ça a l'air d'être un débat technique, mais en fait ça fait une grande différence juridique aussi, puisque les données, même pseudonymisées, doivent encore être protégées par la loi sur les renseignements personnels, ce qui ne serait pas le cas des données anonymisées, puisque, par définition, on ne peut plus réidentifier la personne.

Donc, je pense que toutes ces notions doivent être approfondies au-delà, encore une fois, du débat sur les applications de notification des contacts, mais aussi dans le cadre du projet de réforme de la loi n° 64. J'aimerais aussi ajouter que, si le gouvernement du Québec décide d'aller de l'avant avec cette application, il est fort probable qu'il n'y ait pas d'expérimentation ou que l'expérimentation soit limitée puisqu'il y a une certaine urgence, si bien qu'il devra y avoir un contrôle a posteriori de la mise en oeuvre de cette application.

Et, à titre d'exemple, je voudrais parler de la France et de l'application de StopCovid. Même si la CNIL, la commission nationale informatique et libertés, à deux reprises, au mois de mai et au mois de juin, a appuyé cette application et a considéré qu'elle était conforme au règlement général de protection des données et à la loi française, à la loi nationale, Informatique et Libertés, ça n'a pas empêché de faire un contrôle et de mettre en demeure le ministère de la Santé, le 15 juillet dernier, parce que certaines dispositions ne se conformaient pas parfaitement aux réglementations.

Donc, je pense que ce serait important d'avoir un contrôle étroit et rapide, finalement, à partir du moment où l'application serait déployée, si elle l'est. Et, si on fait l'analogie, même si la CAI, la Commission d'accès à l'information du Québec, donne... Admettons qu'on considère que l'application est conforme, il faudra qu'elle puisse faire un contrôle a posteriori.

J'aimerais, évidemment, aussi évoquer les enjeux sociaux assez rapidement. La question de l'acceptabilité sociale, le taux d'adhésion a déjà beaucoup été mis de l'avant hier par les autres experts. J'ai un peu l'impression aujourd'hui qu'on est un petit peu dans une opposition : soit on choisit une application volontaire, et auquel cas le risque est que l'adhésion soit faible, et donc qu'elle ne soit pas efficace, soit on l'impose, ce qu'ont fait certains États totalitaires, et évidemment on porte atteinte aux libertés individuelles.

La réconciliation entre les deux est possible. On peut faire une balance des intérêts, il en a déjà été question, entre la santé publique et la vie privée. Mais encore faut-il qu'il y ait un gain pour la santé publique, ce qui n'a pas encore

été démontré. Et, même si on considère que, bien, il faut déployer la solution pour le savoir, finalement, c'est tout à fait possible de l'envisager. La vie privée n'est pas un droit... c'est un droit fondamental, mais pas absolu. On peut y porter atteinte, mais, quand même, il faut faire un strict contrôle. Il doit y avoir des critères de cette balance des intérêts, des critères de nécessité, de légitimité, finalité, proportionnalité, efficacité, minimisation des risques. Et cette analyse doit se faire in concreto, en considération de l'application. Donc, la réconciliation est possible. La balance est possible, mais il faut faire une analyse.

Et, au-delà de cette analyse d'experts, j'aimerais évoquer tout de même les enjeux sociaux et l'intégration de toute la population par rapport à l'utilisation de cette technologie. Il faut faire preuve d'inclusion sociale, de pédagogie, parce que, pour l'instant, on est toujours face à une fracture numérique, hein, au-delà de ces applications. Donc, il faut l'avoir à l'esprit. Le gouvernement doit faire ce travail, je pense, de pédagogie, et on doit contribuer à l'aider. Et je voudrais dire que l'OBVIA, l'observatoire sur les impacts sociétaux de l'IA et du numérique, au Québec, fait ce travail. Les chercheurs de l'OBVIA font ce travail de pédagogie et de débat public. Et je vous remercie de nous donner l'occasion d'en parler, d'avoir fait cette consultation d'experts et cette consultation au public en même temps.

Je voudrais ajouter que je ne suis pas d'accord avec l'idée qu'il suffit d'aller de l'avant, de déployer la technologie, et, si ça ne marche pas, ce n'est pas grave, on la retire. Je pense que ce n'est pas neutre et ce n'est pas pas grave, parce que soit ça va entraîner un rejet de la technologie parce qu'on dira : Ça ne marche pas, ça ne sert à rien, et je trouverais ça dommageable parce qu'il y a des applications qui sont utiles pour la société et qu'il faut déployer, ou ça pourrait entraîner une banalisation de la technologie, et on dirait : Bon, ce n'est pas grave, on abandonne un peu sa vie privée. Et c'est un peu le discours de la société de surveillance, de la Quadrature du Net, et ce discours aussi me paraît... cet écueil me paraît dangereux aussi. Donc, je pense qu'entre les deux il y a évidemment des voies à trouver, mais qu'il faut trouver ensemble et pas simplement entre experts.

Et, pour finir, je pense que, ce débat, on doit l'avoir plus globalement, comme je le disais, dans le cadre d'une réforme légale. Il me semble que le Québec doit se doter d'un cadre légal robuste, que, pour l'instant... bien, dont on ne dispose pas pour l'instant. Les lois sur les renseignements personnels ont une vingtaine d'années. Il est temps d'adapter ce schéma. L'Union européenne l'a fait et prévoit d'aller encore de l'avant.

Et je voudrais finir avec... en soulignant que le Québec est une plateforme de... une place forte de l'intelligence artificielle, mais que le Québec ne déploiera tout son talent que si son cadre légal est robuste. Et j'ajouterais que la loi n'est pas là pour contraindre l'innovation, mais, au contraire, pour l'accompagner, la promouvoir et surtout la sécuriser. Et je vous remercie de m'avoir permis d'avoir ces propos introductifs.

Le Président (M. Bachand) : C'est nous qui vous remercions. Donc, nous allons débuter la période d'échange avec le député de Chapleau. M. le député, s'il vous plaît.

M. Lévesque (Chapleau) : Merci beaucoup, M. le Président. Bonjour, Pre Castets-Renard. Un plaisir d'échanger avec vous aujourd'hui. Merci de votre présentation fort intéressante.

D'abord, tout simplement pour clarifier avec vous, vous vous inscrivez également, là, un peu dans ce que le Pr Déziel disait hier, là, que le débat et l'analyse de l'application devaient se faire dans le cadre juridique actuel, donc, que ça soit inclus dans les lois visant la protection de la vie privée et également des renseignements personnels. C'est bien cela?

Mme Castets-Renard (Céline) : Oui, oui, c'est tout à fait ça. Et le Commissariat à la protection de la vie privée a un peu un double discours, a un discours juridique et un discours, je dirais, un peu plus politique. Le discours juridique est de dire qu'éventuellement il n'y a pas de renseignements personnels, mais le discours politique est de constater que, partout dans le monde, le débat se fait dans le cadre des lois de renseignements personnels et vie privée. Et donc le Québec ne pourra pas passer à côté, je pense.

M. Lévesque (Chapleau) : Non, tout à fait. Puis je pense que, si jamais le gouvernement décidait d'aller de l'avant, ce serait son intention, là, d'offrir le maximum de sécurité et de protection, là, aux citoyens québécois. Faisons un peu de droit comparé, là. Vous avez mentionné le droit européen, notamment sur la définition de renseignements personnels. Est-ce que ce serait la définition qui devrait être appliquée ou si on fait, dans le fond, un peu de projection? Ce serait ça qu'on voudrait comme définition ou en auriez-vous une autre à proposer?

Mme Castets-Renard (Céline) : Je vais vous en donner les avantages et les inconvénients, et puis il appartiendra évidemment au législateur de trancher.

L'avantage, je rappelle très rapidement... Donc, en droit de l'Union européenne, donc, depuis déjà 25 ans, on considère qu'une donnée personnelle est une donnée qui permet d'identifier ou de rendre identifiable directement ou indirectement. Donc, c'est une définition très large. Les avantages, c'est qu'effectivement on peut anticiper toute évolution technologique. Et on peut aussi avoir une projection dans le temps, une projection dynamique de la donnée, parce que, même si la donnée n'est pas... On n'identifie pas aujourd'hui la personne. On peut l'identifier demain. Donc, cette action dynamique permet d'anticiper les risques futurs. Donc, ça, c'est l'avantage.

L'inconvénient, il faut quand même le souligner, c'est que la définition est très large et que, du coup, les entreprises, les organismes qui doivent respecter la loi nous disent : Mais toutes les données personnelles... Et donc il faut le respecter partout. C'est un petit peu la tendance dans l'Union européenne et avec le règlement général de protection des données qui a renforcé énormément cette protection. Oui, ça a été un grand branle-bas de combat partout, dans toutes les organisations en Europe et ailleurs, avec toutes les entreprises qui travaillent aussi avec l'Europe et qui échangent des

données personnelles avec l'Europe. Oui, aujourd'hui, je pense qu'il n'y a quasiment pas de bases de données sans données personnelles. Et donc, oui, il faut respecter ce cadre.

• *(11 heures)* •

M. Lévesque (Chapleau) : D'accord, excellent. Vous avez parlé qu'il pourrait y avoir, notamment en lien avec l'acceptation sociale... l'acceptabilité sociale, pardon, un gain pour la santé publique. Toutefois, ça prendrait une balance. Puis vous avez nommé, là, de nombreux critères, notamment la nécessité... et plusieurs autres, notamment, avec une analyse d'experts. Est-ce qu'actuellement vous avez constaté ça dans une juridiction ou, même au Canada, est-ce que ça a été fait? Puis, sinon, comment vous envisageriez cela, soit en amont, en aval, un peu, votre perception sur ces différents critères là, puis comment on les met en application?

Mme Castets-Renard (Céline) : À ma connaissance, ça n'a pas été fait par une juridiction, mais c'est, en principe, l'objet d'études d'impact, des études d'impact de... ou ce qu'on appelle les évaluations des facteurs de vie privée au Canada et au Québec et ce qu'on appelle étude d'impact ou analyse d'impact des données personnelles en France ou en Europe, mais c'est la même logique.

D'essayer de faire une étude en amont, ça rejoint un peu l'idée de «privacy by design», la protection de la vie privée en amont dès la conception, avant le déploiement, pour essayer justement de minimiser les risques, de respecter le principe de nécessité, de finalité, etc. Et cette évaluation est faite précisément... a été faite par le Commissariat à la protection de la vie privée du Canada et par l'Ontario. Et la Commission d'accès à l'information du Québec se propose aussi de faire cette analyse quand une application sera sur la table officiellement, on va dire.

Donc, c'est une analyse qui est faite jusqu'à présent par les autorités de protection des données, donc par les autorités administratives. Mais, sinon, par analogie, ce type de critères, on les retrouve aussi quand les juridictions font des balances des intérêts, comme la Cour européenne des droits de l'homme, la cour de justice de l'Union européenne. Et toutes les cours un petit peu partout dans le monde font très souvent ces balances d'intérêts entre deux droits fondamentaux puisque ce n'est pas une situation nouvelle que d'avoir à faire ce genre de balance.

M. Lévesque (Chapleau) : O.K., merci beaucoup. Vous avez également parlé du cadre légal qui devrait être robuste. C'est-à-dire qu'actuellement, avec les lois, au Québec, que nous avons, je sais qu'elles n'ont pas été dépoussiérées depuis une vingtaine d'années, là, mais notre gouvernement a, bien entendu, l'intention d'aller de l'avant et de renforcer ces lois-là, parce que c'est une priorité, pour nous, et c'est un engagement bien important. On veut protéger la vie privée des Québécois et également les renseignements personnels. Actuellement, le cadre que nous avons pour déployer une application, est-ce que vous voyez des risques? Est-ce que vous voyez des failles, des vulnérabilités? Quelles sont-elles?

Mme Castets-Renard (Céline) : À l'heure actuelle, les lois sont incomplètes. Par rapport aux définitions qui peuvent être données, j'ai cité la définition de renseignement personnel. Ça me paraît aussi assez incomplet par rapport aux droits accordés aux personnes, par rapport à l'étude d'impact aussi, et surtout par rapport aux sanctions et moyens qui seraient accordés à la Commission d'accès à l'information du Québec. Je sais que, dans le projet de loi n° 64, on va de l'avant par rapport à tous ces objectifs-là.

Donc, ça, je trouve ça vraiment essentiel et fondamental à faire. Mais, si je peux me permettre d'aller au-delà de ce cadre-là, toutes les questions liées aux technologies ne se limitent pas à la protection des renseignements personnels et de la vie privée. On a beaucoup d'autres enjeux, de droit de la concurrence, de droit de la consommation. On a aussi, bien sûr, des enjeux de discrimination. Et tous ces enjeux-là doivent aussi être adressés, me semble-t-il, et ça dépasse le cadre de ce type de réglementation.

M. Lévesque (Chapleau) : D'accord, mais, pour, donc, peut-être prendre la balle au bond avec le projet de loi n° 64, je vois que vous êtes bien informée. On pourrait peut-être élargir justement la discussion. Est-ce qu'au niveau des sanctions, au niveau des pouvoirs qui pourraient être donnés, notamment, à la commission, ce sont des éléments, des pistes de solution qui sont intéressantes? Est-ce qu'on va assez loin? Est-ce que c'est un bon projet de loi?

Mme Castets-Renard (Céline) : Oui. Je pense que, de ce point de vue là, il faut aller loin sur les sanctions. Ça a déjà été mentionné. On a affaire à des grands acteurs du numérique, au fameux GAFA : Google, Apple, Facebook, Amazon. Donc, on a affaire à des grands joueurs qui doivent effectivement se rendre compte de leurs responsabilités et doivent rendre compte de leurs actes. Et je pense que des sanctions doivent être suffisamment crédibles pour que la menace soit crédible.

L'Union européenne a mis du temps à le faire, mais le fait sur le fondement des renseignements personnels, le fait sur le fondement du droit de la consommation et de la concurrence. Et le débat paraît... Je ne dirais pas qu'on est très crédibles ou qu'on est à égalité, mais le débat a quand même pris une autre ampleur depuis qu'on a, la Commission européenne en particulier, commencé à envisager des sanctions un peu plus lourdes et depuis aussi que ces sanctions sont médiatisées. Et on a parlé hier de la sanction de réputation, et je pense qu'elle n'est pas négligeable.

M. Lévesque (Chapleau) : D'accord. Dernière petite question, là, spécifiquement sur la Commission d'accès à l'information. Ils sont venus témoigner hier... Elle est venue, c'est-à-dire, témoigner hier, demandant peut-être plus de ressources et également, là, peut-être plus de mordant dans leur réglementation. Est-ce que c'est une voie qui serait envisageable pour vous et, si oui, ça irait dans quel sens?

Mme Castets-Renard (Céline) : Je soutiens absolument cette demande. Et, pour vous donner un exemple, en France, pendant très longtemps, on a... La loi sur la protection des données personnelles date de 1978, et avant le RGPD 2018, on ne prenait pas du tout au sérieux cette réglementation parce qu'il n'y avait pas de sanctions ou qu'elles étaient minimes. Donc, je pense que prendre au sérieux le suivi va avec des sanctions et va avec des pouvoirs forts de ces autorités de protection, des pouvoirs de contrôle, des pouvoirs indépendants et, bien sûr, des pouvoirs financiers, des ressources financières. Ça me paraît absolument essentiel. Et, quand on compare, dans l'Union européenne, on a des situations très variées, et ça a été un des points majeurs de la réforme par le RGPD que de doter toutes les institutions de ces ressources.

M. Lévesque (Chapleau) : Parfait. Merci beaucoup. Je pense que mon collègue de Beauce avait des questions.

Le Président (M. Bachand) : Merci. M. le député de Beauce-Nord.

M. Provençal : Merci, M. le Président. Bonjour, madame. Merci beaucoup de contribuer à l'évolution de nos travaux.

Écoutez, je vais revenir sur un point qui a été soulevé par mon collègue. Quand, dans votre mémoire, vous parlez «de faire une balance des intérêts en présence et reconnaissance [des] droits fondamentaux à concilier plutôt qu'à opposer», mais, dans ça, là, pouvez-vous clarifier et puis élaborer un petit peu plus, s'il vous plaît? Parce que je pense que vous soulevez quand même des enjeux majeurs, là.

Mme Castets-Renard (Céline) : Quand on fait cette balance des intérêts, donc, on va... Si on prend l'exemple, effectivement, de l'application de notification et si on considère deux intérêts, santé publique et vie privée, on peut être amené à privilégier l'un ou l'autre. Mais, si on privilégie l'un, ça ne veut pas dire qu'on abandonne complètement l'autre et qu'il faut...

Donc, en clair, ici, s'il fallait en exiger un, ce serait la protection de la vie privée au profit de la santé publique. C'est cette balance-là qui a été faite, par exemple, par la CNIL, en France, hein, par la Commission nationale de l'informatique et des libertés, en disant : D'accord, la protection des renseignements personnels et de la vie privée, ce sont des droits fondamentaux, mais qui ne sont pas absolus. Donc, on peut réduire, finalement, le niveau de protection, mais, pour autant, il faut des garanties, et ce sont les garanties par rapport aux droits fondamentaux, en faisant les critères que je viens de... que j'ai déjà exposés, en rapport avec les critères que j'ai déjà exposés. Et, par exemple, l'anonymisation des données, ça veut dire qu'il ne faut collecter que les données qui vont être nécessaires à une finalité.

Donc, tout est lié, en fait : la finalité, la nécessité de l'application, la nécessité de la mettre en oeuvre et, évidemment, son efficacité. Et donc toutes ces contraintes doivent s'entendre ensemble. Et on peut considérer que, s'il y a une faille, finalement, dans l'un de ces critères, bien, par répercussion, on risque de ne pas pouvoir atteindre les autres ou, en tout cas, on aura un niveau qui va s'affaiblir. Clairement, si on considère qu'il n'y a pas d'efficacité ou de nécessité avec cette application, on ne va pas pouvoir justifier l'atteinte à la protection de la vie privée et des renseignements personnels. Ça, c'est un arbitrage politique à faire aussi collectivement, me semble-t-il.

M. Provençal : Donc, vous énoncez clairement que la protection de la vie privée doit être prioritaire par rapport à la santé.

Mme Castets-Renard (Céline) : Ça n'est pas ce que j'ai dit.

M. Provençal : C'est ce que j'ai perçu.

Mme Castets-Renard (Céline) : Non, non. Je dis que, dans la balance, ça voudrait dire qu'on... Si on considère la santé dans l'équilibre, on baisse le niveau de protection de la vie privée, mais on ne doit pas le baisser trop et on ne le baisse que si on a un gain significatif. C'est ça, une balance, c'est que si on a un gain significatif en santé publique, qui n'a pas encore été démontré, à ma connaissance.

M. Provençal : Merci. J'aurais un deuxième point. Vous écrivez : «L'opportunité d'une telle application n'est-elle pas perdue d'avance? Peut-on réconcilier droit, éthique et efficacité?» J'aimerais ça que vous me clarifiiez ce que vous venez... ce que je viens d'énoncer, s'il vous plaît.

Mme Castets-Renard (Céline) : Ça fait écho à ce que je disais dans ma présentation. Ça fait quand même plusieurs semaines qu'on réfléchit collectivement et individuellement à tous ces sujets-là, peut-être depuis le mois de mars, avril, et moi personnellement, je n'ai pas l'impression d'avoir avancé dans la réflexion parce qu'à chaque fois je me dis : C'est important que ça reste volontaire parce que je tiens à nos libertés. Et, en même temps, moi, la première, je n'ai peut-être pas spécialement envie de télécharger une application si je ne vois pas l'efficacité ou si je ne vois pas un gain collectif, sans parler d'un cas personnel, mais si je n'en vois pas l'utilité, et je pense que beaucoup de personnes raisonnent comme ça.

Et d'après ce que je perçois de ce qui s'est passé en France avec StopCovid, avec seulement 4 % d'adhésion, c'est que, tout simplement, personne n'a vraiment compris que ça pouvait être utile. L'utilité sociale, c'est quand même quelque chose d'important. Et, du coup, j'ai l'impression que, pour que ça marche, que ça ait un effet, il faudrait le rendre obligatoire, que ce soit très contraignant, un peu comme ce qu'on a vu dans certains États en Asie, plutôt avec une démarche totalitaire, et on comprend bien que personne ne veut ça dans nos sociétés démocratiques.

Donc, c'est en cela que je n'ai pas d'issue, je n'ai pas de solution à cette, ce que j'ai dit, quadrature du cercle. Je ne vois pas bien comment en sortir.

• *(11 h 10)* •

M. Provençal : Je vous remercie beaucoup.

Le Président (M. Bachand) : Merci. Mme la députée de Jean-Talon, il vous reste une petite minute.

Mme Boutin : ...simplement une question. J'en aurais eu plusieurs, mais c'est vraiment très intéressant. Merci d'être là. Vous avez mentionné dans votre présentation qu'il y a des exemples de technologies qui pourraient être utiles à la Santé publique. Avez-vous des exemples concrets?

Mme Castets-Renard (Céline) : Bien sûr. L'intelligence artificielle et le «machine learning» sont beaucoup utilisés en ce moment autour de la pandémie, par exemple, pour la recherche des vaccins, pour accélérer le temps et le «process». Donc là, on peut penser que c'est utile pour la société, hein, même à l'échelle mondiale. Également, aussi, il y a eu du «machine learning» qui est utilisé, ne serait-ce que dans les travaux, dans les études, parce qu'énormément de travaux sont faits par de nombreuses communautés partout dans le monde.

Donc, c'est très difficile d'agréger les informations, les données. Donc, on utilise aussi, bien sûr, des bases de données, mais du «machine learning» aussi sur ces bases de données pour agréger l'information et même pour faire fonctionner ensemble des laboratoires un petit peu partout dans le monde. Donc, pour moi, ça, ce sont des usages utiles.

Et je ne sais pas si je peux me permettre d'évoquer ce sujet, mais vous avez auditionné, mercredi, M. Yoshua Bengio du MILA. Le MILA a fait beaucoup de travaux et beaucoup de recherches épidémiologiques. Les modèles épidémiologiques aussi font partie de l'utilisation... enfin, de ces exemples positifs d'utilisation de l'IA. Et c'est vrai qu'il y a des aspects dans ces recherches qui sont forcément intéressants pour la société. Même s'il y avait... Dans ces recherches, il y a une partie recherche épidémiologique et une partie «contact tracing» ou notification des contacts. Donc, il y a plusieurs enjeux, plusieurs finalités, mais il y a des aspects qui sont utiles pour la santé et la société.

Mme Boutin : J'espère sincèrement que vous allez être invitée dans le cadre des consultations particulières du projet de loi n° 64, Mme Castets-Renard.

Mme Castets-Renard (Céline) : Ce serait avec plaisir. Merci beaucoup.

Le Président (M. Bachand) : Merci. Mme la députée de Vaudreuil, s'il vous plaît.

Mme Nichols : Merci, M. le Président. Merci d'être parmi nous. Bienvenue à l'Assemblée nationale en virtuel.

Alors, vous avez parlé, là, dans vos recommandations, que, si l'application devenait inutile, évidemment, là, de la retirer. Puis on a entendu plusieurs experts aussi à cet effet-là, de même inclure une clause, là, dans le législatif, là, à cet effet-là, parce que ça ne sert à rien de la laisser perdurer inutilement. Et vous faites mention que de revenir en arrière pourrait avoir des séquelles... pas avoir des séquelles, mais vous avez dit : Ce n'est jamais neutre. Alors, moi, je vais y aller avec les séquelles. Je me dis : Où vous voyez la problématique si on revenait en arrière?

Mme Castets-Renard (Céline) : Bien, je pense qu'on ne pourra pas se contenter de dire : On a essayé, ça n'a pas marché, ce n'est pas grave, parce qu'il y va du crédit de la technologie de manière générale. Une prochaine problématique, une prochaine technologie pourrait tout à fait être très bien et très utile pour la société, mais on aura ce mauvais souvenir, hein? Collectivement, on peut tout à fait se dire : Ah! non, mais on a déjà essayé la technologie, ça ne marche pas, ce n'est pas bien. Donc, il faudra refaire des efforts de conviction, d'adhésion, d'explication, alors que ça pourrait être tout à fait utile.

Donc, ça, c'est la question du rejet de la technologie en tant que telle, et de mettre un petit peu tout dans le même panier, et de jeter le bébé avec l'eau du bain. Ce serait quand même un peu dommage, alors que, comme je le disais, en santé, on a des avancées extraordinaires. Le «machine learning», ça marche très bien sur l'imagerie médicale et ce serait quand même dommage de s'en priver au prétexte que toute technologie est mauvaise.

Mais, à l'inverse, il y a aussi un autre problème, c'est que, si on fait un petit peu l'apprenti sorcier et qu'on sort des applications un peu à tort et à travers, si je puis dire... Je caricature, hein, un petit peu, mais, si on le fait de manière excessive, sans se laisser beaucoup de temps de réflexion... Les gens s'habituent un petit peu à avoir des bracelets, des choses sur leur téléphone qui sont déjà des mouchards, hein? Ces téléphones nous dévoilent déjà beaucoup. Il y a une banalisation, une habitude qui ne me paraît pas non plus utile, qui me paraît aussi préjudiciable pour la société, parce que je pense qu'il faut qu'on reste vigilants et critiques, hein? C'est toujours ce que je dis à mes étudiants : Restez toujours à l'écoute et en éveil.

Mme Nichols : Mais vous faites référence, là, à des conséquences en lien avec la réputation qu'on pourrait rattacher à la technologie, mais il y a sûrement aussi, là, des conséquences auprès des citoyens, auprès des utilisateurs, des personnes qui l'auront utilisée tant au niveau des données, mais aussi, là, au niveau plus humain, à cet effet-là aussi. Par rapport au consentement, vous faites... Vous êtes professeure. Vous faites du droit civil. Donc, j'imagine que la notion du consentement est importante pour vous.

Mme Castets-Renard (Céline) : Oui, elle est importante et elle est affirmée dans les lois de protection des renseignements personnels et davantage encore dans la réforme du projet n° 64. Elle est très fortement affirmée aussi

dans le règlement général de protection des données personnelles en Europe. Mais, en même temps, on voit beaucoup de limites et on voit bien aujourd'hui qu'on nous demande d'accepter tout, de cocher des cases, et on a des images qui surgissent, des messages interstitiels qui surgissent tout le temps à notre écran pour dire : O.K., oui, j'accepte, oui, je veux les cookies, oui, tu peux me tracer, etc., parce que, sinon, de toute façon, on n'a pas accès aux services.

Et donc le problème aujourd'hui, c'est que la façon dont ce consentement se matérialise est que, finalement, on est un petit peu prisonnier. Même si on doit avoir... on est censé avoir un consentement éclairé, explicite et avoir une certaine qualité de consentement, dans les faits, ce n'est pas vraiment ce qui se passe en matière technologique. Et là je me permets de vous renvoyer aux travaux de mon collègue et ami, le Pr Vincent Gautrais, qui travaille beaucoup sur la question du consentement.

Mme Nichols : Merci. Au niveau du cadre légal... Je sais qu'on l'a abordé un petit peu plus tôt avec les collègues, mais on parlait du cadre légal. Il n'y a pas vraiment... Présentement, comme on le dit depuis plus de deux jours, là, c'est qu'il n'y pas de mordant. Il n'y a pas de conséquences, là, à tout ça. Votre position... Qu'est-ce que vous recommanderiez comme conséquences? Des conséquences pécuniaires, des conséquences... parce qu'il y a les conséquences, évidemment, pour les entreprises, mais il y a un lien avec l'imputabilité aussi.

Mme Castets-Renard (Céline) : Oui, bien, je pense qu'il va falloir... Alors, sauf erreur de ma part, et vous me corrigerez, c'est peut-être parce que j'ai mal compris le projet de loi n° 64, il me semble qu'on fait un peu un effort de clarification sur qui doit faire quoi, qui doit être responsable de quoi, mais il y a quand même, dans... On est dans des écosystèmes numériques très complexes, et ça, c'est mon collègue Sébastien Gambs qui le disait hier, en disant que, derrière une application, il y a tout un écosystème et il y a tout un tas d'acteurs en arrière-plan.

Et c'est un petit peu pour tout dans l'économie numérique. Il y a toujours des courtiers de données. Il y a toujours d'autres acteurs en arrière que l'utilisateur final ne voit pas forcément. Et donc les données personnelles circulent, et il faut quand même clarifier le rôle de chacun et la responsabilité de chacun. L'Union européenne a répondu à cette question en créant un nouveau statut de sous-traitants de la donnée et en les rendant responsables au même titre que les responsables de traitement.

Et donc je pense qu'il faut avoir cette réflexion-là. Je ne sais pas si c'est forcément le modèle pour le Québec, mais, en tout cas, tenir compte de tout l'écosystème, et de rendre chacun responsable, et avec des sanctions fortes, hein, des sanctions pécuniaires en particulier, et doter, encore une fois, la Commission d'accès à l'information du Québec de ces pouvoirs de sanction et de ces ressources financières, toutes ces mesures iraient vraiment dans le bon sens, je pense.

Mme Nichols : Merci.

Le Président (M. Bachand) : Merci beaucoup. Mme la députée de Saint-Laurent, s'il vous plaît.

Mme Rizqy : Merci beaucoup. Bonjour. Merci d'être parmi nous. Le fédéral a commencé avec Alerte COVID en mentionnant la chose suivante, c'est qu'elle était totalement confidentielle et totalement anonyme, et le commissaire à la vie privée, le 31 juillet, rectifiait le tir en disant que c'était inexact. Partagez-vous le même avis?

Mme Castets-Renard (Céline) : Oui, je partage cet avis et je pense que c'est la différence entre les données pseudonymisées et anonymisées, comme je le disais tout à l'heure. Bien sûr que des précautions sont prises, et qu'on parle de code, et qu'on ne parle pas de l'identité des personnes, et qu'on parle même de mesures de chiffrement, mais il est toujours très difficile, et je pense que tous les spécialistes de la sécurité vous le diront, de garantir l'anonymat parfait et la sécurité parfaite et garantir que...

Mme Rizqy : Mais je vais aller vers le consentement, si vous me le permettez, parce que le temps file. Je vais aller vers le consentement, étant donné que, lorsqu'on a le premier ministre du Canada qui affirme quelque chose qui peut être erroné, la population... Lorsqu'on parle de consentement, il faut que ça soit libre et éclairé sur de l'information juste. Est-ce qu'on devrait tous faire très attention dans notre choix de mots et vraiment s'assurer que les gens comprennent que ce n'est pas totalement confidentiel et pas totalement anonyme? C'est bien ça?

• *(11 h 20)* •

Mme Castets-Renard (Céline) : Alors, je ne veux pas rentrer dans un débat politique, vous vous en doutez, mais je pense qu'effectivement le choix des mots est important, et surtout l'explication derrière les mots, parce que, quand je dis «pseudonyme», «anonyme», je ne suis pas sûr que ce soit clair pour l'ensemble de la population, donc.

Mme Rizqy : Je partage le même avis que vous là-dessus. Dites-moi, le fédéral a aussi commencé la discussion en disant qu'il ne considérait pas que l'information était un renseignement personnel, et ça, ici, il y a une distinction très claire, c'est que, lorsqu'on ne catégorise pas ce type d'information comme un renseignement personnel, bien, à ce moment-là, les cadres juridiques ne peuvent pas trouver d'application. Vous avez mentionné qu'en Europe ça fait déjà 25 ans que même les données qui peuvent être... permettre la réidentification, mais même le croisement de données en d'autres mots, étaient jugées, en Europe, depuis maintenant plus de 25 ans, comme un renseignement personnel. Est-ce que le Canada et le Québec devraient emboîter le pas à l'Union européenne?

Mme Castets-Renard (Céline) : Je pense vraiment, très sincèrement, que le Québec devrait y réfléchir sérieusement. Alors, est-ce que c'est exactement cette définition qu'il faut retenir? Pas nécessairement, mais, en tout cas, il

faudrait essayer d'intégrer ces nouvelles pratiques qui, bien, sont l'utilisation des données aujourd'hui. C'est exactement ces pratiques-là. Donc, il faut bien en tenir compte, je pense. Et, quand je parle d'un cadre légal robuste, c'est aussi un cadre légal adapté aux technologies d'aujourd'hui.

Mme Rizqy : Merci. Et on regarde beaucoup ce que le gouvernement fait, mais j'aimerais aussi m'attarder sur ce que l'industrie fait en parallèle. Plusieurs ont développé leurs propres applications et même maintenant leurs propres bracelets. Le projet de loi n° 64 n'est pas encore étudié, n'est pas encore appelé à l'étude. Pensez-vous qu'on devrait, à l'instar de ce qui a été discuté hier par la Commission d'accès à l'information, même si on n'a pas un projet de loi, à tout le moins avoir un décret pour dire : Calmez-vous, l'industrie, voici maintenant un cadre dans l'attente d'un projet de loi? Pensez-vous que ce serait une avenue qui serait souhaitable, d'agir vraiment rapidement, d'avoir ce décret?

Mme Castets-Renard (Céline) : Si on veut agir dans l'urgence et se concentrer sur les applications de notification de contact, oui, il faut un cadre. Alors, comme Mme Poitras disait hier, un cadre légal serait préférable, mais un décret suffirait, à l'évidence, d'un point de vue juridique. Et, pour vous donner l'exemple de la France, StopCovid a fait l'objet d'un décret.

Mme Rizqy : Ah! merci beaucoup. C'est tout le temps qui me restait.

Le Président (M. Bachand) : Merci beaucoup. M. le député de Gouin, s'il vous plaît.

M. Nadeau-Dubois : Merci, M. le Président. Bonjour. Bonjour, professeure. Merci d'être avec nous en cette fin d'avant-midi. J'ai peu de temps. Je vais aller droit au but.

Vous avez formulé certaines de vos revendications puis de vos remarques, là, ici, en disant : Si le gouvernement va de l'avant, il faudrait mettre tel garde-fou, telle précision, tout ça. Par contre, officiellement, c'est ce qu'on nous dit, la décision n'est pas prise. Donc, il y a encore moyen, je pense, puis c'est encore pertinent, de se questionner sur la pertinence de même aller de l'avant avec une telle application, puis c'est sur ce terrain-là que j'aimerais vous amener. Jugez-vous qu'en ce moment le cadre juridique québécois est adéquat pour protéger les droits et libertés des Québécois, Québécoises, advenant le déploiement d'une application pour lutter contre la COVID-19?

Mme Castets-Renard (Céline) : Sous réserve d'avoir un décret, comme on vient de le dire, oui, parce que même le cadre français, qui est un cadre relativement récent et relativement robuste avec le règlement général de protection des données, au niveau de l'Union européenne, plus la loi informatique et de libertés... On a quand même dû ajouter un décret parce qu'il y a quand même des spécificités liées au déploiement de ce type d'application. Donc, il me paraîtrait vraiment souhaitable de renforcer ce cadre légal sans même considérer une éventuelle réforme des lois.

M. Nadeau-Dubois : O.K., mais ma question, c'était : Est-ce que le cadre actuel est adéquat?

Mme Castets-Renard (Céline) : Bien, a fortiori... Enfin, a contrario, non, et je pense qu'effectivement il faudrait un décret pour accompagner l'application.

M. Nadeau-Dubois : Iriez-vous jusqu'à dire que, pour vous, c'est un peu une condition à ce qu'une telle application soit respectueuse de la vie privée?

Mme Castets-Renard (Céline) : Disons que le décret permettrait justement d'intégrer dans un cadre légal clair et précis les contraintes et les conditions que j'ai posées dans la balance des intérêts et que les autorités de protection des données, hein, le commissariat à la vie privée du Canada, le commissariat de l'Ontario, et la Commission d'accès à l'information du Québec posent, et puis toutes les autorités partout au Canada... Les positions de nécessité, finalité, proportionnalité, etc., il me paraîtrait souhaitable que ces conditions-là soient posées dans un décret, en effet, et contrôlées par la commission.

M. Nadeau-Dubois : Quelques intervenants, notamment la Commission des droits de la personne, la Commission d'accès à l'information, sont venus nous dire qu'à l'heure actuelle il n'y a rien dans les lois québécoises qui interdirait à un employeur ou à un locateur d'exiger qu'un locataire ou un employé télécharge et utilise l'application. Comment vous réagissez quand vous entendez de tels témoignages?

Mme Castets-Renard (Céline) : Alors, pour être tout à fait claire, je ne suis pas du tout spécialiste de droit du travail. Donc, il faudrait quand même regarder si, en droit du travail, il n'y a pas des contraintes par rapport aux informations que l'employeur a le droit de collecter sur ses salariés. En tout cas, si je fais le parallèle avec ce que je connais ailleurs, en particulier en France, l'employeur ne peut pas collecter des données de santé qui n'ont pas un lien direct avec son travail.

Donc, par exemple, très clairement, si vous contractez la COVID, mais que vous êtes en télétravail, vous n'êtes pas un danger pour l'entreprise et pour vos collègues. Donc vous n'êtes pas... Vous ne serez pas obligé de le signaler, par exemple. En revanche, si vous présentez des symptômes et que vous arrivez au travail, vous avez l'obligation de vous protéger, et de protéger les autres salariés, et l'employeur lui-même a l'obligation de protéger. Donc, il peut vous demander un certain nombre de renseignements.

M. Nadeau-Dubois : Mais ça, c'est... Là, vous parlez du cadre juridique français, actuellement.

Mme Castets-Renard (Céline) : Oui. C'est pour vous donner... faire une analogie, parce que... pour vous dire que, les solutions, on les trouve en droit du travail. Je ne suis pas du tout une spécialiste de droit du travail. Donc, c'est pour ça que je vous dis : Il faudrait regarder quand même si, en droit du travail, l'employeur n'est pas limité dans la collecte d'information.

M. Nadeau-Dubois : Merci. Diriez-vous que vous êtes... Prenons comme exemple l'application fédérale. Diriez-vous que le gouvernement fédéral a procédé dans les règles de l'art et de manière adéquate au niveau du respect de la vie privée dans le déploiement de son application? Est-ce que tout a été bien fait? C'est ça, ma question.

Mme Castets-Renard (Céline) : Je dirais que, compte tenu des technologies... enfin, des propositions du marché que nous avons en ce moment... Je ne les connais pas toutes et je suis loin de pouvoir faire le point, mais, en tout cas, par rapport aux différents critères qui ont déjà été signalés, GPS, Bluetooth, centralisé, décentralisé, le gouvernement fédéral a pris toutes les mesures possibles pour avoir la moins pire application, comme il a déjà été dit.

M. Nadeau-Dubois : Parfait. Merci beaucoup.

Le Président (M. Bachand) : Merci beaucoup. M. le député de René-Lévesque, s'il vous plaît.

M. Ouellet : Merci beaucoup. Merci. À mon tour de vous saluer directement d'Ottawa.

Vous avez parlé dans votre mémoire, à la recommandation 3, de faire attention, à savoir que, si on faisait un retour en arrière, il y aurait un coût à ça. Et j'aimerais avoir l'échange suivant avec vous. Le gouvernement n'a pas fait sa niche encore. En tout cas, c'est ce qu'il nous dit. Il n'y a pas de décision qui a été prise. En début de consultation, il y a des fuites dans les médias qui nous ont rapporté que, lors de la consultation Web, 17 000 personnes qui ont participé, 12 000 personnes semblaient être enclines à télécharger cette application. Lorsqu'on écoute d'autres entrevues aussi du ministre de la Transformation numérique ici, au Québec, il semblerait que le gouvernement va y aller par sondages aussi pour aller voir si, effectivement, il y a de l'appétit au Québec...

Mais, quand je lis votre mémoire, ce que vous nous dites... Même si le gouvernement juge qu'il y a suffisamment d'intérêt pour la lancer et... excusez-moi l'expression anglophone, mais gamble sur le fait qu'il y ait plusieurs personnes qui pourraient la télécharger, ce que vous nous dites, c'est : Faites attention avant de la lancer, parce qu'une fois que c'est fait et que, si, au final, comme d'autres pays ailleurs, on décide, après une semaine, deux semaines, de reculer, il y a un coût à ce recul. Et peut-être que, lorsqu'il viendra le temps d'adopter une technologie qui sera beaucoup plus fiable, beaucoup plus utile et nécessaire pour lutter peut-être... pour une autre crise sanitaire, notre population aura été fragilisée par rapport à cette situation-là. Et, dans ce temps-là, on va nuire ou on pourrait nuire, dans le futur, au déploiement d'une technologie beaucoup plus fiable, beaucoup plus sûre, beaucoup plus appropriée et acceptée. C'est ce que vous nous dites dans votre mémoire. C'est bien ça?

Mme Castets-Renard (Céline) : Oui, c'est ce que je dis. Et je ne suis pas sociologue, mais la mémoire collective et la mémoire positive, comme négative, peut jouer parfois en défaveur de nouveautés.

M. Ouellet : Donc, comme législateurs, ce que vous nous dites, c'est : Il n'y a pas de certitude qui existe, mais, avec les indications que vous avez ici, collectivement, en consultations, avec tout ce qu'on a entendu, si vous avez un doute, faites attention, parce que, si vous faites un pas par en avant, le pas subséquent que vous devriez peut-être franchir ultérieurement ne pourrait jamais être franchi parce que la population ne vous suivra pas.

Mme Castets-Renard (Céline) : Ça pourrait arriver. Effectivement, je pense que c'est une grande responsabilité que de décider de déployer ce genre d'outil. C'est loin d'être neutre.

M. Ouellet : Donc, il y aurait une banalisation de la technologie. Mais aussi vous faites référence à cette fracture numérique qui fait que, si le gouvernement va de l'avant avec cette technologie et qu'il y a des gens qui n'en ont pas accès, ils seront laissés de côté. Pensez-vous que, pour le futur, si on déploie encore d'autres technologies pour une deuxième fois, ces populations-là auront l'impression d'être laissées de côté, et donc, effectivement, il y aura un clivage et, malheureusement, pas une adhésion totale à toute autre mesure qui pourrait être influencée par le gouvernement et être mise de l'avant?

• *(11 h 30)* •

Mme Castets-Renard (Céline) : Oui, oui. Je pense qu'il faut probablement travailler d'abord ces questions d'acceptabilité sociale, cette pédagogie, avec la technologie, de manière générale, et d'inclusion avant même, finalement, d'avoir une technologie et un usage à évoquer en particulier. Je pense, ça me paraîtrait assez intéressant d'être proactif plus que réactif.

M. Ouellet : Merci.

Le Président (M. Bachand) : Merci beaucoup. Alors, Mme la professeure, merci beaucoup d'avoir participé à la commission. Et je vous souhaite, au nom de la commission, deux choses : un bon week-end et une bonne fin de quarantaine. Alors, merci beaucoup de votre participation. À bientôt. Merci.

Mme Castets-Renard (Céline) : Merci beaucoup. Merci à vous. Au revoir.

Le Président (M. Bachand) : Alors, je suspends les travaux quelques instants. Merci.

(Suspension de la séance à 11 h 31)

(Reprise à 11 h 43)

Le Président (M. Bachand) : À l'ordre, s'il vous plaît! La commission reprend ses travaux. N'oubliez pas que vous avez le système d'interprétation, de traduction instantanée.

Alors donc, il me fait plaisir, au nom de la commission, d'accueillir Mme Guliani à la commission ici. Alors, bienvenue à la commission. Comme vous savez, vous avez 10 minutes de présentation, et, par après, nous aurons un échange avec les membres de la commission. Les membres de la commission sont libres de parler français ou anglais, à leur besoin. Alors, Mme Guliani, merci beaucoup de votre participation, et je vous cède la parole. Merci.

Mme Neema Singh Guliani

(Visioconférence)

Mme Singh Guliani (Neema) : Great. Thank you so much for having me. Thanks for the opportunity to present on behalf of the American Civil Liberties Union.

The American Civil Liberties Union is a U.S. based nationwide organization. We have more than 3 million members, activists and supporters that work to preserve individual rights and liberties. We're also a member of the International Network of Civil Liberties Organizations, where we also work with the Canadian Civil Liberties Association.

COVID-19 has upended the lives of millions, resulting in hundreds of thousands of deaths worldwide and severe economic toll. And, to address these challenges, many governments are considering exposure notification apps or contact tracing apps, with the hope that they'll help combat the pandemic. However, right now, we don't know whether these contact tracing apps are practical, will work and will be worth the trade-offs.

First, there's the question of the technology itself and whether it can accurately track when someone is at risk of being infected with COVID-19. This is still very much an open question, but, even if we overcome the technical hurdles, there are still other barriers. Individuals must have the trust and confidence to use an app for it to be effective, and there must be a comprehensive public health infrastructure in place that meets the needs of those most vulnerable. For example, what good is an exposure notification alert if someone can't stay home from work, can't get a COVID-19 test and can't self-isolate? And how useful will an app be if those most likely to be infected don't have the smartphone to download it?

Given these issues, at the ACLU, we believe that we must approach the deployment of any app with caution to ensure that it does not inadvertently make things worst. My written briefing provides more information about the necessary safeguards that must be adopted as part of any contact tracing app, but I want to highlight five in particular that are very critical.

One, any deployment of an app must be accompanied by clear benchmarks for efficacy that are evaluated independently and reflect public health and civil liberties expertise. Globally, we have already seen the deployment of technologies that have had questionable efficacy.

For example, in the U.S., an app deployed in Utah, that was intended to help ensure that individuals entering the State of Utah quarantined, was shut down after just 72 hours because it was sending alerts mistakenly to the wrong people. The app wasted thousands of dollars and created confusion for the public. In North Dakota and South Dakota, a Care19 app, which relies on location data, was found to be sending personal information to private companies and reportedly has yet to identify a single asymptomatic carrier. Similarly, in Australia, local health authorities have said that the country's COVID app has yet to identify otherwise unknown contacts, though some have suggested that it's due to the country's low coronavirus rate.

Given these examples, it is positive that, in Canada, there's an external advisory council that can help... metrics to assess the efficacy of the proposed COVID Alert app. If this app does not meet these metrics, it should be discontinued or modified accordingly. In addition, these metrics must be fully transparent and include an analysis of not just whether the technology works, but whether it meaningfully contributes to positive health outcomes. For example, it should measure whether individuals who had not otherwise have been notified or... and it should also assess whether these individuals do, in fact, take steps to prevent further spread of the disease.

Two, it's essential that additional health resources be targeted specifically at vulnerable communities, including those who may not be able to use an app. The consequences of COVID-19... disproportionately on already vulnerable communities. For example, for Ontario, studies have found a strongest association between high coronavirus rates and low-income conditions of work, visible minority status and low levels of education. This mirrors data in Montréal, which shows that immigrants, refugees and lower income individuals live amongst the hardest hit regions. It also reflects our experience in the U.S., where Blacks and Hispanics are dying at a disproportionate rate.

We ignore these vulnerable populations at our own peril. Examples in Singapore and the United States offer a cautionary tale about ignoring the public health of particularly high-risk communities. For example, in Singapore, a resurgence of infections earlier this summer was driven in part by poor conditions in migrant communities, where

individuals face difficulties social distancing and where there was not large scale testing. Similarly, in the United States, public officials have warned that failing to take steps to address spread in jails and prisons could results in 100,000 more deaths than already projected.

Already vulnerable communities are also the ones who may be unable to use an app. For example, in Canada, only 74% of households of incomes less than $20,000 and only 80% of individuals over 60 report having a smartphone, and even smaller numbers of these populations may have a smartphone that is actually capable of operating a contact tracing app. Thus, to insure these populations are not left out of any solutions, it's essential that there be a broader manual contact tracing and health plan targeted at providing health resources to these communities. In addition, there must be investments to provide technical and other systems to people who seek to use this technology.

Three, it is essential that any app deployed minimizes the collection of personal data, and the use of such data should be limited to public health. The best way to insure limited data collection use is through the design of the app itself. On this... positively, this COVID Alert app cannot collect detailed location data of users. Collection of GPS location data is not accurate enough for contact tracing and poses significant privacy risks. Instead of location data, the COVID Alert app collects random user ID's that can be used to notify someone who may have come in proximity with an infected individual. Provinces should further commit to minimizing the collection of personal data by not requiring individuals to provide any additional information as a condition of using the app. They should also insure that any data, like IP addresses, are not retained by the government.

• *(11 h 50)* •

There must also be clear safeguards to ensure that any data collected is not used for punitive purposes, like criminal or immigration enforcement. Reports like those in Ontario, where lists of infected individuals were provided to the police, are already cause for concern, and such concerning practices should not be extended to data collected through a contact tracing app. Moreover, any data that's collected should be promptly destroyed when it's no longer epidemiologically useful for contact tracing purposes. And it's also important that individuals have a mechanism to enforce their rights and seek redress in cases where such restrictions are not followed or the app doesn't work as promised. There may be the need for additional legislation to provide these enforceable rights.

Four, as the World Health Organization has advised, any use of an app should be completely voluntary. Public health experts have found that coercive health tactics often backfire, sparking counterproductive efforts to resist and undermine health outcomes. For contact tracing in particular, voluntariness is essential. We want individuals to work with public health authorities to fill in the blind spots from digital data. For example, we want people to provide contacts they may have had when they were not carrying a phone or provide information about when they may have been wearing protective gear, and thus were unlikely to transmit the disease.

Given this, for any app to have efficacy, it is essential that it be completely voluntary. At a practical level, what this means is the Government will have to make clear that employers, landlords, business owners and others cannot make use of an app in condition of employment, tenancy, public benefits or access to basic necessities, like visiting a grocery store. These restrictions have to be accompanied by appropriate channels for individuals to lodge complaints and obtain redress in cases where these entities do not comply with these limitations.

Finally, it's critical that details related to an app be completely transparent and accompanied by robust oversight. Public release of the source code for Canada's alert app is a strong first step and a good model. In addition to this, however, any memorandums related to how the apps are being deployed in specific provinces should also be released, along with the result of audits and copies of information sharing agreements. Moreover, there needs to be more clarity about who will be primarily responsible for conducting oversight on an ongoing basis to make sure that policies are followed, benchmarks are met, and that the app is being integrated into a broader public health strategy.

Given the seriousness of the pandemic, we should surely not dismiss outright any technology that might help. But, given the uncertainties, it's critical that any deployment of an app be accompanied by strong safeguards or we risk both compromising our liberties and undermining existing public health efforts. So, I look forward to answering any questions that you may have.

Le Président (M. Bachand) : Merci beaucoup pour votre présentation. Alors, la période d'échange débute avec le député de Chapleau. M. le député, s'il vous plaît.

M. Lévesque (Chapleau) : Merci, M. le Président. Bonjour, Mme Guliani. Merci beaucoup d'être avec nous aujourd'hui. Quelques petites questions.

D'abord, peut-être un petit rappel sur, disons, ce qui est envisagé ou ce qui est discuté, là, en termes de principes, autour de l'application. Bien entendu, là, elle serait gratuite. Elle serait faite sur une base... installée sur une base volontaire des citoyens. Il n'y aurait pas de géolocalisation GPS ni de recours à la biométrie, si jamais c'était envisagé par le gouvernement. Et l'application, bon, fonctionnerait certainement avec... sûrement avec l'application Bluetooth, la technologie Bluetooth, décentralisée, pour qu'il n'y ait pas justement de stockage de données ou de collecte d'informations personnelles, avec évidemment une volonté de protéger la vie privée et les renseignements personnels de la population québécoise.

Une question pour vous. En termes de... Donc, vous avez dit qu'effectivement il y a certains groupes qui ne pourraient pas avoir accès à l'application, bon, parce qu'ils n'ont pas la technologie nécessaire, ou le téléphone, ou quoi que ce soit. Est-ce que, pour vous, par contre, puis, peut-être, avec l'expérience américaine, vous allez pouvoir nous éclairer, il y a eu justement certains groupes qui ont pu la télécharger, et il y a eu, à ce moment-là, des gains ou il pourrait y avoir des gains justement sur le fait qu'on réussit à tracer une ou deux personnes qui auraient la COVID-19? Et ces personnes-là ne viendraient pas nécessairement infecter d'autres personnes même si... Donc, globalement, socialement, la société pourrait bénéficier de ça. J'aimerais peut-être avoir un peu votre opinion puis votre perception par rapport à ça.

Mme Singh Guliani (Neema) : So, within the U.S., we don't have a nationwide app. Each State is sort of deciding on their own about how they will deploy apps. And we don't have a State yet that's had an app that has been widely adopted and where we can say with certainty that it has had a positive effect in helping to track the disease. That is very similar, I think, to the experience globally, where, even in countries where there has been broader adoption, we simply don't have the data yet to know whether it's actually had efficacy, because efficacy is not just whether the technology works, it's also whether people actually take action in response to an alert.

And so something public health officials have said is they're not sure whether people will actually take action when they receive an alert on their phone or whether they may receive so many, for example, that they ignore it. And so one of the reasons I think that metrics and benchmarks are so important is that we still don't know whether these apps will actually work and whether they'll be worth the money and the effort that is used to deploy them. And, given that we know for a certainty that many people will not be able to take advantage of them, it must be integrated into a broader health strategy that addresses particularly vulnerable communities.

M. Lévesque (Chapleau) : Donc, si je comprends bien, vous dites que ça pourrait être un outil qui s'ajouterait à d'autres mesures sanitaires qui seraient, dans le fond, déployées par la Santé publique. Est-ce que c'est bien ça que je comprends?

Mme Singh Guliani (Neema) : Yes, so, I guess I would say a couple of things.

One is that it must be integrated into a broader public health strategy and it shouldn't be diverting resources from manual contact tracing efforts. One of the concerns that has come up and has been raised in the United States is this idea that, you know, we'll focus all of contact tracing through these digital mecanisms, and that will leave out many people. So it shouldn't supplant manual contact tracing.

And then, too, you know, this should be looked at as something that may have possible efficacy, and looked at closely. It may turn out that, once we look at the data... it turns out that the health benefits are marginal or nonexistent. And, if they are marginal or nonexistent, then the app should be discontinued.

And then, finally, certainly, it has to, you know, be pushed out along with other health resources. As I mentioned it, it's not very good for someone if they receive an alert, but they still have to go to work, and they don't have access to testing, and they don't have access to a place where they can self-isolate. So, at a practical level, for it to be helpful, we also need to make sure that all of those other health resources are being provided.

M. Lévesque (Chapleau) : Merci. Peut-être, en lien avec les lois, justement, sur la vie privée puis les renseignements personnels... peut-être nous faire une petite présentation ou nous brosser le portrait, si jamais vous être capable de le faire, là, aux États-Unis, si ça a été considéré, justement, dans certains États ou dans tous les États qui ont décidé de mettre en place une application. Est-ce que ces lois-là ont été, disons, considérées, appliquées? Est-ce que ça a été important pour ces États-là? Et, si c'est le cas, peut-être nous donner la marche à suivre qui a été faite, parce qu'évidemment on veut offrir, si jamais le gouvernement voulait aller de l'avant avec l'application, la plus grande protection possible sur la vie privée et les renseignements personnels.

Mme Singh Guliani (Neema) : Well, in the U.S., there was a national privacy legislation proposed to address COVID-19 specifically, but that legislation has not passed. In order to protect personal data, you know, I would recommend a couple of steps.

One is... a positive aspect of the COVID Alert model is that it does minimize data collection, right? We're not collecting location data and GPS data, which is a good thing. I would also encourage provinces who move forward to also not require individuals to, for example, provide demographic data or contact data as a condition of using the app or downloading the app. So minimize the data collection... something that's very important.

Two, robust safeguards to make sure that even the minimal data that is collected is, you know, not retained for more than, you know, 30 days, or two weeks, or the minimum amount of time that is necessary for contact tracing purposes, and limits to make sure that that data is not used for anything other than public health.

And then, finally, what I'll say is, you know, having an independent, you know, overseer who's looking at this on an ongoing basis. What we've seen in other contexts with technology in the U.S. is, often, there are policies and plans, and those policies and plans aren't always followed. And, so, having an independent oversight mechanism to make sure that data is being secured, is being, you know, deleted appropriately and is not being shared is essential to give the public the confidence to even download and use the app. What we don't want is a situation where people are afraid to use it because they're worried about their privacy and their civil liberties concerns.

• *(12 heures)* •

M. Lévesque (Chapleau) : Merci. Une petite dernière question. Vous avez parlé des tiers, justement, qui pourraient, bon, exiger, pour pouvoir accéder à un service, ou à un commerce, ou même, dans le fond, un employeur qui exigerait l'application, est-ce que vous avez vu de telles pratiques aux États-Unis, dans les États où il y avait déploiement d'une application? Donc, un employeur aurait refusé justement à un travailleur d'accéder à son lieu de travail parce qu'il n'avait pas l'application. Et il y a eu d'autres groupes qui sont venus nous parler d'une possibilité, peut-être, d'un décret et de, donc, un changement législatif par rapport à ça pour justement protéger la vie privée et, justement, la possibilité que les tiers, dans le fond, retirent la fonction volontaire de l'application.

Mme Singh Guliani (Neema) : So I lost connectivity for a moment, but I think what you were asking is about requirements from employers. Did I get that right?

M. Lévesque (Chapleau) : ...question des tiers. Donc, est-ce qu'il y a des exemples aux États-Unis où est-ce qu'il y a un employeur aurait interdit justement à un employé de pouvoir accéder à son lieu de travail sans avoir l'application?

Mme Singh Guliani (Neema) : One of the things that has not happened in the U.S. that is necessary is for, in a space that... you know, employers, landlords and others requiring use of the app as a condition of, let's say, a job or entering your grocery store. We haven't seen widespread requirements for mandatory use of an app just because we haven't seen, you know, widespread deployment of an app in the United States.

In other countries, we have seen that. So, for example, in places like India, using the metro and other things, you know, people have required... download an app. I'm generally concerned about any sort of mandatory regime, both because we really need individuals to participate in a contact tracing effort for it to be successful, and what public health experts have advised is that, when you make something mandatory and you make it coercive, you know, public willingness to participate and provide accurate data is minimized, and that's what I think we don't want.

And, so, I would say, if you do choose to move forward with an app, it's important to consider policies and laws that discourage employers and others from making use of an app mandatory, because I suspect that what that will do is undermine your broader public health efforts by engendering distrust among the population.

M. Lévesque (Chapleau) : Merci beaucoup.

Le Président (M. Bachand) : Merci. Mme la députée de Jean-Talon, s'il vous plaît.

Mme Boutin : Bonjour, Mme Guliani. Merci beaucoup de votre présence. J'aime beaucoup plusieurs de vos recommandations qui vont quand même dans le sens de plusieurs experts, d'ailleurs. Pour rebondir rapidement, là... Le caractère volontaire de cette application-là est très important, et puis je pense que tout le monde a pris en considération, là, le risque d'avoir des tiers ou un employeur qui force un employé à «downloader» une application, là. Personne n'est pour ça, je crois.

J'ai une question par rapport à ce que vous avez dit par rapport au traçage manuel. Peut-être que l'expérience américaine, sur certains États, a déjà des données ou peut-être pas, mais on se pose toujours la question de l'utilité de la technologie au service de la santé publique, parce que la technologie ne va pas remplacer le traçage manuel. Puis est-ce que vous croyez que, potentiellement, un outil technologique comme une application pourrait avoir un effet positif pour contribuer, dans le fond, à faciliter le travail manuel de collecte de contacts, d'identification de contacts, et pas de remplacer, mais peut-être rediriger certaines de ces ressources humaines là vers des populations qui n'ont pas accès à la technologie ou qui sont plus vulnérables? Est-ce que vous croyez que ça pourrait potentiellement avoir un effet positif et est-ce que... Si oui, est-ce qu'il y a des exemples concrets ou pas encore?

Mme Singh Guliani (Neema) : We really don't know yet, right? So we don't know whether the apps will actually be useful or, for example, whether they'll lead to a lot of false notifications that actually waste health resources because you'll have people quarantining or seeking testing when, in fact, they don't need that... we have right now is really one of the reasons why investments... we know work, like manual contact tracing, are important... we'll need those manual mechanisms. It's not a replacement to get information on your phone versus having an individual talk to a health professional, receive information about how to get testing or how to receive health access. What we're hearing from public health professionals is that there's just a difference in the individual response when they're faced with an electronic notification versus an actual human contact where they can get the help they need. And so, you know, the hope is that these apps will help, but we just don't know whether they will, in fact, prove to be fruitful or whether they'll waste health resources.

Mme Boutin : Et, selon votre expérience, est-ce que vous savez si d'autres technologies à travers les juridictions à travers le monde sont disponibles pour faciliter le travail de la Santé publique puis mieux contrer la pandémie ou est-ce qu'on est mieux de se concentrer seulement sur les méthodes traditionnelles?

Mme Singh Guliani (Neema) : So there are various technologies that have been proposed, right? There's examples where different governments have tried to put out information to help people assess their own symptoms, like symptom trackers. There have also been, for example, in Rhode Island and also in Singapore, efforts that would... have apps that would let somebody, you know, store their location data and then, if they were, in fact, infected, they could voluntarily choose to provide that information to a public health authority.

So there are things that may help and may augment manual methods and may augment, you know, different public health mechanisms, but, I would say, with all of these proposals, there really isn't solid data. And we need metrics to assess the trade-off because all of this requires resources, and we want to make sure that these resources are actually going to the most high-risk populations. And a challenge with technology writ large is, often, the most high-risk populations are not the ones who are going to have access to technology. And so that, I think, is one of the challenges with using technology. I'm not saying that we should ignore it. I'm not saying we shouldn't look at it. We should just be really practical about what it can actually help with and what its gaps are going to be.

Mme Boutin : Je comprends très bien. Vous venez de mentionner l'importance des indicateurs de mesure. Est-ce que... J'imagine, malgré qu'il n'y a pas d'étude encore sortie, qu'il y a des juridictions... certains pays sont en train de mesurer ou ont mesuré avec des indicateurs l'efficacité de ces technologies-là et même l'atteinte à la vie privée. Est-ce

qu'il y a déjà du «benchmark», excusez l'anglicisme, là, des indicateurs... I could switch in English, but I'm in Québec, so I prefer to speak in French. Est-ce que vous savez s'il y a déjà des indicateurs de performance pour mesurer l'efficacité de ces applications-là, de certaines juridictions, qui pourraient inspirer le Québec avant même de la mise en place... avant même le développement d'applications?

Mme Singh Guliani (Neema) : So there haven't been standard benchmarks that have been widely accepted, that have been put out. I think there are various things to measure. One is the technology itself. There has been some analyses that suggest that there are just technical challenges, with Bluetooth being sort of used as for proximity. So, for example, whether you have your phone in your pocket affects the signal and may actually affect whether you get a notification.

And so what we need to do is understand the extent of that issue, right, and how much it results in either false positives or false negatives. But that information has to be looked at in the specific context of the overall public health strategy. How does that fit into what the availability of testing might be in a particular region or for particular populations? How does that fit into what the follow-up is? Is it a case where individuals receive an alert? And there's also no public health education that provides information about what an individual should do or... connects them to other health resources.

So I don't have sort of standard benchmarks. But what I would say is that it's a combination of the technology, what people are doing, and what the broader public health infrastructure is providing, and assessing how that applies, and, you know, what you would do instead, what those resources could be used instead for to assess whether it's something that you want to continue encouraging people to use and continue to invest in.

Le Président (M. Bachand) : Merci beaucoup. Je cède maintenant la parole à la députée de Saint-Laurent, s'il vous plaît.

Mme Rizqy : Thank you for joining us, Mrs. Guliani. It's a real pleasure having you with us.

I want to address with you some questions regarding people of color, more specifically the Black Community, but also the Brown-skinned people. Unfortunately, we don't have data here, in Québec, despite the Québec Public Health... said they will collect data to see how people of color are more infected by or more affected by COVID-19. I believe that, actually, the United States... I believe it was in Chicago where you actually conducted a study regarding COVID-19 and the impact on the Black Community. Can you tell us more about that?

• *(12 h 10)* •

Mme Singh Guliani (Neema) : Sure. So particular States have released information and data about what populations are most affected, and, you know, as you've highlighted, it's become very clear in the United States that already vulnerable populations are the ones that are being hardest hit by COVID. So, in certain parts of the United States, for example, the death of Black People is three times their proportion of the population, right? And, in places like New York, we are definitely seeing that Hispanic and African-American communities are hard hit.

You know, it's not 100% clear as to what are the main drivers of these disparities. It's probably a combination of pre-existing health conditions, you know, individuals in those communities potentially having jobs that require them to have more actions that put them at higher risk of contracting the disease, lack of health access and lack of sort of community resources.

And so I think, you know, what we're really seeing is a very complex problem that, in fact, reflected problems that we had before COVID-19, and COVID-19 is shining a light and making all of those existing health disparities and racial disparities... making these things much worse.

Mme Rizqy : Is it fair to say that minorities, especially immigrants, when they come either in the United States or, let's say here, for instance, Québec, they usually don't live in the most expensive neighborhood? They will... more likely to live in a neighborhood with more density. And I can give you an example. Here, in Québec, we have some districts that people... they don't have the Internet. Like, 30% of them with lower income, they don't have access to the Internet. Do you think that the apps can actually help them or, at the contrary, it will actually put them back on the line to be tested?

Mme Singh Guliani (Neema) : So, in terms of immigrant communities, you know, there's obviously very different experiences in the U.S. There are, you know, populations and, you know, high-density populations of immigrants in various cities. I think the challenges of an app, in those contexts, could be significant for a couple reasons.

One, just the technology. So, one of the things we have to assess is how does the technology really operate in a place that's densely populated. So, for example, if you're in an apartment building, I might be in close proximity to you, but we might have a wall between our apartments, and so how does the app operate in those circumstances? Does it provide false positives and false negatives?

The second thing I would say is it's important to assess what are the other health resources being provided to that community. So, if I receive an alert, do I have the economic assistance so that I don't have to go to work and I can self-isolate? Do I have an extra bedroom or an extra place to go so that I'm not interacting with other members of my family or friends who can possibly be infected? Am I sort of already... and have other health issues that may have been untreated, right, diabetes, hypertension, other pre-existing health conditions that have been shown to be correlated with the worst COVID outcomes?

And so, you know, all of those things very much work in tandem, and, with an app, we're layering that on top of the fact that we may be dealing with a situation where high percentages of the people can't even use it because they don't have a smartphone, they don't have connectivity or they have an old smartphone that doesn't operate. And so that's one

of the reasons, I think... Before you deploy the app, these are the questions... There has to be a plan to address these very real problems. Otherwise, you'll just leave large segments of the population out of the solution.

Mme Rizqy : Thank you. I know we invited you regarding the app, but I saw you in front of the U.S. Congress about facial recognition and I really want to hear about it, because, right now, the State police, Sûreté du Québec, without any public hearing, without any public consultation, decided to go ahead and to buy the application with facial recognition. Can you tell us what are your concerns about it?

Mme Singh Guliani (Neema) : There are significant concerns with facial recognition, both in terms of individuals' right to free speech, also their privacy concerns.

So, as an initial matter, you know, what you're describing that occurred in Québec is similar to what happened in the United States, where we had... a lot of police departments deployed facial recognition. They didn't receive authorization from their legislature. They didn't, you know, require a public consultation or comments to talk to those communities most impacted. And the result of that process has become very clear.

Number one, the technology, even in the most recent studies, has been shown to be definitely inaccurate on certain subgroups, so individuals with darker skin, women. It doesn't work as well on people who look like me versus, for example, a light-skinned male. You know, the ACLU represented an individual named Robert Williams, who was actually mistakenly arrested in part because of an error with face recognition, and he only found out that face recognition was used, in his case, really on accident. The police let it slip, when they were interrogating him, that they had used face recognition.

So there's very real consequences, but, even beyond the accuracy, let's say the technology was, in fact, accurate, which it's not, there are also fundamental concerns about the effect that it has on the population writ large. I mean, it's the power, for the Government, to track an individual as they go to a protest, as they go to a doctor, as they go to a place of worship, and that's something that communities are very concerned about. And we've actually seen those deployments in concerning ways. In the most recent protests, we've seen reports of face recognition as being used at protests to identify individuals. In Baltimore, years ago, police were found to be looking at pictures posted to social media of a protest, you know, protesting police brutality. The police were looking to identify individuals so that they could be arrested.

And so those raise fundamental concerns about whether the technology is being used in a way that violates First Amendment rights and really creates a situation that is not tenable for the public. And, you know, I think also, increasingly, we're thinking about face recognition in the U.S. in the context of broader policing problems, and really seeing surveillance and face recognition as part of the problem with overpolicing, and a need to shift those resources to, you know, other types of interventions that can help, you know, prevent crime and also to enhance public safety for all communities.

Mme Rizqy : Do you believe that facial recognition can actually replicate systematically more bias issues and discrimination?

Mme Singh Guliani (Neema) : Absolutely. I mean, we can't look at the technology in isolation. We have to consider the technology based on who is going to be using that technology. And, in the United States, there are systemic and historical discrimination built into policing systems. You know, African-Americans are more likely to be shot by the police. They're more likely to be stopped by the police and they're more likely to be arrested by the police. And so we can't pretend that those historical problems don't exist. You know, what face recognition does is provide the opportunity to supercharge and to enhance those existing biases and those existing problems. And so we very much have to look at not just, you know, the data, how the technology might work in perfect conditions, but how they will work in real life, given the existing problems with policing.

Mme Rizqy : I've been following your work for quite a long time now and I just want to say thank you for all the issues that you raise, especially for minority groups. Thank you.

Mme Singh Guliani (Neema) : Thank you.

Le Président (M. Bachand) : Il reste deux minutes. Mme la députée de Vaudreuil, allez-y.

Mme Nichols : Merci, M. le Président. Merci beaucoup. Merci. Bienvenue à l'Assemblée nationale du Québec.

En effet, vos travaux sont très intéressants, très pertinents. Parfois, la distance nous empêche de pouvoir vous suivre. Donc, on doit faire des recherches pour pouvoir s'y connecter. On s'en sert souvent, là, à titre comparatif, puis évidemment on essaie de regarder la législation, mais on sait bien qu'il y a, des fois, là, des milieux qui nous séparent au niveau des comparaisons quant à la législation, mais est-ce qu'en lien, peut-être, plus avec le traçage, moins la reconnaissance faciale... mais est-ce qu'il y a une législation autour de cette application-là et est-ce que c'est une législation détaillée qui prévoit des conséquences?

Mme Singh Guliani (Neema) : Are you asking with relation to the contact tracing apps within the United States?

Mme Nichols : Oui, pas la reconnaissance faciale, avec le... oui.

Mme Singh Guliani (Neema) : So there's no legislation governing use of the app or, you know, privacy specifically with regards to COVID-19. Each State is essentially, you know, charting their own path and no State has passed specific COVID-19 legislation or privacy legislation. So it is a broader problem that we don't have clear guidelines and it's a broader problem that the U.S. still lacks strong data privacy legislation writ large to, I think, address what we're now seeing as very clear privacy problems that have become enhanced during the pandemic.

Mme Nichols : C'est quand même préoccupant qu'il n'y ait pas des normes, là, qui encadrent tout ça. Je vous remercie beaucoup de votre intervention.

Le Président (M. Bachand) : Merci beaucoup. M. le député de Gouin, vous avez la parole. Merci.

M. Nadeau-Dubois : Merci, M. le Président. Hello, Mrs. Guliani. It's a pleasure to have you here, at the National Assembly. I will resume my questioning in French. I find it important for my fellow countrymen here to understand me and follow our discussion.

J'aimerais vous entendre en tant qu'experte des libertés civiles. Dans le contexte où les risques pour la vie privée et les libertés civiles des applications pour lutter contre la pandémie sont bien réels et que les bénéfices, eux, sont non démontrés, voire purement hypothétiques, jugez-vous que, du point de vue des droits et libertés, le jeu en vaut la chandelle et que c'est une bonne décision que de mettre en place de telles applications?

Mme Singh Guliani (Neema) : What I would say is that I think it's important to approach it with a lot of caution. And so, you know, from my perspective, if you are going to consider apps and these technologies, testing them first before you are making a significant investment and widespread deployment is important, and considering what we know are going to be the risks and dangers, right, minimizing the data collection, addressing the privacy concerns, acknowledging the populations that will not benefit and having a strategy to deal with these populations. So I would say testing before widespread deployment and then having those metrics developed on the front end.

• *(12 h 20)* •

M. Nadeau-Dubois : Est-ce que ce serait une bonne idée de les déployer sans les tester auparavant?

Mme Singh Guliani (Neema) : I don't think it's a good idea to deploy it before there has been some sense or some indication that it will have some efficacy and before the policies are in place. But I think the real risk is that, if you don't...

M. Nadeau-Dubois : Merci.

Mme Singh Guliani (Neema) : Sorry.

M. Nadeau-Dubois : Je suis désolé. J'ai très peu de temps. Je vais être obligé de vous bousculer un peu. Ça sera probablement ma dernière question, d'ailleurs. Jugez-vous que de telles applications peuvent avoir comme conséquences d'augmenter les inégalités en matière de santé?

Mme Singh Guliani (Neema) : If the apps are deployed in isolation, without a broader public health strategy, what you do risk is creating those inequities. For example, if you've deployed an app and you didn't have the policies to make sure that an employer wasn't able to force somebody to use the app, what you could end up with is a situation where, let's say, individuals are being coerced into using an app. That's not good for that individual. It's not also good for your broader public health, you know, strategy, when you're trying to get the public to have confidence. So what I would say is those are policies that should be put out concurrently with an app and thought about on the front end to avoid potential negative consequences.

M. Nadeau-Dubois : Thank you very much. Merci beaucoup.

Le Président (M. Bachand) : Merci beaucoup. M. le député de René-Lévesque, s'il vous plaît.

M. Ouellet : ...de vous saluer, Mme Guliani. Vous avez parlé beaucoup de l'importance, effectivement, de l'équité, qu'il y ait un traitement juste, si on déploie cette application, et qu'on ait des services sanitaires qui puissent aller dans les communautés les plus fragiles et ceux et celles... les communautés, pardon, qui sont les plus touchées. Mais la véritable conversation, c'est que, même si on ne déploie pas cette application, cette prémisse de base, de donner du support et du service dans les communautés qu'on sait qui ont été plus touchées, devrait guider les législateurs. Donc, on ne devrait pas attendre nécessairement de déployer cette technologie pour dire qu'en la déployant il y aura une iniquité entre ceux qui y ont accès et ceux qui ne l'ont pas. Mais notre véritable enjeu devrait être plutôt de s'assurer que les communautés qui sont plus fragiles et qu'on sait qui ont été plus contaminées devraient mériter l'attention du gouvernement. Est-ce que vous êtes d'accord avec ça?

Mme Singh Guliani (Neema) : So I lost the audio for a brief moment. I think your question was about provision of services to already vulnerable populations. Did I get that right? I lost it for a couple of minutes while you were speaking.

M. Ouellet : ...résumé très court. Si on doit déployer l'application, vous faites référence à l'importance d'avoir des mesures sanitaires qui seraient déployées dans les communautés les plus fragiles. Or, la véritable question, c'est que, si ne nous déployons pas cette application, ne devrions-nous pas... assurer quand même de déployer des ressources dans les milieux les plus fragiles... et ceux et celles qui, par le passé, par les études qui ont été faites, ont été les plus touchés?

Mme Singh Guliani (Neema) : Yes, I mean, absolutely. What we're seeing with COVID-19 is a need for targeted health resources at high-risk communities, and especially those high-risk communities that have already experienced a disproportionate share of infections and death and that we know are being hardest hit by the pandemic. I think that, with the app, one of the things to think through is how you're going to fit that app into your broader public health system. How does it work? Is it that you have an app, and that's a separate stream, and then you also have manual contact tracers? Is it that manual contact tracers are being diverted to only provide services to maybe people who have been notified through the alert system? That's what you would not want.

And so I think that making sure that those resources are not being diverted from those communities and making sure that there will be particular extra health resources, given that those populations will not be able to use an app, is essential. But, you know, to answer your question, I guess, very shortly, yes, absolutely, we need more health resources targeted at vulnerable communities.

M. Ouellet : Merci beaucoup, Mme Guliani.

Le Président (M. Bachand) : Merci beaucoup, M. le député. M. le député de Chomedey, s'il vous plaît.

M. Ouellette : Mrs. Gulianl, thank you for being with us today, truly appreciated. It's also to give us really good information. I may continue in French also, because, like my other colleague mentioned, we're in Québec.

Vos conclusions, il y a beaucoup de points d'interrogation. Vous avez répété souvent : «We don't know». Il n'y a pas d'études ou de littérature positive sur l'utilisation d'applications comme ça. Et je pense que la confiance du public, la confiance des citoyens dans les décisions de leur gouvernement est très importante. Est-ce que vous êtes d'accord avec moi là-dessus?

Mme Singh Guliani (Neema) : Yes, 100%, public health and confidence in the public health authorities is absolutely essential if we are going to have positive health outcomes.

M. Ouellette : Ce qui est arrivé dans l'État de l'Utah, où le gouvernement a décidé d'aller de l'avant avec une application et de la fermer 72 heures plus tard, croyez-vous que ça peut avoir un impact sur la confiance des citoyens de l'Utah et le désintéressement sur les prochaines mesures gouvernementales?

Mme Singh Guliani (Neema) : I think there are a couple of things that really affect what the public confidence and the public reaction...

One is just the transparency, right, and clear information, and none of this should be hidden. People should know what data is being collected. They should know what's being shared, how it's being shared, and all of that data should be made public. I think that that's very helpful in retaining public confidence.

The second thing I will say is we've heard concern from communities, particularly many high-risk communities, about sharing of information with law enforcement or immigration enforcement authorities. And so I think education restrictions you can have to prevent those fears is very important, because people quite simply won't use an app if they're worried that the information could be funneled to police or other people and could be used against them.

And then, finally, I think it's very important for the public to know, you know, that the Government is making sound decisions. And what helps with that is, you know, not having a situation like Utah, where, clearly, something was pushed out without proper testing, and without proper evaluation, and, frankly, without even the policies in place to make sure that privacy and civil liberties are respected. So, to maintain the public trust, there are things that can be done, but you have to approach things with caution and address the problems on the front end, not the back end

M. Ouellette : Thank you, Mrs. Guliani.

Le Président (M. Bachand) : Merci beaucoup pour votre participation à la commission aujourd'hui. C'est très, très apprécié. Et vous serez toujours la bienvenue au Québec et à Québec. Merci beaucoup.

Mme Singh Guliani (Neema) : Thank you so much. It was my pleasure.

Mémoires déposés

Le Président (M. Bachand) : Merci. Cela dit, avant de conclure les auditions, je procède au dépôt des mémoires de personnes et organismes qui n'ont pas été entendus lors des auditions publiques, soit le mémoire de Mme Maroussia Lévesque, le Barreau du Québec et la Centrale des syndicats du Québec.

Cela dit, le député de Chapleau, vous avez demandé la parole.

M. Lévesque (Chapleau) : Merci beaucoup, M. le Président. J'en comprends qu'il y a eu entente entre les leaders des différents partis politiques, formations politiques, pour que nous tenions une séance de travail à 14 heures cet après-midi. Également, il y avait entente pour remise des observations et recommandations de la part des différents partis politiques. J'ai des copies à remettre de notre parti. Donc, voilà, je ne sais pas si on veut procéder avec la remise.

Le Président (M. Bachand) : Merci beaucoup. Voulez-vous en faire un dépôt officiel?

M. Lévesque (Chapleau) : J'en fais un dépôt officiel.

Le Président (M. Bachand) : Donc, j'autorise le dépôt officiel du document. Est-ce qu'il y a d'autres interventions avant la... Mme la députée de Vaudreuil.

Mme Nichols : Oui, merci, M. le Président. Alors, en effet, là, il y avait une séance qui avait été demandée en vertu de l'article 176 du règlement. Le gouvernement a fixé, là, à cet après-midi, 2 heures, la séance. Et nos recommandations seront faites en séance tenante, là. Il est quand même 12 h 30. Alors, on sera présents à la rencontre de 14 heures.

Le Président (M. Bachand) : Parfait. Merci beaucoup. Alors, c'est noté. La demande est notée. Donc, la commission fera parvenir les détails dans les plus brefs délais.

Cela dit, je vous remercie infiniment de votre contribution. La commission ajourne ses travaux sine die. Merci beaucoup.

(Fin de la séance à 12 h 30)