



ASSEMBLÉE NATIONALE DU QUÉBEC

PREMIÈRE SESSION

QUARANTE-DEUXIÈME LÉGISLATURE

Journal des débats

de la Commission permanente des institutions

Le jeudi 13 août 2020 — Vol. 45 N° 78

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 (2)

**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 jeudi 13 août 2020 — Vol. 45 N° 78

Table des matières

Auditions (suite)	1
Commission des droits de la personne et des droits de la jeunesse (CDPDJ)	2
Commission d'accès à l'information (CAI)	11
M. Benoit Dupont	20
M. Sébastien Gambs	29
M. Mourad Debbabi	38
M. André Mondoux	47
M. Pierre-Luc Déziel	57
Association québécoise des technologies (AQT)	68
M. Steve Waterhouse	77

Autres intervenants

M. André Bachand, président

M. Gabriel Nadeau-Dubois

M. Mathieu Lévesque

Mme Lucie Lecours

Mme Joëlle Boutin

Mme Marwah Rizqy

M. Martin Ouellet

M. Guy Ouellette

M. Luc Provençal

Mme Marie-Claude Nichols

* M. Philippe-André Tessier, CDPDJ

* Mme Marie Carpentier, idem

* Mme Diane Poitras, CAI

* Mme Nicole Martel, AQT

* M. Alain Lavoie, idem

* Témoins interrogés par les membres de la commission

Le jeudi 13 août 2020 — Vol. 45 N° 78

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 (2)

(Neuf heures)

Le Président (M. Bachand) : Bon matin, tout le monde. À l'ordre, s'il vous plaît! Ayant constaté le quorum, je déclare la séance de la Commission des institutions ouverte. Je vous souhaite, bien sûr, la bienvenue, et je vous demande, à toutes personnes présentes présentes dans la salle, de bien vouloir éteindre la sonnerie de votre appareil électronique.

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 débiter, 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 Rizzy (Saint-Laurent); M. Fontecilla (Laurier-Dorion) est remplacé par M. Nadeau-Dubois (Gouin); M. LeBel (Rimouski) est remplacé par M. Ouellet (René-Lévesque).

Le Président (M. Bachand) : Merci beaucoup. Ce matin, nous entendrons les personnes des groupes suivants, donc : la Commission des droits de la personne et des droits de la jeunesse, la Commission d'accès à l'information du Québec, le directeur scientifique du Réseau intégré sur la cybersécurité, de même que le titulaire de la Chaire de recherche du Canada en analyse respectueuse de la vie privée et éthique des données massives. Donc...

M. Nadeau-Dubois : M. le Président.

Le Président (M. Bachand) : Oui.

M. Nadeau-Dubois : Si je peux me permettre, juste un petit instant, avant qu'on entende notre premier invité, hier, durant la journée, à plusieurs reprises, les députés membres de la Coalition avenir Québec, dans leurs questions, ont fait allusion à une consultation qui a eu lieu dans les dernières semaines au Québec, une consultation en ligne sur l'application dont on discute cette semaine, il en a même été allusion dans le cas du point de presse de la députée de Jean-Talon. Les députés semblent avoir de l'information que les députés de l'opposition n'ont pas au sujet de cette consultation. La députée de Jean-Talon a même révélé en point de presse qu'il y avait eu 17 000 personnes qui avaient participé à la consultation.

Pour qu'on puisse collaborer ensemble puis qu'on puisse travailler de manière réellement collégiale, au-delà de nos allégeances politiques, je demanderais aux députés de la Coalition avenir Québec de bien vouloir nous transmettre l'information qu'ils ont au sujet de cette consultation-là, parce que sinon on se retrouve dans une consultation où il y a deux catégories de députés : des députés qui sont dans le bon parti et qui ont donc, de toute évidence, de l'information au sujet des résultats de cette consultation et des députés qui sont dans les mauvais partis et qui, eux, n'ont pas ce privilège.

Alors, avant qu'on commence puis pour qu'on commence nos délibérations, aujourd'hui, d'un bon pied, sur un ton de collégialité puis de travail transpartisan, moi, j'aimerais qu'on nous donne accès à ces informations-là. Ça a filtré dans une organisation de presse, ça filtre par moments, par certains points de presse, dans certaines questions. Alors, moi, j'aimerais qu'on nous transmette cette information-là, puis, je pense, ça aiderait beaucoup à la bonne marche de nos travaux aujourd'hui.

Le Président (M. Bachand) : Merci, M. le député. Je vais vous rappeler que tout le monde possède des informations sur ce dossier, mais il n'a jamais été question de publication, alors donc il n'y a pas de dépôt de document. Ce sont des informations qui peuvent avoir... mais il n'y a pas de publication. Donc, on ne peut pas déposer quelque chose qui n'est pas publié. Ça va? Merci beaucoup.

Auditions (suite)

Donc, nous allons débiter les auditions. Alors, je souhaite donc la bienvenue aux gens de la Commission des droits de la personne et des droits de la jeunesse.

M. Nadeau-Dubois : ...

Le Président (M. Bachand) : Pardon, M. le député?

M. Nadeau-Dubois : J'ai dit j'allais appeler le reporter de TVA, Alain Laforest, puisque lui semble avoir plus d'information que moi comme député.

Le Président (M. Bachand) : Merci, M. le député. Alors, je cède donc la parole aux gens de la Commission des droits de la personne et des droits de la jeunesse. Alors, Me Tessier, Me Carpentier, vous avez 10 minutes de présentation, et, par après, nous allons procéder à la période d'échange. Alors, bienvenue, Me Tessier.

**Commission des droits de la personne
et des droits de la jeunesse (CDPDJ)**

M. Tessier (Philippe-André) : Merci, M. le Président. Mmes et MM. les députés, alors, évidemment, Philippe-André Tessier, président de la Commission des droits de la personne et des droits de la jeunesse. Je suis accompagné de Me Marie Carpentier, conseillère juridique à la recherche à la commission.

Evidemment, je vous remercie de l'invitation qui est faite à la commission de participer à ces consultations particulières et audiences publiques sur les outils technologiques de notification des contacts, sur la pertinence de ce type d'outils, leur utilité et, évidemment, le cas échéant, les conditions de leur acceptabilité sociale dans le cadre de la lutte contre la COVID-19.

Conformément à sa mission d'assurer le respect et la promotion des principes énoncés à la Charte des droits et libertés de la personne du Québec, la commission a examiné la proposition du gouvernement afin d'en vérifier la conformité aux principes énoncés dans cette charte et d'en faire les recommandations qu'elle estime appropriées.

Au cours des derniers mois, nombreux experts et défenseurs des droits et libertés de la personne ont manifesté leurs réserves ou leur opposition à ce sujet et ont réclamé la tenue d'un débat public sur la question. La commission tient donc tout d'abord à saluer que le gouvernement prenne acte des préoccupations exprimées quant au recours à des outils technologiques dans la lutte contre la pandémie et qu'il organise un débat public.

La commission salue également le fait que le gouvernement envisage d'adopter seulement le type d'outil technologique considéré comme étant le plus respectueux de la vie privée et qu'il exclut les dispositifs de surveillance enregistrant notamment les données de localisation des personnes. Le gouvernement a en effet posé ce qu'il estime être les conditions d'acceptabilité sociale d'une application de notification d'exposition en faisant la liste des fonctionnalités désirées. On peut noter l'accent sur le caractère gratuit et volontaire, la confidentialité, le traitement minimal des renseignements personnels et le stockage protégeant la vie privée. Cela témoigne d'une prise en compte d'observations émises par plusieurs experts et organisations de santé publique et de défense des droits et libertés.

Suivant le mandat qui lui incombe, la commission a procédé à son analyse non pas sur l'acceptabilité sociale, mais sur les dispositions de la charte, en se basant notamment sur les atteintes potentielles au droit au respect à la vie privée et au droit à l'égalité garantis par les articles 5 et 10 de la charte. Notre réflexion se situe donc dans le contexte plus large où le développement de nouvelles technologies met en jeu des intérêts économiques qui peuvent entrer en conflit avec l'exercice des droits et libertés de la personne, notamment, évidemment, en lien avec l'exploitation des données. Des inquiétudes ont notamment été exprimées par rapport au fait que les moments de crise sont propices à l'adoption de mesures de surveillance qui deviennent permanentes et au fait que les entreprises de l'industrie des technologies interviennent de plus en plus souvent dans la vie des personnes et des communautés.

Il est fort probable qu'une application qui serait recommandée par le gouvernement opérerait sur le système de notification d'exposition développé en partenariat avec Apple et Google. Ces derniers ont assuré qu'ils ne procéderont pas à la monétisation des données échangées sur leur système de notification d'exposition et que le système sera désactivé une fois sa finalité atteinte. Cela commande une évaluation en continu.

À ce jour, le gouvernement du Québec n'a pas indiqué à quelle application spécifique il entend recourir. Or, le choix d'une application de notification d'exposition soulève plusieurs questions. Il sera nécessaire de connaître l'ensemble des spécifications de l'outil retenu afin d'être en mesure de mieux évaluer les atteintes potentielles. Ainsi, dans un contexte anxiogène, comme je le disais plus tôt, il peut être risqué de demander à des populations en situation de vulnérabilité d'adopter un outil technologique qui n'a pas fait ses preuves et qui n'a pas fait l'objet d'analyses rigoureuses basées sur des expérimentations empiriques. À ce sujet, on ne sait toujours pas quel usage les personnes feront des ces applications et quelles en seront les répercussions en termes de santé publique. Par exemple, l'utilisation d'une application pourrait encourager, c'est certain, le développement d'un faux sentiment de sécurité au point potentiellement de ne pas respecter les autres mesures de santé publique de distanciation. Conséquemment, l'application devra faire l'objet d'une évaluation rigoureuse et surtout, encore une fois, en continu par des instances indépendantes.

Donc, compte tenu de ces conséquences potentielles, la commission recommande que le gouvernement prévoie une procédure d'évaluation continue et transparente de son application de notification d'exposition et que celle-ci soit notamment fondée sur les droits et libertés inscrits à la charte. Pour que ces évaluations soient possibles, il est primordial également que l'application et son fonctionnement soient transparents et accessibles. On formule donc une recommandation à cet effet.

En outre, étant donné les difficultés liées à l'identification des relations causales et à l'application des principes de responsabilité civile dans le domaine des nouvelles technologies, il serait opportun de déterminer des règles précisant

les responsabilités à l'égard des dommages qui pourraient découler du recours à une application de notification d'exposition. La commission recommande ainsi que le gouvernement détermine des règles d'imputabilité dans le cadre du recours à une application de notification d'exposition.

Par ailleurs, comme l'a bien reconnu le gouvernement dans son document de consultation, ce ne sont pas tous les Québécois qui disposent d'un téléphone intelligent plus récent. C'est le cas de 77 % d'entre eux, pour ce qui est d'un téléphone intelligent, en 2019. Évidemment, comme vous l'avez entendu hier, les données disponibles démontrent que cette distribution-là est inégale selon l'âge, le revenu, le niveau de scolarité et le genre : on a 53 % des personnes avec un revenu de moins de 20 000 \$, 35 % des personnes de 75 ans et plus. C'est ce qui est appelé communément la fracture numérique, puis elle n'est pas, évidemment, limitée à l'accès à un téléphone intelligent, mais aussi à un modèle suffisamment récent pour avoir une version d'un système d'exploitation qui supporte une application de notification. Les besoins des personnes en situation, aussi, d'itinérance ou en d'autres situations de vulnérabilité devraient faire l'objet d'évaluation en continu, encore une fois.

Une répartition inégale des bénéfices attendus d'une application gouvernementale de notification pourrait être discriminatoire si une atteinte à la vie et à la sûreté de cette personne était fondée sur des motifs prévus par la charte comme l'âge, le sexe ou la condition sociale. Nous recommandons donc que le gouvernement déploie des efforts pour pallier les effets de cette fracture numérique avant de donner son aval à une application. Le gouvernement a bien souligné le fait que l'application sera gratuite, mais le document de consultation ne fait pas état d'autres mesures pour faciliter les principes d'inclusion et d'accessibilité. Évidemment, des atteintes discriminatoires peuvent également découler de l'usage d'une application qui ne respecte pas ces principes, notamment, et on pense ici aux personnes en situation de handicap.

Le gouvernement souligne la présence d'une limite technique d'une application de notification d'exposition basée sur la technologie Bluetooth en affirmant qu'elle ne tiendrait pas compte de certains contextes, par exemple masque de protection, séparation par une surface vitrée. Cette technologie risque donc également de générer un nombre considérable de faux positifs, et les impacts pourraient être disproportionnés sur certaines populations, en particulier les personnes à faibles revenus et racisées. Ces personnes sont en effet plus susceptibles de vivre dans des milieux densément peuplés ayant enregistré des taux de contamination élevés et devoir travailler dans des contextes propices à cette contamination. Dans l'évaluation continue de l'application, il sera alors nécessaire de tenir compte des risques de génération d'effets négatifs financiers et psychologiques sur ces groupes déjà marginalisés.

En outre, de l'avis de la commission, le recours à une application de notification d'exposition constitue une forme de surveillance. De ce fait, elle porte atteinte au droit au respect à la vie privée garanti par la charte. Évidemment, ce droit n'est pas absolu. En effet, une personne peut valablement y renoncer. Pour être valable, cette renonciation doit satisfaire certaines exigences. En ce sens, nous recommandons au gouvernement que celui-ci s'assure que le consentement à la collecte, à l'usage et à la transmission de données soit libre et éclairé, donné à des fins spécifiques pour une durée déterminée, portant sur les données nécessaires et qu'il puisse être renouvelé régulièrement.

• (9 h 10) •

La commission comprend que le modèle proposé par le gouvernement repose sur un tel consentement. Toutefois, si des tiers, par exemple des employeurs, des commerçants ou des locataires, exigeaient d'une personne qu'elle utilise l'application pour transiger avec elle, on ne pourrait plus parler, alors, de renonciation valide. Le cadre juridique actuel n'est malheureusement pas suffisant pour interdire un tel usage. Dans le cas, donc, où des tiers requerraient l'usage de l'application, il faudrait s'assurer que la plainte au droit au respect de sa vie privée soit justifiée, c'est-à-dire que le recours à une telle application n'est pas irrationnel, arbitraire et que les moyens choisis soient proportionnels au but visé. Dans ces circonstances, il faudrait examiner avec attention l'utilité de l'application, son efficacité ainsi que le niveau de sécurité qu'elle présente avant de conclure qu'elle est conforme aux dispositions de la charte.

Alors, l'application utiliserait la technologie Bluetooth, et certains doutes ont été exprimés quant à la capacité de cette technologie de détecter avec précision les expositions des personnes infectées. Un tel usage par des tiers pourrait également porter atteinte aux droits et libertés, notamment aux libertés fondamentales. Ainsi, la commission recommande que le gouvernement interdise à des tiers d'exiger l'utilisation d'application de notification et d'exposition et qu'il mette en place des mesures de surveillance et de contrôle pour s'assurer que cette interdiction d'exiger l'utilisation d'application soit effective.

En état d'urgence sanitaire, la commission, donc, ne se prononce pas contre le recours à une telle application de notification d'exposition. Nous sommes toutefois d'avis que l'utilisation d'une telle application doit respecter les conditions que je viens d'énumérer pour éviter de compromettre les droits et libertés garantis par la charte. Je vous remercie de votre attention.

Le Président (M. Bachand) : Merci infiniment, Me Tessier. Donc, je me tourne vers la partie ministérielle. M. le député de Chapleau, s'il vous plaît.

M. Lévesque (Chapleau) : Merci beaucoup, M. le Président. Merci, Me Tessier, Me Carpentier, merci beaucoup d'être ici ce matin. Merci de votre témoignage.

Donc, comme vous l'avez dit, effectivement, l'application, là, s'il est avéré que le gouvernement décide d'aller de l'avant, ce serait effectivement gratuit, anonyme, sécuritaire et installé sur une base volontaire, sans géolocalisation, évidemment, sans recours à la biométrie puis il n'y aurait pas de stockage de données ou de renseignements personnels, là, comme vous en avez fait mention.

Peut-être une petite question... Revenons sur la fracture numérique. Hier, justement, on a eu beaucoup de groupes qui sont revenus sur cette question-là, avec la problématique, justement, là, des différents... soit des différents groupes d'âge ou des différents milieux sociaux. Est-ce qu'il n'y a pas lieu de penser qu'il y aurait... pourrait y avoir un gain pour la santé publique, justement, que certains groupes puissent l'avoir? Notamment, on peut penser aux jeunes qui, bon, ont accès à la technologie, qui peuvent... dans le fond, qui pourraient être notifiés dans le cas d'un contact avec une personne qui aurait eu la COVID-19. Et la société, tu sais, de façon plus grande, en bénéficierait, du fait que cette personne-là ne va pas voir grand-maman, ne va pas voir grand-papa et reste... dans le fond, s'isole et va faire un test. Donc, j'essaie de voir, là, l'équilibre entre le gain qu'on pourrait avoir en termes de santé publique puis, effectivement, là, les droits prévus à la charte.

M. Tessier (Philippe-André) : Merci pour la question. Bien, c'est le défi auquel l'état d'urgence sanitaire, présentement, interpelle les commissions des droits, mais évidemment pas juste au Québec, partout à travers le monde. C'est cet équilibre-là qui doit être recherché entre les différents droits. Évidemment, le droit à la vie est aussi garanti par nos chartes, et donc il faut l'opposer au droit à la vie privée. Il faut balancer ces intérêts-là, qui, des fois, peuvent sembler contradictoires. Alors, évidemment, on a bien entendu, aussi, les différents commentaires et les différents propos qui ont été tenus à cet égard-là.

Ce qu'il faut se rappeler, c'est toujours la même chose, c'est que, lorsqu'on va faire cet exercice-là de balancer, on va regarder les faits, dans la mesure du possible, les faits qui sont disponibles. Ce que l'on sait, c'est qu'il y a une surreprésentation au niveau des victimes de cette maladie-là qui sont des personnes âgées. Il y a une surreprésentation aussi pour les travailleurs dans le milieu de la santé. Il y a certaines populations qui ont été identifiées comme étant vulnérables qui sont aussi plus affectées par cette maladie-là. Donc, c'est sûr et certain qu'il peut y avoir des bénéfices. Vous donnez l'exemple des jeunes qui pourraient être en contact et qui ont, eux, des téléphones intelligents, mais il faut, à ce moment-là, le balancer avec le fait... c'est quoi, l'impact de cette maladie-là aussi sur ces jeunes-là? Et cet exercice-là, c'est ce à quoi la commission interpelle le gouvernement pour dire : Advenant qu'il y a une application qui est mise de l'avant, bien, le droit à la vie privée et les chartes s'appliquent, et, évidemment, si le gouvernement ne veut pas se voir contester ces éléments-là par des membres de la société, bien, il faut qu'il soit sûr de pouvoir faire cette démonstration-là factuelle de l'utilité sociale de cette application.

M. Lévesque (Chapleau) : Je vois quand même que vous considérez que ça pourrait être un outil qui pourrait s'ajouter aux autres mesures de santé publique. Donc, ça ne devrait pas être un seul outil de façon prioritaire ou de façon unique pour combattre la pandémie, tu sais, ça peut être dans le panier, disons, des outils, là, pour la Santé publique.

M. Tessier (Philippe-André) : Je pense que ce que la commission a voulu venir dire devant vous, puis je pense que ça a été un peu dans notre allocution ou quand vous regardez notre mémoire, nous ne nous opposons pas à l'adoption d'une telle application, c'est très clair. Ce que l'on fait dans notre rôle, c'est qu'on fait nos recommandations pour dire...

Et puis on est très conscients aussi, puis on l'a dit, je l'ai dit dans mes notes d'allocution, qu'il y a déjà certaines situations qui ont été identifiées, il y a eu des expérimentations dans d'autres pays, il y a l'application fédérale qui a été lancée. Donc, il y a déjà un peu d'eau qui a coulé sous les ponts, qui nous permet de faire cette appréciation-là et puis de voir qu'il y a des préoccupations... On donnait l'exemple de la géolocalisation qui a été complètement évacuée puis on va... Bon, alors, oui, c'est des avancées et c'est dans cet exercice-là de balancer, hein, vie privée, selon 9.1 de la charte, et de s'assurer que cette disposition-là est conforme. Bien, ce genre d'initiative là gouvernementale, on le dit, on le salue, parce qu'effectivement ça va dans le bon sens, si on suit ce genre de recommandation là.

M. Lévesque (Chapleau) : J'aimerais bien vous entendre sur la notion d'élargissement du... notion de renseignements personnels. Donc, vous aimeriez peut-être élargir les renseignements personnels. Puis dans quelle mesure puis comment vous feriez cela, là, pour le faire?

M. Tessier (Philippe-André) : Est-ce que tu veux répondre?

Mme Carpentier (Marie) : En fait, notre cadre d'analyse, c'est la charte, le droit au respect de sa vie privée, qui est inscrit à la charte, donc cette analyse-là n'est pas limitée à la notion de renseignements personnels. Donc, on n'est pas limités par le cadre des lois sur la protection des renseignements personnels dans le domaine privé ou la loi sur le public. Donc, la notion de vie privée est plus englobante que celle de renseignements personnels. Donc, notre analyse est fondée sur le droit au respect de sa vie privée, qui découle de la charte.

M. Lévesque (Chapleau) : Ce serait sur cette analyse-là que ce serait basé, O.K. Puis justement, peut-être, sur la réglementation puis la législation actuelle, avez-vous des commentaires? Est-ce que vous la considérez satisfaisante? Est-ce que vous trouvez qu'il y aurait même, tu sais, moyen de l'améliorer? Peut-être même vous avez eu l'occasion de voir le projet de loi n° 64.

M. Tessier (Philippe-André) : Bien, oui, c'est sûr. Bien, c'est pour... Ma collègue et moi, on va répondre à tour de rôle, là, mais simplement pour vous dire que pour ce qui est... Évidemment, on n'est pas sur la commission

parlementaire sur le p.l. n° 64 puis on prend le temps, évidemment... Et une chose est sûre pour nous, ce qu'on a identifié de façon quand même... de façon assez importante, c'est l'interdiction pour les tiers. Alors, c'est sûr et certain que, présentement, cette interdiction-là n'existe pas, elle n'est pas dans les livres. Donc, vous nous demandez qu'est-ce qui manque, présentement, ça, c'est sûr que, oui, ça manque. Ça, c'est clair que, là, là-dessus, il y a un enjeu, parce que la pente... quand on parle... une pente glissante.

Puis je suis bien au fait, là... on a bien écouté aussi, hier, ce qui s'est passé. Donc, on ne veut pas verser non plus dans le catastrophisme ou dans le solutionnisme, tu sais, je pense qu'on essaie d'avoir une approche équilibrée sur le domaine, sur la question, mais c'est sûr et certain que, quand on voit un trou, quand on voit un espace, bien, généralement, il y a une tentation pour des gens de pouvoir se glisser dans ce trou-là, des tiers d'exiger... et que ce soit des employeurs, des locataires, peu importe, n'importe qui qui se retrouve... de venir exiger l'application, et c'est là où ça glisse, parce que c'est là où le consentement libre et éclairé, il s'étiole, puis c'est un risque quand même assez conséquent.

M. Lévesque (Chapleau) : C'est beau. Peut-être une petite dernière question avant de passer la parole à ma collègue des Plaines. Vous avez parlé d'analyse en continu, d'évaluation continue, de surveillance et de contrôle. Comment vous envisagez cet élément-là que vous nous présentez?

M. Tessier (Philippe-André) : Ce que je peux vous dire, c'est que la commission a collaboré... hier, vous avez entendu M. Maclure, le président de la Commission en éthique, science et technologie, donc la commission a collaboré aux travaux. Évidemment, on collabore également avec la Commission d'accès à l'information, on a participé récemment à leur consultation sur les systèmes d'intelligence artificielle.

Donc, il y a déjà des acteurs, quand même, gouvernementaux crédibles, qui sont la CDPDJ, la CAI, la CEST et l'INESSS également, qui... donc, il y a déjà ces organismes-là qui ont des professionnels à l'intérieur de ces organismes-là qui peuvent exercer ce genre de rôle là en continu. Pour nous, c'est sûr et certain que l'État s'est doté de ces organismes-là de conseil et d'avis, bien, c'est un bon moment, peut-être, pour les mettre à contribution.

Le Président (M. Bachand) : Merci beaucoup, M. le député. Mme la députée de Les Plaines, s'il vous plaît.

Mme Lecours (Les Plaines) : Merci beaucoup, M. le Président. Tout d'abord, merci de votre présence aujourd'hui. C'est important qu'on puisse, justement, avoir des éclairages et des recommandations.

Vous avez parlé, justement, d'évaluation en continu, vous avez parlé d'un fonctionnement transparent également. Vous avez mentionné, à un moment donné, la discrimination par rapport aux handicapés. J'aimerais ça que vous développiez un petit peu là-dessus.

M. Tessier (Philippe-André) : Encore là, nous, on dit : Il faut faire attention. Évidemment, il y a des protocoles, il existe différents types de protocole en ligne qui sont là pour faire en sorte que ces applications-là soient accessibles, que ça soit, par exemple, pour non-voyants au niveau des lecteurs.

Ce qu'il faut toujours comprendre, c'est que, lorsqu'il y a une situation de crise sanitaire, il va y avoir des mesures nouvelles qui sont mises en place. Bien, par exemple, là, présentement, bien, à certains endroits, on va mettre des pistes cyclables partout, on va piétonner les rues. Bien là, on n'a peut-être, des fois, pas pensé au fait que la personne qui a besoin du transport adapté pour se rendre chez elle, bien, ça limite son accès à son transport adapté puis à son déplacement. Et souvent, nous, à la commission, on est très sensibilisés à ces enjeux-là en lien avec les personnes en situation de handicap qui vont le dénoncer. Il y a des... C'est des gens qui sont déjà, en partant, stigmatisés — puis je parle handicap visible ou invisible, là, donc moteur, peu importe, là, la notion large de handicap — alors c'est sûr et certain que, lorsqu'on met en place ce genre de système là, il faut toujours avoir la petite pensée en disant : Bien, c'est une bonne idée, mais... oui, mais est-ce qu'on a pensé aussi aux personnes en situation de handicap? Puis c'est un peu le sens de notre propos dans le mémoire. Ces principes-là sont bien connus, technologiques, et tout...

• (9 h 20) •

Mme Lecours (Les Plaines) : ...dans la fracture du numérique, non. C'est deux choses différentes. O.K.

M. Tessier (Philippe-André) : Non, c'est deux... Oui, c'est ça, c'est deux choses différentes. C'est ça, tout à fait.

Mme Lecours (Les Plaines) : O.K. Un petit peu de temps encore? Vous avez parlé, évidemment, de l'utilité. C'est clair que la commission est là pour ça, pour en voir aussi... pas l'adaptabilité, mais l'acceptabilité sociale et l'utilité dans un moyen additionnel à ce qui se fait déjà. Un peu comme mon collègue vous a posé la question, de quelle façon est-ce que, selon vous, on pourrait, justement, le considérer comme utile, en complément avec ce qui se fait déjà?

Mme Carpentier (Marie) : Notre posture est à l'effet que cette notion-là d'utilité va vraiment varier en fonction du fait que les tiers ont accès à l'application ou non.

Si l'application sert vraiment essentiellement à notifier une personne puis que la personne n'a pas de conséquence attachée avec le fait qu'elle a l'application ou qu'elle ne l'a pas ou avec le résultat que fournit l'application, l'utilité, je dirais, en termes de santé publique, les conséquences en termes de droits de la personne sont moindres.

Si des tiers peuvent avoir accès, soit obliger quelqu'un à avoir l'application ou soit voir le résultat que produit l'application, là, la question de l'utilité puis de l'efficacité de l'application est vraiment plus en cause. Puis on sait que l'efficacité de l'application est relative, étant donné que la technologie Bluetooth n'a pas été développée à cette fin-là, donc ce n'est pas une technologie qui a été prévue pour cet usage-là.

Et en amont, en fait, il y a quand même la question des tests qui vont produire le résultat que l'application fait. Donc, même les tests, on sait qu'ils sont efficaces, ils ne produisent pas de faux positif, mais ils produisent 30 % de faux négatifs. Donc, l'efficacité... l'utilité de l'application est limitée par l'efficacité des tests en partant.

Donc, à partir du moment où les tiers prendraient des décisions de transiger avec une personne, la question de l'utilité est beaucoup plus importante si des tiers sont en cause. La commission est d'avis que, là, il faudrait faire une étude approfondie sur le fonctionnement spécifique de l'application avec toutes les données nécessaires, ce qu'on n'a pas pour l'instant, là. On a des caractéristiques générales, mais on n'a pas toutes les caractéristiques de l'application. Puis nous, on peut faire une évaluation des impacts sur les droits de la personne, mais ça prendrait aussi d'autres sortes d'experts qui seraient capables de nous démontrer l'utilité en termes de santé publique et les risques informatiques qui sont liés avec cette application-là.

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

Mme Boutin : Bonjour, Me Tessier et Me Carpentier. Merci d'être là. Votre rapport était fort intéressant. Je ne sais pas si... Je suis un peu loin de mon micro, hein?

Bien, je vais rebondir un petit peu sur ce que vous avez dit sur les tests. Premièrement, par rapport à cette application-là, le code est ouvert, puis c'est quand même relativement transparent, mais j'aimerais... j'ai deux questions, en fait. Premièrement, sur votre recommandation 1 et la recommandation 3, j'aimerais qu'on approfondisse un petit peu, parce que vous mentionnez l'importance d'intégrer un processus d'évaluation en continu. Moi, j'aimerais savoir qu'est-ce qu'on pourrait évaluer. Puis est-ce qu'on le fait juste en continu ou en amont et est-ce qu'on évalue l'efficacité? Si on évalue l'efficacité, comment est-ce qu'on pourrait procéder pour que ça soit statistiquement intéressant? Dans le fond, est-ce qu'on demande à un groupe de participer? Moi, j'ai beaucoup de questionnements par rapport à ça, puis c'est revenu, là... puis je pense que ça va revenir aujourd'hui puis demain également, là, parce qu'il n'y a pas de rapports internationaux vraiment publics qui nous ont permis de démontrer l'efficacité ou non. On a des constats internationaux, mais il n'y a rien, tu sais, d'assez tangible.

Ça fait que peut-être que nous, si jamais on allait de l'avant... si le gouvernement allait de l'avant, tu sais, en amont, pourrait déjà établir ces mécanismes-là. J'aimerais vous entendre là-dessus, approfondir un petit peu.

Le Président (M. Bachand) : En 1 min 30 s.

M. Tessier (Philippe-André) : Comme j'ai dit tout à l'heure à votre collègue, le but de cette recommandation-là, puis je pense que vous y faites référence, c'est qu'il y a différents rapports, il y a différentes initiatives internationales qui ont été mises de l'avant, il y a certaines mesures qui sont faites en fonction de... bon, bien, par exemple, le taux d'adhésion, est-ce qu'il... Et c'est sûr et certain que les questions qu'on peut identifier... Nous, on se pose des questions sur les questions d'imputabilité dans le cadre de recours en application. Bien, c'est aussi ces éléments-là, qui qui est responsable s'il y a des problèmes.

On peut essayer de prendre notre boule de cristal, vous et moi, puis imaginer, bon, qu'est-ce qui peut arriver, mais c'est pour ça qu'on parle de mécanismes d'évaluation en continu, c'est parce qu'il y a des choses, peut-être, qu'on ne soupçonne pas qui vont se produire, qui peuvent avoir un impact. Et d'avoir cet exercice-là, ça ne veut pas dire qu'à tous les mois il y a des éléments qui se font, là. On parle d'évaluations en continu, ça peut être sur une période. Puis évidemment, bien, on le rappelle aussi que... puis je pense que ma collègue y faisait référence, c'est qu'on veut que ça soit basé sur un cadre d'analyse qui est global, qui est celui de la vie privée prévue à la charte, pas seulement à celui du renseignement personnel prévu dans les lois qui visent à protéger les renseignements privés ou l'accès à l'information. Je ne sais pas si ça répond à votre question.

Le Président (M. Bachand) : Il vous reste 30 secondes, Mme la députée.

Mme Boutin : Bien, au niveau, justement... brièvement, sur la gouvernance et l'imputabilité, est-ce qu'on pourrait mettre, je ne sais pas, moi, un groupe, un comité d'experts, quelque chose en amont?

M. Tessier (Philippe-André) : Bien, c'est un modèle qui est retenu puis qui est quand même adopté ailleurs, là. Nous, notre but, ce n'est pas de vous dire comment le faire, mais c'est sûr qu'il y a différents modèles qui existent, là, puis je pense qu'il y a des gens ailleurs qui vous ont parlé également de différentes possibilités en ce sens-là. Donc, on peut juste vous dire que nous sommes intéressés et disponibles.

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

Mme Rizqy : Merci beaucoup. Bonjour. Je vais tout de suite rebondir, d'ailleurs, sur l'imputabilité et le groupe indépendant. Prenons, par exemple, un cas concret que nous sert la vie privée, lorsqu'il y a des plaintes logées... par

exemple celui au centre d'achats, en Alberta, où est-ce qu'on a utilisé un logiciel de reconnaissance faciale à l'insu des gens, il y a eu une plainte qui a été logée. Ça fait maintenant deux ans, et le rapport n'a toujours pas été déposé.

Alors, au niveau de, oui, mettre en place un chien de garde, mais présentement est-ce que nos chiens de garde ont des lois qui ont du mordant et assez de ressources pour rapidement s'assurer d'avoir non seulement un rapport mais aussi des conséquences à ceux qui enfreignent nos droits à la vie privée?

M. Tessier (Philippe-André) : Bien, écoutez, pour ce qui est de la Commission d'accès à l'information, je vais... je pense qu'ils passent juste après nous, je vais les laisser répondre à votre question.

Pour ce qui est de notre maison, c'est sûr et certain que la question des délais, c'est une question qui est toujours préoccupante pour nous. On essaie toujours de répondre dans les meilleurs délais aux citoyens lorsqu'ils déposent des plaintes. C'est sûr et certain que, lorsqu'il y a des situations nouvelles qui impliquent des intérêts variés, ça pose des défis pour des organisations comme les nôtres, qui se voient confier des responsabilités de faire des enquêtes.

C'est pour ça que, quand on vous parle d'évaluation continue puis en suivi, c'est qu'il n'y a rien qui peut se... surtout sur des éléments comme ça qui sont nouveaux, qui sont complexes, des analyses rapides peuvent être des fois, malheureusement, bâclées. Et il faut se mettre... il faut être très prudents, lorsqu'on est des institutions comme les nôtres, de faire des analyses qui sont rapides ou bâclées parce que, là, on peut mettre vraiment en péril la confiance des citoyens envers les institutions. Ça fait qu'il faut faire cet exercice-là...

Mme Rizqy : Je comprends, mais un délai de deux ans, quatre ans, des fois, dans d'autres cas... Pour la population, c'est quoi, l'effet dissuasif lorsqu'un rapport peut tarder ou semble tarder si on n'a pas mis assez de ressources dans nos institutions pour, justement, rapidement, sans bâcler le travail... mais habituellement on est capables quand même de donner une conséquence un peu plus rapide que quatre ans maximum.

M. Tessier (Philippe-André) : Écoutez, nous, c'est sûr et certain que, de ce point de vue là, c'est pour ça que nous, on joue notre rôle, aussi, aujourd'hui en amont en faisant des recommandations pour éviter ce genre de situation là ou pour sensibiliser les parlementaires puis le gouvernement aux réalités liées aux droits de la personne.

Maintenant, c'est sûr que, les délais, il n'y a... comment je pourrais vous dire, ce n'est pas simplement une question de délai, ici. L'enjeu, c'est que l'évaluation continue dont on parle et les règles qu'on met en place ou la recommandation, par exemple, de l'utilisation des tiers, c'est que, oui, on peut porter plainte puis, oui, on peut faire ce genre de démarche là, mais ce qui est beaucoup plus porteur, c'est lorsqu'il y a les règles qui sont clairement établies au début, les balises sont mises clairement au début et que c'est très clairement dit, par exemple, par le gouvernement — ça a un impact — qui dit : Les employeurs, vous n'avez pas le droit de l'exiger. Ce n'est peut-être pas contraignant au sens légal du terme, mais c'est sûr que c'est un puissant indice, quand le gouvernement dit aux employeurs du Québec : Écoutez, vous ne pouvez pas exiger l'application quand le monde rentre chez vous pour travailler. Ça donne aussi un outil au travailleur, qui dit : Bien là, écoute, boss, je t'aime bien, mais il me semble que j'ai entendu le premier ministre dire que tu n'avais pas le droit de faire ça. Donc, il y a ce genre de geste là, qui peut être posé en amont, qui aide, disons.

• (9 h 30) •

Mme Rizqy : Mais aujourd'hui, au XXI^e siècle, la donnée, là, les entreprises courent après ça. Et tantôt vous avez fait référence à un trou et que, malheureusement, lorsqu'il y a un petit trou, là, aussi petit soit-il, les gens vont avoir tendance, malheureusement, à vouloir l'explorer, ce trou.

Et ça m'amène à la question suivante. Puisque le risque zéro, évidemment, on le sait très bien, n'existe pas, par contre il peut toujours y avoir un risque de croisement de données, et, là-dessus, ce risque de croisement de données, il est réel. Et aujourd'hui les entreprises... parce que, oui, il y a le gouvernement qui peut avoir une application, mais rien n'empêche une entreprise privée telle que, par exemple, Facebook de développer sa propre application et avoir, encore une fois, une fuite de données, aujourd'hui, les conséquences pécuniaires, si jamais il y a une fuite de données, pour le secteur privé, c'est assez limité, là, au Québec et au Canada.

Mme Carpentier (Marie) : Ce qu'on dit, dans notre analyse... Notre analyse porte sur le fait qu'à notre avis, avec la proposition gouvernementale, si les tiers n'ont pas accès à l'application, le consentement peut être valide. Donc, il y a toujours le consentement, à l'origine. Donc, la question de la protection des données personnelles... Les gens acceptent d'avoir un compte Facebook s'ils acceptent d'avoir une application... C'est... On ne recommande pas l'adoption d'une application. Je pense que, ça, je peux dire ça. Mais on dit que, si les règles de consentement sont respectées et si c'est interdit aux tiers d'avoir accès à l'application, le consentement à la renonciation au droit au respect de sa vie privée pourrait être valide. Je ne sais pas si ça répond...

Mme Rizqy : Oui, oui. Donc, je comprends que vous ne recommandez pas l'application. Si jamais on va de l'avant, il faudrait... Mais est-ce que vous permettez d'ajouter la chose suivante? Au niveau de la pédagogie qu'on fait, aujourd'hui, sur le consentement, sur notre droit à la vie privée, elle est très limitée, la littératie numérique, là, elle est très, très peu développée. Alors, comment peut-on parler de consentement libre et éclairé, et, si je peux me permettre, pour nos aînés, et la population vulnérable, et les populations plus stigmatisées?

M. Tessier (Philippe-André) : Oui, c'est sûr que c'est des préoccupations qu'on illustre dans notre mémoire. Je pense que c'est pour ça que, lorsqu'il y a ce genre d'outil là qui est déployé, s'il est déployé, puis je reviens sur le

fait que ça prend des actions gouvernementales fortes pour venir expliquer, faire comprendre — je pense qu'il y a ce genre de choses là qui se produisent, présentement, dans le contexte que l'on vit, avec d'autres mesures gouvernementales qui sont mises en place — bien, c'est sûr et certain qu'il y aura cet effort-là qui devra être fait pour s'assurer qu'il y ait une véritable compréhension de la population, de ce que ça veut dire et c'est quoi, les conséquences, c'est quoi, les impacts.

Mme Rizqy : Tantôt, vous parliez aussi que ça n'a pas fait ses preuves. Vous avez aussi comme mission de vraiment, aussi, protéger les plus vulnérables, les populations stigmatisées. Prenons un exemple très concret, Montréal-Nord. Rappelons-nous, ma collègue la députée de Montréal-Nord, au départ, il n'y avait pas... la Santé publique n'avait pas identifié Montréal-Nord, c'étaient les gens du terrain, les gens du sociocommunautaire, la députée qui se battaient dans l'eau bénite pour dire : Non, non, il y a quelque chose qui se passe ici, on est éloignés, on est dans des méga blocs-appartements, on a besoin de venir être testés, malgré que, lorsque la Santé publique a déployé une unité mobile de dépistage, la première journée, là, ça ne s'est pas rué, il a fallu envoyer des gens frapper aux portes.

Pensez-vous sincèrement que ce type d'application permettrait d'améliorer la situation ou, pire, pourrait faire en sorte que ceux qui n'ont pas accès à Internet, environ 30 % dans ce secteur, eux autres, au contraire, dans la file de réactions et d'accès au droit à la santé, c'est-à-dire d'avoir accès aux tests, ils arriveraient un peu plus loin dans la chaîne de commandement parce qu'ils ne seraient jamais notifiés, à moins qu'on aille cogner à leur porte?

M. Tessier (Philippe-André) : Je veux juste dire... puis évidemment la consultation d'aujourd'hui est sur l'application, là, mais, sur le grand angle, là, la commission, on est sortis pour, justement, mettre en lumière le fait que la crise sanitaire avait révélé... avait été un révélateur des inégalités sociales plus sous-jacentes et profondes qui existent. Pour donner l'exemple de Montréal-Nord, on a même fait une sortie là-dessus pour dire que c'est des inégalités structurelles qui préexistent et c'est des faiblesses structurelles où on voit ces éclosions-là, les CHSLD, les populations plus vulnérables. Donc, ça, et on n'est pas les seuls à l'avoir dit, il y a quand même eu ces éléments-là qui sont ressortis. Puis c'est sûr et certain qu'il faut voir l'application, puis c'est un peu ce qu'on dit aussi dans notre mémoire, comme étant un des moyens. Il y a énormément de moyens qu'il faut mettre en place pour s'assurer que les populations vulnérables et... bon, les personnes âgées ou autres, qu'on vienne combler cette fracture numérique là, oui, pour l'application, mais, en termes de santé publique, il y a d'autres mesures à mettre en place, puis ce n'est peut-être pas l'objet du propos d'aujourd'hui, mais on les a quand même dits dans les quatre, cinq derniers mois. Je vous dirais qu'on est sortis quand même beaucoup là-dessus pour, justement, rappeler au gouvernement l'importance d'insister sur ces aspects-là, parce qu'effectivement, vous l'avez dit, il n'y a pas nécessairement d'accès à Internet ou de téléphone intelligent, mais... C'est ça.

Mme Carpentier (Marie) : Dans notre mémoire, on mentionne aussi l'importance de s'assurer que les conséquences négatives qui pourraient être liées... de faire attention à la répartition des conséquences négatives qui pourraient être liées avec un faux positif qui pourrait produire l'application, par exemple les conséquences psychologiques d'avoir un faux positif puis les conséquences économiques, le fait d'être obligé de se confiner. Donc, oui, dans le mémoire, on le mentionne, que c'est important que le gouvernement voie à pallier. Ceci dit, quels sont les moyens pour pallier à ça, bien, c'est votre prérogative.

Mme Rizqy : Je voudrais ne pas vous poser la question suivante. Aujourd'hui, oui, on parle de traçage, une application, l'application de notification, dis-je bien, mais il y a aussi deux autres affaires assez importantes, je crois : le dossier de reconnaissance faciale, qui est en cours, où est-ce qu'on sait que la Sûreté du Québec est en appel d'offres, où est-ce qu'il n'a pas eu de débat, et il y a aussi l'identité numérique. Tout ça, est-ce que vous n'avez pas l'impression que ça mériterait d'être discuté et... Je vois que vous hochez déjà la tête, alors je vais vous laisser parler.

M. Tessier (Philippe-André) : Oui, bien, écoutez, je vais vous dire, là, lorsqu'on parle de la situation COVID, encore une fois, bien, la situation COVID met en lumière des situations, des enjeux. Justement, bon, c'est quoi, l'ironie, là? C'était quelqu'un qui mettait un post sur Facebook pour dénoncer une application de traçage. Je veux dire, tu sais, il y a ces questions-là qui se posent par rapport à l'ensemble des GAFAM. Puis, encore une fois, le Québec n'est pas le seul. Donc, ces questions-là, elles se posent. Elles se posaient avant la pandémie, elles vont se poser après. C'est clair que ces enjeux-là sont fondamentaux, oui.

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

M. Nadeau-Dubois : Merci, M. le Président. Bonjour à vous, maîtres, au pluriel. Merci d'être avec nous ce matin en commission. J'ai un peu plus de deux minutes, alors je vais être direct. Est-ce qu'il y a, actuellement, dans le corpus législatif québécois, des dispositions qui interdiraient, comme vous le recommandez, à des tiers d'exiger l'application?

M. Tessier (Philippe-André) : Pas à notre connaissance, non.

M. Nadeau-Dubois : Parfait. Sans une telle modification législative, donc, qui viendrait interdire cet accès par des tiers, est-ce qu'une telle application représenterait, selon vous, un danger pour les droits et libertés des Québécois et des Québécoises?

M. Tessier (Philippe-André) : C'est sûr et certain que, comme on l'a dit tout à l'heure, là, en l'absence de telles mesures, il faut, à ce moment-là, disons, des prononcés très affirmatifs et très clairs sur les consignes et les conditions à respecter, pour le grand public, pour au moins s'assurer qu'il y ait une compréhension, mais...

M. Nadeau-Dubois : Comment? Est-ce que vous recommandez que ça prenne la forme de dispositions législatives?

M. Tessier (Philippe-André) : Pour nous, puis c'est ce qu'on met dans notre recommandation, c'est que ça serait des mesures législatives, effectivement.

M. Nadeau-Dubois : Parfait. Est-ce qu'à votre... selon votre lecture du projet de loi n° 64, il y a, dans ce projet de loi déjà déposé à l'Assemblée nationale, des dispositions qui répondent aux critères que vous venez d'énoncer?

M. Tessier (Philippe-André) : Je ne peux pas me prononcer sur 64, on ne l'a pas encore étudié. M. le député, avec respect, là, je suis obligé de vous dire que...

M. Nadeau-Dubois : Est-ce qu'il y a d'autres choses qui sont manquantes dans notre cadre législatif pour rendre l'utilisation d'une telle application respectueuse des droits et libertés des Québécois et des Québécoises?

M. Tessier (Philippe-André) : L'autre élément aussi, c'est sûr et certain, sur lequel on vous sensibilise, à la recommandation 3 de notre mémoire, c'est les questions d'imputabilité. Donc, c'est sûr et certain que, dans le domaine technologique, c'est un peu flou, qui est responsable de quoi. Alors, c'est sûr et certain que ce qu'on pense qui est une bonne façon de faire, c'est... souvent, ça va être de créer des présomptions pour s'assurer que... Bon, donc, ça, c'est ce genre de mécanisme là qu'on peut mettre en place dans le domaine technologique.

M. Nadeau-Dubois : ...ça prenne la forme d'une disposition législative.

M. Tessier (Philippe-André) : Encore une fois, c'est quelque chose qui peut être, effectivement, de l'ordre d'une disposition législative, oui.

M. Nadeau-Dubois : Parfait. Merci beaucoup.

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

M. Ouellet : Merci beaucoup. À mon tour de vous saluer. Merci pour votre mémoire. Je veux revenir à la première recommandation que vous faites, notamment sur la gouvernance et l'importance d'avoir cette gouvernance-là en continu et cette surveillance-là. Vous en faites une recommandation. Seriez-vous prêt, aujourd'hui, d'en faire une exigence si le gouvernement décide d'aller de l'avant avec le type d'application de traçage qui est discutée, mais qui n'est peut-être pas celle qui sera proposée?

• (9 h 40) •

M. Tessier (Philippe-André) : Le mandat que la commission a en vertu de la charte, c'est de faire des avis et des recommandations au gouvernement.

M. Ouellet : Bien, est-ce que... O.K.

M. Tessier (Philippe-André) : Donc, notre mandat législatif est de faire des recommandations.

M. Ouellet : Est-ce que vous recommandez fortement?

M. Tessier (Philippe-André) : Bien, tout... Je veux dire, évidemment, une fois par année, la commission dépose son rapport annuel. La charte prévoit, à son article 75, que ce rapport est déposé directement à l'Assemblée nationale, et là-dedans on fait la liste de nos recommandations et des suivis ou non de nos recommandations. Les parlementaires peuvent exercer un contrôle sur l'action gouvernementale à travers des institutions comme la nôtre, celle du Protecteur du citoyen, du Vérificateur général. C'est sûr que nos recommandations doivent être suivies, dans la mesure où on encourage et on incite le gouvernement à les suivre. Puis, lorsqu'elles ne sont pas suivies, bien, on est transparents avec les parlementaires puis on le dépose à l'Assemblée nationale.

Mme Carpentier (Marie) : Si je peux me permettre...

M. Ouellet : Oui, allez-y.

Mme Carpentier (Marie) : ...cela étant, on a bien indiqué qu'on n'avait pas toutes les informations disponibles pour donner notre avis définitif sur l'application. Puis c'est certain que, s'il y a une application qui était proposée, on referait un examen pour vérifier si elle est... si l'application est conforme aux dispositions de la charte.

M. Ouellet : Le débat est là. On parle de peut-être utiliser l'application fédérale, mais ça peut être une autre application. Tu sais, je veux dire... Puis je lisais la découpe de presse du ministre de la Stratégie numérique, ce matin, à Radio-Canada, qui dit qu'on a peut-être un débat futile tant et aussi longtemps que le gouvernement n'aura pas décidé d'aller dans le même sens que ses sondages et ses consultations auront donné, indiquant la volonté des Québécois et des Québécoises d'aller de l'avant, et, au final, la solution proposée pourrait être totalement différente de celle qu'on parle aujourd'hui.

Donc, merci pour ces éclairages, ils sont importants. Et notre travail, à la commission parlementaire, c'est de tracer des guides qui vont nous aider lorsque le gouvernement aura décidé quelle application... quelles devraient être les mesures pour en assurer la sécurité, l'accessibilité, l'acceptabilité et surtout qu'on ne fasse pas ça pour rien. Alors... Puis je ne veux pas vous mettre en boîte, là, je comprends votre rôle...

M. Tessier (Philippe-André) : ...on vous dit, puis... recommandations, puis on en a parlé avec les autres parlementaires, c'est que c'est sûr et certain qu'évidemment, aujourd'hui, on ne sait pas c'est quoi, l'application, avec un L majuscule. Maintenant, cela dit, les autres recommandations demeurent pertinentes, dans la mesure où, peu importe l'application choisie, s'il y en a une de choisie, bien, c'est pour ça qu'on parle de mécanismes d'évaluation puis de suivi en continu, c'est parce que, fondamentalement, il y aura d'autres questions qui vont se poser, il y aura... il y a d'autres enjeux sous-jacents plus larges quant à l'utilisation des données, l'utilisation du numérique, donc c'est sûr et certain que ces éléments-là vont continuer d'être analysés.

Le Président (M. Bachand) : Merci. Merci, Me Tessier. Je dois céder la parole... je veux céder la parole au député de Chomedey, pardon.

M. Ouellette : Merci. Bonjour à vous. Effectivement, votre mémoire est en fonction des informations que vous avez. Bien, nous, nos questions sont en fonction des informations qu'on a. Vous comprenez que c'est un choix politique. Vous comprenez que, présentement, le gouvernement base avec les... ce qui filtre, la complémentarité sur 12 000 citoyens du Québec qui sont favorables à cet outil-là, là. On va oublier le 75 %, c'est 12 000 citoyens. On ne le sait pas encore, on ne les a pas toutes, les informations.

On comprend aussi que vous êtes en... C'est un processus d'évolution. Là, vous venez de nous faire une image aujourd'hui, mais, en fonction des informations que vous avez et en fonction du document de consultation. On comprend que, dès que le gouvernement va avoir décidé... On souhaite que ça soit par processus législatif, on souhaite que le gouvernement n'utilise pas l'état d'urgence sanitaire pour y aller par décret. Ça, c'est parce que c'est une autre chose qui est possible.

Mais ce que je remarque, c'est qu'aujourd'hui vous venez allumer une lumière rouge puis vous nous dites : La définition de la vie privée, la définition globale de la vie privée... vous nous parlez d'équilibre, vous nous parlez de bonne gouvernance, vous nous parlez de transparence, d'imputabilité puis de reddition de comptes. C'est des choses qui devront apparaître, parce que, si j'ai bien compris, vous allez être le premier à venir nous dire, si ce n'est pas là : Bien, on est passés, le 13 août, on vous a dit ce qu'il en était, et je pense que vous allez... on vous suggère très, très, très fortement de vous en assurer parce que ça pourrait amener des contestations puis ça pourrait amener, de la part des citoyens, un rejet de la position politique gouvernementale. Est-ce que j'ai bien compris?

Le Président (M. Bachand) : M. Tessier, je vous laisse la fin, quelques secondes.

M. Tessier (Philippe-André) : Oui, merci. Bien, écoutez, oui, c'est sûr que nous, nous allons... en vertu de notre mandat, en vertu de la charte, on va continuer à regarder cette situation-là.

Je peux vous dire aussi, puis je veux juste rassurer les parlementaires là-dessus, l'ensemble des décrets et arrêtés ministériels font office, présentement, de législation. C'est sûr que la commission les analyse et les étudie un par un et les regarde tous pour s'assurer de leur conformité, tel que notre mandat le prévoit.

Le Président (M. Bachand) : Merci beaucoup. Alors, merci encore une fois d'avoir été avec nous ce matin. Cela dit, je suspends les travaux pour quelques instants. Merci beaucoup.

(Suspension de la séance à 9 h 45)

(Reprise à 9 h 52)

Le Président (M. Bachand) : À l'ordre, s'il vous plaît! La commission reprend ses travaux. Merci beaucoup.

Alors, il nous fait plaisir d'accueillir les gens de la Commission d'accès à l'information, soit Me Diane Poitras, présidente, et M. Martin Carbonneau, agent de recherche. Alors, vous avez 10 minutes de présentation, comme vous le savez, après on aura un échange avec les membres de la commission. Merci beaucoup d'être ici, et la parole est à vous.

Commission d'accès à l'information (CAI)

Mme Poitras (Diane) : Bonjour. Je me présente, je suis Diane Poitras, présidente de la Commission d'accès à l'information. Je suis accompagnée de M. Martin Carboneau, qui est professionnel en veille, recherche et promotion à la commission.

Alors, au nom de la commission, je tiens à vous remercier pour cette invitation. Même si nous sommes conscients que les enjeux relatifs aux applications de notification d'exposition imposent une réflexion plus globale que ceux concernant la vie privée et la protection des renseignements personnels, nos commentaires, aujourd'hui, vont porter uniquement sur ce volet et sur la transparence, enjeux qui sont au coeur de notre mission.

Comme l'invite à le faire le document préparé par le Secrétariat du Conseil du trésor en vue de la présente consultation, notre mémoire vise à cerner les enjeux et les modalités d'encadrement relatives à la protection des renseignements personnels de ces outils technologiques, mais de manière générale, il ne porte pas sur une application en particulier. Une analyse plus poussée de la commission sera donc requise si le gouvernement décide d'aller de l'avant avec une application de notification des contacts pour que nous puissions émettre un avis et formuler des recommandations spécifiques sur la solution qui serait retenue.

Dans son mémoire, la commission énonce 11 principes essentiels à respecter afin de guider la démarche si le gouvernement décide d'appuyer ce genre d'outil. Pour chacun de ces principes, nous formulons des recommandations qui se veulent concrètes, bien que générales, comme je l'ai mentionné. Pour appuyer notre dernière recommandation du mémoire, qui est d'adopter un cadre juridique spécifique au déploiement et à l'utilisation d'une application au Québec comme d'autres pays l'ont fait, nous soumettons également une liste des éléments qui devraient être inclus dans cette loi ou ce décret. Ces principes s'inspirent essentiellement de la législation actuelle et de ceux mis de l'avant par la déclaration commune du 7 mai de l'ensemble des commissaires à la protection de la vie privée du Canada, sauf ma collègue de l'Alberta, qui était en train d'étudier l'application ABTraceTogether. Ce sont d'ailleurs ces principes qui ont servi à l'évaluation de l'application Alerte COVID, qui a été réalisée par mes homologues du fédéral et de l'Ontario récemment. Compte tenu du temps qui m'est alloué, je vais aborder succinctement quelques principes et insister seulement sur certaines recommandations que nous formulons dans le mémoire. Je vous y réfère pour un portrait plus complet.

Le premier principe est déterminant, en conditionne plusieurs, et la Commission des droits de la personne en a parlé avant nous, c'est d'établir la nécessité et la proportionnalité du recours à une application de notification d'exposition. Une telle application est susceptible d'avoir des conséquences sur le droit au respect de la vie privée et la protection des renseignements personnels. Je pense que tout le monde en convient. Toutefois, ce droit, évidemment, n'est pas absolu. On peut y porter atteinte si on démontre que c'est nécessaire pour répondre à un objectif légitime et important et que l'atteinte au droit fondamental est proportionnelle à cet objectif. Pour ce faire, le gouvernement devrait d'abord déterminer le ou les objectifs de santé publique spécifiques poursuivis par l'application. Ces objectifs doivent être fondés sur la science et s'inscrire dans la stratégie de lutte contre la COVID-19 des autorités de santé publique.

Le gouvernement devrait aussi être en mesure de démontrer la proportionnalité de la mesure, notamment en se demandant si la solution retenue minimise l'atteinte à la vie privée. Par exemple, l'intrusion dans la vie privée des individus est plus importante pour certaines technologies comme la géolocalisation, ou la biométrie, ou encore pour une solution prévoyant un stockage centralisé de l'information par opposition à une application où les renseignements sont stockés sur les appareils des utilisateurs, qu'on appelle décentralisée.

Il faut aussi pouvoir conclure qu'elle permet d'atteindre les objectifs poursuivis, donc que l'application est efficace ou, du moins, susceptible de l'être. Or, l'efficacité de ces applications, vous l'avez entendu, reste à déterminer. Selon l'OMS, on ne peut pas évaluer directement leur impact sur la gestion de la crise à l'heure actuelle, faute de données ou d'études probantes. On sait que ces applications ont plusieurs limites, notamment liées à l'utilisation de la technologie comme telle, comme l'imprécision des mesures de distance ou le fait qu'on ne prend pas en considération des éléments de contexte comme le port du couvre-visage ou la présence de cloisons quand on détermine qu'un contact est à risque.

On constate aussi que les applications déployées, actuellement, dans le monde ont des effets plutôt mitigés. Leur taux d'adoption, qui est déterminant aussi pour leur efficacité, est généralement faible, actuellement. Il dépend beaucoup de la confiance et des craintes des citoyens, mais aussi, vous l'avez entendu, de l'accès à des téléphones intelligents suffisamment récents pour supporter l'application. Or, une partie importante de la population, souvent parmi la plus vulnérable, n'en possède pas. Ça réduit d'autant l'efficacité de ces applications tant pour ces personnes que pour celles avec lesquelles elles entrent en contact.

• (10 heures) •

Enfin l'OMS rappelle que ces solutions technologiques doivent s'inscrire dans un ensemble de mesures complémentaires, notamment des tests de dépistage en nombre suffisant et complétés par un traçage manuel des contacts efficace. Ainsi l'efficacité d'une telle mesure doit être évaluée avant son déploiement, mais aussi en continu par la suite. Et, dans un objectif de transparence et d'imputabilité en lien avec notre principe 10, la commission recommande d'établir des critères pour évaluer cette efficacité et un mécanisme d'évaluation indépendante en continu par rapport aux objectifs qui auront été fixés et d'en rendre compte de manière transparente.

Il importe également de s'assurer qu'une autorité indépendante surveille le respect des principes visant le respect de la vie privée, la suffisance des mesures de protection en place et la conformité légale de l'application. La commission souligne qu'elle a déjà l'expertise et les pouvoirs d'enquête et d'inspection qui lui permettraient de jouer ce rôle.

Deuxième principe que j'aimerais porter à votre attention, c'est de minimiser l'atteinte aux droits dès la conception de l'application. C'est pourquoi la commission recommande qu'une évaluation des facteurs relatifs à la vie privée concernant la solution retenue soit réalisée, comme la plupart des pays l'ont fait avant le déploiement, qu'elle soit soumise à la commission pour avis et diffusée publiquement et de porter une attention particulière au choix de la technologie utilisée de même qu'à la nature des renseignements qui seraient éventuellement recueillis.

Le troisième principe est à la fois déterminant tant pour la proportionnalité de la mesure que pour la confiance envers une telle application. Il s'agit d'en garantir le caractère volontaire et d'assurer un consentement valide. Pour ce faire, la commission recommande de fournir une information claire, simple et complète aux utilisateurs sur son fonctionnement et les renseignements personnels qui seront recueillis et utilisés, d'obtenir un consentement explicite et spécifique lors de l'installation de l'application et, par la suite, pour chaque finalité de santé publique qui implique des renseignements personnels, de permettre le retrait du consentement et la désinstallation de l'application en tout temps et de détruire sans délai tout renseignement concernant l'utilisateur, et, point essentiel, d'interdire à quiconque d'exiger l'installation de l'application ou la consultation de son contenu, par exemple pour conditionner l'accès à un lieu, un bien, un service ou un emploi.

Évidemment, la commission recommande d'adopter, à toutes les étapes, une démarche transparente. Nous saluons d'ailleurs les démarches consultatives publiques et institutionnelles tenues respectivement par le gouvernement et l'Assemblée nationale à ce sujet. Et, dans la continuité de cette initiative, la commission recommande notamment de diffuser les motifs qui justifieraient éventuellement une décision de recourir à une telle mesure exceptionnelle et les modalités de son déploiement et de diffuser, évidemment, le code source de l'application et des dispositifs qui y sont liés pour permettre une évaluation externe indépendante.

Les cinquième et sixième principes visent à limiter tant la collecte, l'utilisation et la communication de renseignements personnels, par exemple en privilégiant l'utilisation de renseignements anonymisés ou dépersonnalisés et de favoriser une application qui fonctionne en mode décentralisé et qui recueille le moins de renseignements possible liés aux individus. Il importe, évidemment, de mettre en place une infrastructure technologique sécuritaire qui comprend des mesures de protection répondant aux plus hauts standards et de s'assurer que l'ensemble de l'écosystème dans lequel évoluerait une éventuelle application est entièrement sécurisé. Évidemment, il faut déterminer les conditions de mise hors service pour que la... et détruire les renseignements recueillis pour que cette mesure exceptionnelle ait un terme.

Et finalement, comme plusieurs homologues et experts, la commission considère qu'une application doit s'accompagner d'un encadrement juridique spécifique pour garantir aux citoyens le respect des principes énoncés précédemment. C'est une des recommandations de l'OMS et du comité consultatif d'experts du CIFAR, qui a été mandaté pour formuler des recommandations au sujet de ces applications au gouvernement du Canada. C'est pourquoi la commission recommande d'adopter, par loi ou par décret, un cadre juridique spécifique au déploiement et à l'utilisation de l'application au Québec, comme d'autres pays l'ont fait, dont la France, la Suisse et l'Australie. En effet, certains enjeux soulevés ne sont pas encadrés adéquatement par la loi actuelle, comme par exemple le respect du caractère volontaire de l'utilisation de l'application, l'utilisation des renseignements aux seules finalités de santé publique qui seraient identifiées ou encore la durée déterminée de la mesure. L'autorégulation ne nous paraît pas acceptable dans les circonstances, vu les enjeux en cause et la confiance nécessaire.

En terminant, la commission réitère que, si le gouvernement décide de déployer une application de notification des contacts, elle entend analyser l'outil et l'évaluation des facteurs à la vie privée qui sera produite afin de fournir des recommandations plus spécifiques et de rendre un avis précis. Il me fera plaisir de répondre à vos questions davantage à ce sujet. Je vous remercie.

Le Président (M. Bachand) : Merci pour votre présentation. Je me tourne vers le gouvernement. M. le député de Chapleau, s'il vous plaît.

M. Lévesque (Chapleau) : Merci beaucoup, M. le Président. Merci, Me Poitras. Merci d'être ici. Merci de votre présentation.

J'aimerais peut-être commencer, là... Vous aviez parlé d'équilibre et de certains critères, notamment de nécessité, de légitimité, d'importance, donc, en lien avec les objectifs de la Santé publique pour déployer un tel outil. Croyez-vous, justement, qu'un outil, s'il est dans l'équilibre, pourrait être pertinent et pourrait s'ajouter aux différentes mesures de santé publique qui sont déjà en place? Est-ce que la commission est à l'aise avec ça?

Mme Poitras (Diane) : En fait, comme on est dans la théorie, pour l'instant, qu'on n'a pas une application spécifique avec des objectifs précis d'identifiés... C'est très difficile de répondre à une question dans la théorie.

M. Lévesque (Chapleau) : Mais, théoriquement, disons?

Mme Poitras (Diane) : Ce qu'on regarderait, pour nous, c'est la conformité légale, et la proportionnalité de la mesure, et le respect des droits par l'application.

M. Lévesque (Chapleau) : Ce serait plus ça. Et donc... Merci. Et, au niveau du rôle que la commission pourrait avoir, vous avez mentionné, bon, une autorité indépendante, une autorité compétente. Comment vous voyez votre rôle? Quel serait... Puis peut-être, même, poussons plus loin. Est-ce qu'au niveau de la réglementation et des

lois il y aurait des éléments qui seraient pertinents pour que vous ayez... pour pouvoir, dans le fond, bien jouer ce rôle-là si jamais il y avait lieu?

Mme Poitras (Diane) : Évidemment, si on parle... Avant le déploiement de l'application, comme je l'ai mentionné, la première étape serait d'évaluer et de donner un avis sur une évaluation des facteurs relatifs à la vie privée, par rapport à une application spécifique qui serait établie, pour faire des recommandations plus précises. Par la suite, on pourrait s'assurer du respect des principes. Puis, si notre recommandation d'adopter un cadre juridique est acceptée ou est suivie, en fait, ça serait de voir au respect de ce cadre juridique et du cadre actuel, évidemment, par le biais des pouvoirs qu'on a. Et, pour des mesures plus concrètes, il faudrait voir qu'est-ce que prévoit un éventuel projet de loi, par exemple, ou quelle est l'application, quelle est l'évaluation des facteurs relatifs à la vie privée, etc.

M. Lévesque (Chapleau) : Parfait. Merci. Vous avez parlé de la notion de tiers et le fait que ça deviendrait une application conditionnelle pour soit un emploi ou entrer dans un endroit. Vous pouvez peut-être élaborer ces craintes-là puis voir, là, ce qu'il en est, puis ce serait peut-être une piste de solution que vous verriez pour ça?

Mme Poitras (Diane) : En fait, les pays qui ont légiféré ou qui ont adopté un décret l'ont fait d'abord et avant tout pour s'assurer du caractère volontaire, parce que, dans l'état de la législation actuelle, ce serait difficile. En tout cas, un employeur... prenons l'exemple d'un employeur, là, un employeur pourrait tenter de justifier que la mesure est nécessaire, que la collecte des renseignements est nécessaire. Et la commission a... Comme tout le monde, là, dans la population, on a vu des initiatives spontanées, souvent faites avec la meilleure bonne foi, mais qui avaient des impacts ou qui soulevaient des enjeux importants de vie privée. Alors, pour nous, la solution, c'est vraiment un encadrement, une interdiction spécifiée dans un cadre juridique, loi ou décret. Évidemment, on privilégie la loi, là, mais je me contenterais d'un décret.

M. Lévesque (Chapleau) : ...certains groupes, le fait qu'ils l'aient pourrait représenter un gain sociétal ou un gain pour la santé publique du fait que ce groupe-là y ait accès? On pense aux jeunes, qui sont en recrudescence, actuellement, au niveau des cas. Est-ce que le fait qu'eux, ce groupe-là, ils aient accès, et certains groupes autres aussi... qui pourrait réduire, dans le fond, les risques de santé publique, est-ce que ça, ça pourrait justifier l'utilisation d'une application, selon vous?

Mme Poitras (Diane) : En fait, tout revient au test de nécessité et de proportionnalité que j'ai indiqué. Et, pour l'instant, la commission ne détient pas de données probantes qui permettent de répondre à cette question sur des données scientifiques, alors j'hésiterais de spéculer sur la réponse à donner.

M. Lévesque (Chapleau) : Merci beaucoup. M. le Président, merci.

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

Mme Boutin : Mme Poitras, M. Charbonneau, merci d'être là. C'est très, très pertinent. Comme toujours, votre travail est toujours très rigoureux.

J'aimerais rebondir tout de suite sur la question des tiers parce que je pense que c'est quelque chose qui va revenir. Je me posais la question parce que, dans la Loi de la protection des renseignements personnels dans le secteur privé, l'article 18, bon, il y a des exceptions qui font en sorte qu'un employeur peut recueillir des renseignements personnels. Mais, tu sais, on s'entend que peut-être, quand la loi a été rédigée, il n'y avait pas d'application mobile, là. Puis c'est pour ça, le but, aussi, d'avoir le projet de loi n° 64 puis de réformer, aussi, la loi, la LCCJTI, tu sais, de moderniser tout cela. Mais actuellement est-ce qu'un employeur pourrait forcer un employé à télécharger l'application?

Mme Poitras (Diane) : Dans les faits, oui, ils peuvent le faire. Je vous dirais qu'on est conscients qu'il y a des employeurs qui ont développé des outils et des applications, et qu'ils exigent de leurs employés qu'ils le portent, et que ce sont des outils de traçage, de notification d'exposition.

Mme Boutin : ...

Mme Poitras (Diane) : Oui, bien, ça ne veut pas dire que c'est légal, ça ne veut pas dire que le concept de nécessité et de proportionnalité est rencontré. La commission n'a pas eu l'occasion d'analyser encore cette situation-là, mais je sais qu'on a notamment une enquête en cours.

Mme Boutin : Parce que je pense que, pour le gouvernement, ça va être important, là, de respecter vos recommandations. La vie privée puis le respect des données personnelles est quelque chose d'assez préoccupant qu'on prend au sérieux, là. Puis, dans les outils législatifs qui seraient disponibles, bon, éventuellement, peut-être dans le projet de loi n° 64 ou autre projet de loi, un décret pourrait être quelque chose de potentiellement satisfaisant à court terme?

Mme Poitras (Diane) : C'est sûr qu'une loi, c'est toujours préférable, mais, comme je vous ai dit, je me contenterais... entre rien puis un décret, je vais me contenter du décret. Mais c'est clair pour nous que l'objectif, c'est d'avoir un encadrement, pour certains éléments, complémentaire à la législation actuelle, qui est insuffisante.

Mme Boutin : J'aimerais vous amener sur un autre sujet, au niveau peut-être de la gouvernance, en amont, tu sais, si jamais le gouvernement allait de l'avant. Tu sais, moi, c'est quelque chose... Tout ce qui est imputabilité, reddition de comptes, gouvernance, c'est assez important. Comment pourrait s'intégrer... parce qu'il pourrait y avoir une gouvernance au niveau... qui intégrerait des questions de sécurité de l'information, peut-être plus cybersécurité, mais, au niveau de la protection des renseignements personnels, vie privée, comment est-ce que vous voyez ça, sous quelle forme?

Mme Poitras (Diane) : Je ne suis pas sûre de bien comprendre votre question.

Mme Boutin : Bien, je ne veux pas vous mettre de mots dans la bouche non plus, là, mais est-ce qu'on pourrait mettre en place un comité spécial? Quel type de gouvernance permettrait d'assurer une bonne imputabilité au niveau de la protection des renseignements personnels, mais également un suivi, une évaluation en continu?

Mme Poitras (Diane) : O.K. Mais je peux donner un exemple qui s'est fait au fédéral, ils ont créé un comité d'experts multidisciplinaires qui, justement, vise à conseiller le gouvernement sur les mesures à mettre en place, évaluer l'efficacité, les mesures de protection des renseignements personnels, la sécurité, les impacts sociaux aussi, etc. — c'est sûr que ça, c'est une bonne façon — avec transparence des avis et des recommandations qui sont faits par ces comités. Mais, pour moi, ça, c'est comment le gouvernement peut assumer son rôle de gouvernance, ça n'enlève pas le besoin d'évaluation externe indépendante aussi.

Mme Boutin : Une évaluation externe indépendante, vous parlez... comme par un groupe hors gouvernement, par exemple?

Mme Poitras (Diane) : Oui, bien, comme pour le volet protection des renseignements des renseignements personnels, respect de la vie privée, transparence. La commission jouerait son rôle qui lui est dévolu, là, selon sa mission, évidemment.

• (10 h 10) •

Mme Boutin : Je pense que ma collègue la députée des Plaines a des questions... Ah! Beauce-Nord.

Le Président (M. Bachand) : Oui, M. le député de Beauce-Nord, s'il vous plaît.

M. Provençal : Merci, M. le Président. Merci beaucoup pour votre mémoire. J'aimerais poser une question en lien avec la recommandation n° 3 de votre mémoire, qui est en lien avec le caractère volontaire et la notion du consentement valide. À l'intérieur de ça, vous dites «obtenir un consentement distinct, spécifique et explicite». Bon, premier consentement, l'installation, ça, c'est clair pour moi, mais «demander un consentement distinct pour chaque finalité de santé publique», pouvez-vous me clarifier cet élément-là, s'il vous plaît?

Mme Poitras (Diane) : Par exemple, je vais prendre l'exemple d'Alerte COVID, actuellement il y a un consentement initial pour utiliser l'application. Et, par la suite, si vous recevez un diagnostic positif, on va vous redemander un consentement pour communiquer les informations, les contacts numériques, là, que vous avez eus, qui sont stockés sur votre téléphone intelligent, de les communiquer au serveur fédéral pour qu'il puisse l'envoyer, par la suite, à tous les utilisateurs de l'application pour qu'ils fassent le match — excusez l'anglicisme — pour voir si vous avez été en contact avec une personne qui a été testée positive. Donc, un consentement... ça, c'est un exemple d'un deuxième consentement où il y a un deuxième événement important.

M. Provençal : Ça va. Parce que, de la manière que je le percevais, c'est qu'on pouvait prévoir ou penser que ça pourrait servir aussi pour autre chose qu'au niveau santé, mais là vous vous limitez vraiment à la situation qu'on vit présentement.

Mme Poitras (Diane) : Idéalement, oui, mais on sait que, dans les projets à travers le monde, il est arrivé qu'il s'est greffé, à un moment donné, une autre fonctionnalité qu'on a voulu imposer. Puis, pour nous, c'est que, si on voulait, hypothétiquement, ajouter une autre fonctionnalité, c'est clair qu'il faudrait redemander un consentement.

M. Provençal : Je viens de comprendre. Merci beaucoup, madame. Merci, M. le Président.

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

Mme Boutin : ...parce que vous avez mentionné, dans votre rapport... puis j'ai trouvé ça très intéressant, je pense, c'est la recommandation 9, où est-ce qu'il y a des outils ou une information... Mettons que quelqu'un télécharge l'application puis il a des questionnements par rapport, justement, à sa vie privée, tout ça, donner une

source d'information où les gens pourraient téléphoner, comment est-ce que vous voyez ça? Est-ce que vous, vous pourriez jouer ce rôle-là? Est-ce que vous avez assez de ressources pour faire ça? Parce que, admettons, je ne sais pas, moi, je donne un chiffre par hasard, 25 000 personnes ont des questions par rapport à leur vie privée puis ils téléphonent, est-ce que ce serait une ligne, un site Internet? Puis je trouve que c'est très intéressant, pour ma part, là.

Mme Poitras (Diane) : Non, dans ma tête, ce n'était pas la Commission d'accès à l'information qui jouait ce rôle-là. Je pense que c'est plus — appelons-les comme ça — aux promoteurs ou ceux qui gèrent l'application de répondre à ces questions-là sur le fonctionnement, etc. Pour Alerte COVID, par exemple, c'est un organisme gouvernemental. Je ne sais pas si M. Carboneau se souvient, on va vérifier, mais je sais que c'est un organisme... je ne me souviens pas si c'est Santé Canada ou le centre numérique canadien, un des deux, là, qui va jouer ce rôle-là.

Mme Boutin : Ils ont mis en place des ressources. Mais, probablement, en relation avec les gens... mettons que ça pourrait être en relation avec vous, par exemple, là, un groupe d'experts qui répondent aux questions, mais, s'il y a des questions spécifiquement sur leurs droits en matière de vie privée et protection personnelle...

Mme Poitras (Diane) : Ah! ça, c'est sûr que, si c'est des questions... Je m'excuse, je ne voulais pas vous couper la parole. Mais, si vraiment c'est des questions sur leurs droits, ça, c'est la commission. Mais je pense qu'il y a un premier niveau, un peu comme quand, une personne, avant de porter plainte chez nous, on l'encourage à faire une démarche auprès de l'entreprise ou de l'organisme pour tenter de régler la situation. Puis, s'ils ont des questions sur le fonctionnement, sur la circulation des données, je pense que ça, ce n'est pas à la commission de répondre, ce serait plus aux promoteurs de...

Mme Boutin : En tout cas, c'est une discussion intéressante, parce qu'on a tendance, dans la vie de tous les jours, à «downloader» toutes sortes d'applications, à aller sur des sites. On nous demande le consentement pour des cookies ou des choses comme ça, mais on n'a jamais l'opportunité de poser des questions ou de savoir en quoi est-ce que mes droits sont vraiment protégés. Tu sais, on le fait tous, ici, là, tout le monde, ici, est sur des médias sociaux, soit utilisent Google Maps, Bluetooth, on est tous à risque, mais on ne sait jamais vraiment comment est-ce que nos renseignements personnels sont protégés ou non. Puis j'ai trouvé intéressante cette recommandation-là, pour ma part, de pouvoir avoir l'opportunité d'avoir accès à, je ne sais pas, un juriste ou quelqu'un qui pourrait répondre à nos questions.

Mme Poitras (Diane) : Tout à fait. Bien, c'est le genre de question qu'on a souvent, pas nécessairement sur des applications ou des produits spécifiques, mais effectivement... Et il y a peut-être une certaine partie de la population qui est habituée avec les applications et le numérique, mais il y a quand même une bonne partie de la population qui n'a pas cette facilité et pour qui les concepts de toute cette collecte de données, cet univers numérique ne va pas de soi.

Le Président (M. Bachand) : M. le député de Chapleau.

M. Lévesque (Chapleau) : Oui, M. le Président. Peut-être une petite dernière question, là, en lien au processus menant, dans le fond, au développement ou, du moins, à la mise en oeuvre de l'application. Vous avez parlé, bon, des analyses nécessaires en cybersécurité puis différentes analyses... Est-ce que vous entrevoyez également, peut-être, une analyse de votre commission avant même le déploiement? Est-ce que... Dans le fond, j'aimerais voir quelles étapes vous voyez puis qu'est-ce que vous envisageriez de façon vraiment à améliorer, là, toute la notion de protection de vie privée des Québécois, de renseignements personnels? C'est vraiment l'objectif aussi. Donc, si on peut avoir votre son de cloche là-dessus, ce serait bien apprécié.

Mme Poitras (Diane) : Bien, en fait, je verrais fort bien comme ça s'est déroulé dans plusieurs autres juridictions, c'est-à-dire un avis sur une évaluation des facteurs à la vie privée qui serait réalisée. C'est comme une analyse de tous les enjeux de vie privée et de protection des renseignements personnels qui est réalisée par... ici, ce serait le gouvernement, une instance, un organisme public quelconque... qui est analysé par la commission, avec des échanges, on pose des questions, etc., pour qu'on voie l'ensemble de l'écosystème, on formule des recommandations précises. Et, dans un deuxième temps, ce serait de regarder sous le capot, une fois que l'application est déployée, d'aller vérifier si ce qu'on a avancé dans l'évaluation des facteurs à la vie privée ou ce qu'on avance dans la description de comment fonctionne l'application, si ça se concrétise.

M. Lévesque (Chapleau) : ...que vous avez parlé de vos collègues des autres provinces, également fédéral, est-ce qu'ils ont eu l'occasion de faire ça, cette espèce d'analyse?

Mme Poitras (Diane) : Oui, mon collègue du fédéral... mes collègues du fédéral et de l'Ontario ont analysé les volets respectifs, fédéral et provincial, de l'application Alerte COVID et, dans les deux cas, ont mentionné qu'ils allaient faire une phase II. Pour le fédéral, je crois que c'est d'ici la fin...

M. Lévesque (Chapleau) : Puis les résultats initiaux, justement, fédéral, je serais curieux de voir quelles recommandations ou quels résultats qu'ils ont émis. Qu'est-ce qu'ils ont dit de ça? Il y a-tu eu un rapport?

Mme Poitras (Diane) : Oui, oui, oui, ils ont fait un avis. L'avis est public sur le site de mon homologue fédéral. Parmi les recommandations : attention, par rapport aux renseignements anonymisés ou non, de bien expliquer, d'être transparents et d'être factuels, de bien expliquer, de donner une information compréhensible aux citoyens, d'avoir une surveillance indépendante, qu'eux voulaient aller regarder sous le capot par la suite. Il y a en a d'autres, là, mais, spontanément, c'est celles qui me... ah oui, et le caractère volontaire, ils conviennent que ça aurait pris un encadrement juridique, mais ils ont dit : Bien, si le gouvernement insiste suffisamment, pour l'instant, ça fait, mais ça prendrait un encadrement juridique.

M. Lévesque (Chapleau) : Merci beaucoup.

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

Mme Rizzy : Merci beaucoup, M. le Président. Bonjour. Merci pour votre présence. Le groupe juste avant vous, c'était la Commission des droits de la personne et droits de la jeunesse, ils ont fait quelques constats, comme par exemple que l'application en question n'a pas encore fait ses preuves, ça a été fait dans l'urgence, c'est développer un faux sentiment de sécurité, et ils sont arrivés à la conclusion de ne pas recommander d'aller de l'avant. Partagez-vous le même avis de ne pas aller de l'avant?

Mme Poitras (Diane) : Je ne sais pas, pour l'instant, de quelle application il s'agit, je ne sais pas quel serait l'objectif spécifique de santé publique. Pour l'instant, nous formulons des recommandations, des principes à respecter si on va de l'avant. Par la suite, j'aurais besoin de regarder qu'est-ce qu'a l'air l'application.

Mme Rizzy : D'accord. Et ici, par exemple, vous avez regardé, j'imagine, celle du fédéral un peu?

Mme Poitras (Diane) : J'ai suivi les travaux de mes homologues.

Mme Rizzy : O.K. Si, par exemple, c'était celle du fédéral, est-ce que ça, vous avez déjà regardé un peu votre... Est-ce que vous avez une opinion là-dessus ou pas encore? Ce sera plus tard?

Mme Poitras (Diane) : En fait, il faudrait regarder le volet provincial, parce que le fédéral a regardé son volet, l'Ontario, son volet, ça ne veut pas dire qu'au Québec on développerait la même chose, la même façon de donner la clé diagnostique en cas de diagnostic positif, que ça serait développé de la même façon. Donc, il faudrait regarder l'écosystème ici, au Québec.

Mme Rizzy : D'accord. Le 31 juillet dernier, le commissaire à la vie privée, au niveau fédéral, écrivait que, par exemple, celle développée par le fédéral, c'était inexact de dire que c'était totalement anonyme. Partagez-vous le même avis?

Mme Poitras (Diane) : Effectivement, ils ont... Et c'est clairement, maintenant, l'évaluation des facteurs relatifs à la vie privée de... Santé Canada le mentionne, que les risques de réidentification sont très faibles, mais qu'ils existent.

Mme Rizzy : Parfait. Parce que je pense que... quand vous mentionnez, à juste titre, qu'il faut que ça soit un consentement libre et éclairé, je crois que c'est important, même, nous, les élus, M. le Président, dans notre langage, de le mentionner parce qu'ici on pourrait induire malencontreusement les citoyens en erreur.

Vous faites mention, dans votre mémoire, de la gestion de la donnée. Donc, par exemple, quelqu'un qui télécharge l'application sur son téléphone serait, par exemple, sur son téléphone, mais par la suite ça s'en va à la Santé publique. Et là c'est la question d'où est-ce qu'on va stocker la donnée. Donc, vous... ça devrait être stocké où?

Mme Poitras (Diane) : En fait, ça dépend. Il y a plusieurs modèles qui existent. Je vais prendre l'exemple...

Mme Rizzy : Voulez-vous que je spécifie, peut-être, ma question? Ça pourrait peut-être vous aider.

Mme Poitras (Diane) : Le modèle décentralisé est moins à risque, donc, que les clés soient conservées sur le téléphone et que l'appariement de si vous avez été en contact avec une personne à risque se fait sur le téléphone. Mais il reste que ça prend un serveur central quelque part pour gérer la clé et envoyer l'ensemble des informations au téléphone.

Mme Rizzy : Est-ce qu'il y aurait un risque... Avec la volonté gouvernementale, qui a été annoncée dès février 2019, que les serveurs du gouvernement, à plus de 80 %, seraient privatisés, est-ce que ça aussi, ça pourrait être un danger ou est-ce que vous recommanderiez que, par exemple, tout ce qui a trait à la santé publique reste du contrôle gouvernemental?

• (10 h 20) •

Mme Poitras (Diane) : Bien, c'est sûr qu'il faudrait voir... mais plus les données sont sensibles, plus il y a un encadrement... plus il y a de risques à envoyer des données sensibles en infonuagique, ça, c'est évident. Il faut voir quelles sont les données puis quel est l'encadrement, quelles sont les ententes. Mais c'est sûr qu'il y a un risque de perte de contrôle.

Mme Rizqy : Tantôt, vous avez parlé de l'objectif légitime recherché. Donc, on a une solution qui nous est proposée, qui a été davantage proposée d'abord par l'industrie, Apple, et Google, et par la suite Shopify, qui nous propose ce type de technologie. Moi, je me pose la question, où est l'objectif? Mais habituellement, quand on a une solution, c'est parce qu'on a un problème à répondre. Est-ce que vous avez fait l'exercice de regarder en quoi cette application nous aurait été utile dans la préparation de la pandémie, c'est-à-dire l'achat de masques, prendre des décisions dans la distribution du matériel sanitaire auprès de la Santé publique, ou est-ce que vous pensez qu'on aurait peut-être dû, nous, avant d'aller de l'avant avec cette solution proposée, attendre d'avoir les conclusions d'un rapport indépendant dans la gestion de crise pour savoir si, oui ou non, l'objectif recherché est légitime ou pas?

Mme Poitras (Diane) : En fait, il faudrait voir quel serait l'objectif. Dans ma compréhension, il y a différents types d'applications qui existent, mais prenons celle... canadienne, son objectif est de soutenir la recherche de contacts en identifiant très, très rapidement des personnes asymptomatiques pour qu'elles aillent se faire dépister, tester et éviter... diminuer le risque de la chaîne de contamination.

Mme Rizqy : Je vous pose la question suivante parce que j'ai souvent entendu, au niveau fédéral, le commissaire à la vie privée demander des lois avec plus de mordant et plus de ressources parce que les délais sont quand même longs lorsqu'il y a une plainte qui est logée. On parle des fois de deux ans, des fois trois ans et des fois quatre ans. Et, dans un cas très spécifique, il y a eu, par exemple, le programme de reconnaissance faciale dans un centre d'achats en Alberta, et ça fait maintenant plus de deux ans qu'on attend les conclusions du rapport. De votre côté, est-ce que vous avez besoin de lois avec plus de mordant, avec toutes ces nouvelles technologies qu'on essaie de nous vendre, et des ressources additionnelles pour répondre aux demandes?

Mme Poitras (Diane) : Oui.

Mme Rizqy : Parfait. C'est une réponse très courte.

Mme Poitras (Diane) : Ce sera bref.

Mme Rizqy : Parce que, je vous donne un autre exemple, je ne sais pas si vous vous rappelez, en avril 2018, Facebook disait... partait... ou, même, disait des fois : On part avec une bonne intention lorsqu'on est capables de voir où sont nos amis. Alors, plusieurs ont téléchargé l'application, et, au palais de justice, on s'est rendu compte que certains avocats avaient trouvé la faille et étaient capables d'identifier les membres d'un jury, et ça avait beaucoup inquiété les membres du Barreau, avec raison, parce qu'on doit absolument garder anonymes les membres du jury. Mais quelle a été la conséquence pour les avocats puis Facebook lorsqu'on a appris tout ça? Il n'est rien arrivé, finalement. Et c'est là qu'au fond moi, je m'interroge, parce qu'on développe plein de technologies, on prend plein de données dans le secteur privé, mais ils n'ont pas démontré leur capacité à bien gérer la donnée des gens. Et vous, aujourd'hui, est-ce que, si jamais le gouvernement va de l'avant... Je comprends que tout le monde dit : Ça va nous prendre un chien de garde pour s'assurer que tout va bien, mais les conséquences, quand ça ne va pas bien, c'est quoi, aujourd'hui?

Mme Poitras (Diane) : Bien, c'est sûr que, dans les pays qui ont légiféré, notamment pour interdire d'exiger de quelqu'un qu'il utilise l'application ou de voir son contenu, on a imposé des sanctions, aussi, sévères. Je pense que ça irait de soi, là. Il ne suffit pas d'interdire dans la loi, il faut qu'il y ait une sanction qui aille avec et une possibilité d'enquêter, d'imposer ces sanctions de façon efficace, et il faut que ça soit dissuasif.

Mme Rizqy : Mais, lorsqu'on regarde, par exemple, Apple, qui était la première entreprise qui a fait plus que 1 000 milliards de capitalisation boursière, par exemple, une amende de 5 milliards de dollars, ça peut sembler impressionnant, mais, pour eux, c'est très peu. Est-ce que vous pensez qu'à un moment donné ça doit devenir une responsabilité des administrateurs d'une entreprise, lorsqu'il y a des... vraiment, où est-ce qu'on voit que la vie privée a été complètement bafouée, des gens, et que les données se retrouvent dans l'espace public pour, à un moment donné, avoir des lois qui feront en sorte que les géants du Web, notamment, à force de croiser nos données, respectent davantage notre droit à la vie privée? Parce que j'ai l'impression qu'on banalise de plus en plus notre droit à la vie privée.

Mme Poitras (Diane) : C'est une piste intéressante. Moi, je vous dirais qu'il y a beaucoup de travail qui se fait au niveau international. Pour la communauté internationale des homologues sur la protection des renseignements personnels, c'est très, très important et c'est ce qu'on essaie de voir, parce que peut-être qu'une amende de 5 millions ou 5 milliards, ce n'est pas beaucoup, mais, si on est plusieurs pays à l'imposer pour le même événement, à un moment donné, ça commence à finir par faire mal puis ça fait mal à la réputation.

Mme Rizqy : Oui, absolument. Et j'aimerais revenir sur l'employeur. Présentement, nous, on étudie pour... au niveau gouvernement, mais ça n'empêche pas que les entreprises, eux autres aussi, là, sont en train de faire des applications pour se doter de technologies pour aussi suivre leurs employés, et je me demande... Même si on dit que ça devrait avoir un caractère volontaire, les personnes les plus vulnérables, les plus stigmatisées, bien, si leur employeur leur dit : Tu vas le faire, habituellement, ce n'est pas eux autres qui vont porter plainte, n'est-ce pas, parce que des fois leur emploi est précaire, et ils peuvent avoir peur de perdre leur emploi, et ils peuvent dire : Bon, je vais le faire, et peut-être même qu'ils ne connaissent même pas leurs droits.

Mme Poitras (Diane) : Bien, c'est sûr qu'il y a une partie qui va porter plainte, une partie, non, mais, bon, je peux vous dire qu'on reçoit des plaintes de toutes formes, de toutes les sphères de la population, là.

Mme Rizqy : O.K., mais ça, est-ce qu'il y a un risque que les gens qui... notamment les nouveaux arrivants, ceux qui sont plus... qui ne maîtrisent pas nécessairement la langue et qui, par conséquent, maîtrisent encore moins leurs droits, est-ce qu'ils seraient désavantagés dans leur connaissance du droit ou, justement, du droit à la vie privée?

Mme Poitras (Diane) : Oui, c'est sûr que c'est un risque. C'est pour ça qu'on mentionne d'avoir une information claire, avec le nom d'une personne-ressource aussi, pour être en mesure d'appeler, au besoin, s'ils ont des questions et qu'on puisse les informer adéquatement de leurs droits.

Mme Rizqy : Et, à très, très courte échéance, parce que je sais que le temps file, si jamais... En ce moment, là, moi, je suis... Là, vous dites qu'il y a une enquête en cours parce que vous avez reçu une plainte puis qu'il y a déjà un employeur... puis je ne vous demande pas de... aucune information par rapport à cela, mais, présentement, est-ce qu'on devrait se doter d'un outil pour contraindre les employeurs immédiatement, là, que ce soit par décret ou par loi, là...

Mme Poitras (Diane) : C'est sûr que, dans la mesure où ce serait non nécessaire de le faire parce que les conclusions de l'enquête ne sont pas rendues, évidemment, c'est sûr que ce flou au niveau... il y a un certain flou au niveau de la loi et un manque de mordant... fait qu'on risque d'être inondés et de refaire des enquêtes à répétition sur la même problématique, et un outil législatif pourrait être intéressant.

Mme Rizqy : Merci.

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

M. Nadeau-Dubois : Merci, M. le Président. Bonjour à vous. Merci d'être ici avec nous ce matin.

Je me permets de continuer dans la foulée de ma collègue de Saint-Laurent. Êtes-vous d'accord avec moi si je... Êtes-vous d'accord avec l'information suivante? Je dirais qu'actuellement une application qui serait lancée demain matin sans qu'il y ait aucune modification au cadre juridique québécois, cette application-là évoluerait dans un flou juridique.

Mme Poitras (Diane) : Ce ne serait pas complet, mais il y a certains pans importants, de principes importants, dont j'ai mentionné... que nous mentionnons dans le mémoire, qui ne seraient pas encadrés.

M. Nadeau-Dubois : Donc, qui seraient flous. Il y aurait un flou juridique à plusieurs égards.

Mme Poitras (Diane) : Oui, en tout cas sur des aspects importants.

M. Nadeau-Dubois : Parfait. Sans une modification législative correspondant, grosso modo, à ce que vous recommandez à votre recommandation 11, est-ce que, sans une telle modification législative, il y aurait des dangers significatifs pour la vie privée et les renseignements personnels des Québécois et des Québécoises si une application était lancée demain matin?

Mme Poitras (Diane) : On considère que... toujours, on est dans le théorique, là, je ne sais pas le niveau d'atteinte à la vie privée de l'application qui serait déployée, mais, oui, il y aurait des risques qui ne seraient pas encadrés par une telle application.

M. Nadeau-Dubois : Je vais vous faire répéter quelque chose qui est écrit dans le mémoire, mais j'ai envie de vous entendre le dire. J'ai remarqué que vous parlez non pas seulement de cadre juridique, dans votre recommandation 11, mais d'un cadre juridique spécifique. Et donc est-ce que je comprends bien l'esprit de votre recommandation en disant que ce que vous recommandez, ce n'est pas que des ajustements mineurs soient faits à des lois actuelles, mais qu'un cadre juridique spécifique soit adopté pour encadrer spécifiquement une application de lutte contre la COVID-19?

• (10 h 30) •

Mme Poitras (Diane) : Ce serait idéal, parce qu'il y a des enjeux particuliers liés à cette mesure qu'on veut exceptionnelle, et donc, dans l'idéal, cette loi n'aurait plus sa nécessité une fois que l'application serait mise hors service. Mais il y a des pays qui ont intégré ces dispositions-là dans la loi-cadre. Puis, comme je vous dis, moi, je me contenterais de tout encadrement juridique qui serait adopté.

Le Président (M. Bachand) : Rapidement, M. le député.

M. Nadeau-Dubois : Est-ce que les lois avec lesquelles vous travaillez, actuellement, comme commission ont été rédigées à une époque où les technologies dont on discute aujourd'hui existaient?

Mme Poitras (Diane) : Non, évidemment.

M. Nadeau-Dubois : Merci.

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

M. Ouellet : Merci beaucoup, M. le Président. Donc, vous êtes la troisième commission qui vient nous dire l'importance d'avoir un suivi de l'application pour s'assurer qu'il n'y a pas... sans dire «de débordements», mais de mauvaises utilisations ou, du moins, on est capables de monitorer ce qui se passe pour, un, améliorer l'application, mais surtout être certains d'avoir des mécanismes de reddition de comptes. Donc, ça, je pense que c'est important, j'en avais parlé en début de commission.

J'aurais peut-être une question pour vous. Le gouvernement assure que sa solution qui sera retenue sera soumise à l'examen du Centre gouvernemental de cyberdéfense. Est-ce que vous avez été approchés, vous, par le gouvernement afin de faire aussi l'examen de l'application qui sera choisie?

Mme Poitras (Diane) : Je ne sais pas si on le serait, mais j'en prendrais l'initiative et je ferais moi-même mon examen sous le capot, comme je le disais, des éléments de sécurité.

M. Ouellet : Donc, vous n'attendriez pas la demande gouvernementale de l'étudier. Vous le feriez de votre propre initiative, comme organisation, pour donner un avis.

Mme Poitras (Diane) : Dans la mesure où le gouvernement détient des renseignements, nous pouvons exiger des questions et on peut faire enquête de notre propre initiative.

M. Ouellet : Pourquoi prendre cette initiative?

Mme Poitras (Diane) : Pour nous assurer que ce qu'on affirme... pour qu'on ait une analyse indépendante de la situation et nous assurer que les droits des citoyens sont respectés.

M. Ouellet : Donc, on vous écoute aujourd'hui en commission, selon votre champ d'études et votre champ d'expertise, sur une application probable qui n'a pas encore été déterminée de façon finale. Donc, je crois comprendre que, lorsque le gouvernement aura décidé quelle est l'application, ça pourra être une tout autre que celle qui a pu être évoquée dans les médias. Je serais intéressé, moi, comme député d'opposition, à recevoir vos recommandations, parce que, là, j'en ai une partie, aujourd'hui, sur un théorique, mais je suis un gars assez pratico-pratique et, quand je ne maîtrise pas tout, j'aime m'entourer d'experts compétents et chevronnés, et donc j'espère, et je vous fais la demande, bien honnêtement, Mme la présidente, de recevoir par courriel ou de déposer à la commission vos recommandations suite au choix du gouvernement par rapport à la mise en application d'une nouvelle application.

Mme Poitras (Diane) : Comme on a mentionné dans notre mémoire, pour nous, c'est clair que l'avis de la commission devrait être public, même.

M. Ouellet : Merci.

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

M. Ouellette : Merci, M. le Président. Bonjour à vous deux. J'ai été un peu surpris, à la lecture de votre mémoire, parce que j'avais l'impression... Dans le document de consultation en ligne du gouvernement, on réfère, à la page 8 du document, à la Loi d'accès aux documents, puis ça nous donne l'impression, là, que la consultation en ligne est conforme à absolument tout ce qui touche la Loi d'accès. Avez-vous été consultés avant que ça prenne forme, la consultation en ligne du Secrétariat du Conseil du trésor?

Mme Poitras (Diane) : Non.

M. Ouellette : Vous n'avez pas été consultés.

Mme Poitras (Diane) : Pas à ma connaissance, en tout cas.

M. Ouellette : Bon, dans vos recommandations, il y a une chose qui a attiré mon attention, c'est que vous dites... Votre première recommandation, la première chose que vous nous dites, vous nous dites que ce qui devrait être fait devrait être basé sur la science. Ça, ça semble être quelque chose qui est très important parce que vous le mettez dans votre première recommandation, puis vous finissez avec le cadre législatif. Donc, on parle de science, si jamais on a à régler une problématique, pas un sondage, là, on parle de science. Il faut vraiment que ce soit factuel et qu'on soit en mesure de démontrer à la population qu'on s'en va dans la bonne direction.

Mme Poitras (Diane) : En fait, l'objectif de l'application doit être fondé sur la science, c'est-à-dire qu'on doit dire... On pense qu'un objectif de santé publique qui serait x, y, z, basé sur la science, l'application pourrait nous aider à atteindre cet objectif-là. C'est de ça qu'on parle.

M. Ouellette : O.K. Et à votre recommandation 11, on parle du cadre législatif. Bon, vous semblez, à défaut de rien, vous accommoder de peut-être un décret, là, parce que ça s'est passé ailleurs. Et moi, j'ai un peu peur des décrets parce qu'on est en état d'urgence sanitaire, et un décret en urgence sanitaire, c'est un décret gouvernemental sans imputabilité, là, que le gouvernement décide. Un cadre législatif, c'est beaucoup mieux parce que c'est sujet à l'idée des 125 députés de l'Assemblée nationale.

Je veux juste que vous me précisiez, votre décret, là, si... un décret par l'état d'urgence sanitaire, c'est-tu quelque chose auquel vous avez pensé? Parce que c'est la première chose qui m'est venue en tête, que ça soit un décret imposé par le gouvernement.

Mme Poitras (Diane) : En fait, je réitère que... C'est sûr que la loi, avec le débat démocratique, elle implique... sur une réelle application concrète serait idéale, mais je me contenterais d'un décret, peu importe le... Moi, tout cadre juridique serait mieux que rien.

Le Président (M. Bachand) : Sur ce, je vous remercie infiniment d'avoir participé aux travaux de la commission, et je suspends les travaux quelques instants. Merci beaucoup.

(Suspension de la séance à 10 h 36)

(Reprise à 10 h 49)

Le Président (M. Bachand) : À l'ordre, s'il vous plaît! La commission reprend ses travaux.

Alors, nous avons le plaisir d'accueillir monsieur... le Pr Benoît Dupont, directeur scientifique, Réseau intégré sur la cybersécurité de l'Université de Montréal. Alors, M. Dupont, vous avez 10 minutes de présentation, et après ça on aura un échange avec les membres de la commission. Bienvenue.

M. Benoît Dupont

M. Dupont (Benoît) : Merci, M. le Président. Mmes et MM. les députés, merci pour l'invitation à réfléchir devant vous lors de cette consultation sur les applications de notification.

Comme je l'ai cependant déjà écrit dans un article qui a été repris dans *Le Soleil*, même si cette consultation porte sur les applications de notification, il y a plein d'autres technologies qui sont aussi développées pour essayer de lutter contre la COVID-19, qui vont de l'intelligence artificielle à la reconnaissance faciale en passant par l'usage de drones, et je pense que les enjeux qui sont discutés dans cette commission ne s'appliquent pas uniquement aux applications mais aussi à toutes ces autres technologies, dont certaines vont probablement ou pourraient porter atteinte aux libertés individuelles et à la protection de la vie privée. Alors, je vais articuler les 10 minutes que j'ai en deux grands moments. Le premier, c'est sur une réflexion sur les obstacles à l'efficacité de ce type d'application, et le deuxième moment, sur les enjeux de sécurité et de vie privée.

• (10 h 50) •

J'ai regardé les interventions, hier, et j'ai vu que beaucoup de questions et beaucoup de réflexions portaient sur le seuil à partir duquel... le nombre de téléchargements de ces applications à partir duquel on atteint une certaine efficacité. Donc, c'est effectivement très important. J'ai entendu des études citées qui vont de 40 % à 60 % de la population qui doit télécharger ce type d'application. On sait aussi qu'on pourrait probablement atteindre des effets positifs en deçà de 40 %, mais ça reste très hypothétique. Le problème, c'est qu'on n'a parlé, jusqu'à présent, que du nombre de téléchargements, c'est-à-dire combien de... quel est le pourcentage de la population qui va la télécharger. Ce dont on n'a pas encore discuté mais ce qui est beaucoup plus important, c'est combien... quels sont les taux d'utilisation active, c'est-à-dire combien des gens qui ont téléchargé ces applications vont réellement les utiliser sur leur téléphone intelligent au quotidien.

Et on a la chance d'avoir, avec l'exemple de la France, quelques statistiques qui sont loin d'être encourageantes, puisque l'application StopCovid, en France, lors du premier mois, a été téléchargée par seulement 2 % de la population, ce qui est assez peu, évidemment, au vu des chiffres dont on a discuté hier. Un mois plus tard, c'était monté à 4 % de

la population. Mais ce qui est plus intéressant, c'est que seulement 25 % des gens qui avaient téléchargé l'application, donc 25 % de 4 %, l'utilisaient de façon active, et 20 % l'avaient désinstallée de leur appareil intelligent.

Donc, non seulement l'enjeu, c'est de convaincre une large proportion de la population de télécharger ces applications, mais un enjeu secondaire tout aussi important, c'est celui de convaincre les gens de l'utiliser au quotidien — il y a beaucoup de problèmes techniques, notamment avec certains appareils Apple, pour des raisons que je maîtrise moins bien mais que mes collègues informaticiens pourront vous expliquer — mais aussi de ne pas désinstaller l'application, ce qui reflète aussi un manque de confiance de la population dans ce type d'outil.

Et un autre exemple assez intéressant sur lequel on commence à avoir un peu de recul, c'est celui de l'Australie, qui fait face à une deuxième vague de contagion, notamment dans l'État du Victoria, à Melbourne. Et là l'analyse de l'application, qui est déployée depuis trois mois maintenant, montre que les jeunes de 18 à 24 ans sont deux fois moins susceptibles de télécharger l'application que les personnes âgées de 55 à 74 ans. Donc, on pourrait imaginer que ce serait l'inverse parce que les jeunes sont plus adeptes avec les nouvelles technologies, mais... Excusez-moi, je vais revenir en arrière. Non seulement ils la téléchargent deux fois moins, mais c'est eux qui propulsent la deuxième vague de contagion par leurs comportements. Donc, on a un problème parce que les gens qui la téléchargent et l'utilisent le moins sont ceux qui seraient... qui en bénéficieraient le plus, mais on a un certain nombre d'obstacles et... de confiance.

Et donc, dans cette deuxième vague, les autorités sanitaires du Victoria, après une semaine à avoir tenté d'utiliser l'application, l'ont carrément abandonnée. C'est une application fédérale, mais utilisée par chacun des États, et l'État... les autorités sanitaires l'ont abandonnée parce qu'elle ne leur servait à rien et elle venait interférer avec les activités des équipes de traçage manuel. Donc, elle créait trop de pression, avec un bénéfice jugé comme étant négligeable. Donc, ils l'ont... le ministre de la Santé du Victoria a déclaré qu'ils ne s'en serviraient plus jusqu'à nouvel ordre, jusqu'à ce qu'ils aient récupéré un contrôle sur la maladie. Donc, ça, c'est pour les taux d'adoption.

Hier, vous avez aussi discuté de la technologie Bluetooth, du choix des technologies, GPS versus Bluetooth. Je pense que c'est important de comprendre les problèmes de fiabilité, aussi, à ces technologies. Je ne suis pas, encore une fois, un informaticien, mais j'ai lu quand même quelques témoignages des inventeurs du protocole de communication Bluetooth, qui expriment de très fortes réserves à l'utilisation de leur technologie, la technologie qu'eux-mêmes ont inventée, en disant : Bien, elle est très... elle est excellente pour un certain nombre de fonctionnalités, mais, pour calculer la distance entre deux appareils mobiles, ce n'est absolument pas suffisamment robuste. Ce sont des ondes radio, il y a trop d'interférences avec l'environnement physique immédiat, que ça soit construit, que ça soit végétal, il y a trop de distorsions dans les ondes pour qu'on puisse mesurer avec fiabilité la distance entre un appareil émetteur et un appareil récepteur, ce qui crée beaucoup plus de faux négatifs et de faux positifs que nécessaire, avec les faux négatifs anxiogènes et des faux positifs qui poussent un peu à des comportements plus complaisants de la part des gens qui ne pensent pas être contaminés alors qu'ils le sont. Ça, ce sont les aspects techniques.

Il y a aussi des obstacles à l'efficacité qui sont des obstacles épidémiologiques. On sait depuis quelques semaines maintenant qu'un certain nombre d'individus ou d'événements sont des superpropagateurs de la maladie. Très simplement, ce que ça veut dire, c'est que 10 % à 20 % des personnes infectées sont responsables de 80 % des infections secondaires et que 70 % des personnes infectées ne vont jamais contaminer personne d'autre au cours de leur maladie. Et ça, les applications de notification n'ont aucun élément contextuel pour savoir qui est un superpropagateur et qui ne l'est pas. Et, dans les superpropagateurs, 40 % des gens n'éprouvent aucun symptôme de la maladie, donc ils n'ont aucune raison d'aller se faire tester et aucune raison de rentrer dans leur application qu'ils sont contaminés pour qu'on retrace les gens avec qui ils ont été en contact.

Et même les applications du style COVI, dont Yoshua Bengio parlait hier, qui travaillent en amont avec... en récoltant les informations sur les symptômes des utilisateurs directement, auraient de la difficulté avec ce type de pattern, parce qu'évidemment les gens n'éprouvant aucun symptôme tout en étant malade ne rentreraient pas ces symptômes-là, et l'intelligence artificielle ne pourrait pas détecter qu'ils sont infectés. Donc, ça, ça pose aussi, quand même, cet événement... enfin, cette réalité, nouvelle réalité des superpropagateurs, réalité scientifique, un problème, parce que les modèles d'efficacité de ces applications qui ont été conçues sont... reposent sur un principe de linéarité, c'est-à-dire tout le monde est infectieux de la même façon, et on découvre que ce n'est pas vrai du tout.

Et dernier élément, c'est un élément comportemental aussi, on a la chance, avec l'Australie, de voir comment les gens se comportent face à une deuxième vague, face à l'épuisement, à la fatigue de maintenir la distanciation sociale pendant plusieurs mois, et on voit que, dans la deuxième vague, en Australie, dans l'État de Victoria, où 3 000 personnes ont été testées positives, quand les autorités de santé publique ont fait du porte-à-porte pour savoir si les gens respectaient leur confinement et leur quarantaine, plus de 800 étaient introuvables, donc ils n'étaient pas chez eux au moment où ils auraient dû être en quarantaine stricte parce qu'ils avaient été testés comme étant positifs par les autorités.

Donc, il y a toute une réalité, aussi, qui est que les humains, quand ils reçoivent ce type d'information, ne se comportent pas nécessairement comme des êtres rationnels. Et on doit intégrer ça aussi dans la manière dont on envisage l'utilisation de ces applications, parce qu'il y a plein de gens qui vont recevoir une notification positive, et qui ne vont pas modifier leurs comportements, et qui vont continuer à se comporter de façon très risquée pour l'ensemble de la société. Donc, je pense qu'il faut comprendre aussi ça. Il y a beaucoup de travaux en économie comportementale qui expliquent notre inaptitude, en tant qu'humains, à interpréter les données relatives aux risques pour nous et pour notre entourage. Donc, ça, ce sont les enjeux d'efficacité.

Je ne sais pas combien de temps il me reste, mais, assez rapidement, les enjeux de sécurité et de vie privée. Évidemment, ces applications sont développées par des organisations qui sont plus... qui relèvent plus de la santé

publique et qui ne sont pas forcément... qui n'ont pas forcément l'expertise technique spécifique en matière de sécurité dans des environnements d'applications de téléphonie mobile qui sont très problématiques. Pour vous donner quelques exemples, des entreprises comme Google et Apple ont elles-mêmes des défis énormes. J'ai vérifié cette semaine, le système Android de Google possède 6 300 vulnérabilités recensées à la date... cette semaine par l'institut national des standards et des technologies américain, la technologie... le système d'exploitation iOS d'Apple, 3 700 vulnérabilités recensées — ça, ce sont par les concepteurs mêmes des systèmes d'exploitation, imaginez ceux qui conçoivent les applications et qui ne disposent pas de toute l'expertise technique de ces entreprises — technologie Bluetooth, 400 vulnérabilités recensées. Ça veut dire que, si vous développez des applications pour ces systèmes, bien, vous devez disposer de l'expertise pour vous assurer que vous n'introduisez pas ces vulnérabilités ou que vous ne les laissez pas persister dans votre application, ce qui est très difficile. Et, en juin 2020, une entreprise de cybersécurité qui s'appelle Guardsquare a analysé 17 applications qui avaient été déployées en juin et, sur les 17, il y en avait 16 qui étaient extrêmement faciles à pirater et à analyser pour mener des attaques de sécurité.

Le Président (M. Bachand) : Merci, Pr Dupont. Vous êtes juste sur le 10 minutes, en passant, bravo! Alors, Mme la députée de Jean-Talon, s'il vous plaît.

Mme Boutin : M. Dupont, merci d'être là. J'aurais à peu près... Je pense qu'on pourrait discuter très, très longuement, c'est extrêmement intéressant. Vous nous avez amenés sur plusieurs territoires, là, qui nous amènent à nourrir, là, beaucoup, beaucoup la réflexion.

Bien, si je vous entends, honnêtement, moi, je suis très inquiète. Outre l'application, à la base, là, tu sais, je pense que tout le monde, ici, on devrait se poser certaines questions par rapport à nos téléphones intelligents, là, mais, bon, nous sommes tous à risque, j'imagine.

On parlait de la technologie Bluetooth, puis, bon, bien, je pense que vous comprenez pourquoi on a écarté d'autres technologies de géolocalisation ou GPS, parce que, toujours... on soupèse toujours le contre entre, bon, une plus grande efficacité à collecter des données de santé pour contribuer, justement, à contrer une pandémie ou autre, bon, on a écarté ces choix-là à la base, là, pour considérer seulement le Bluetooth. Moi, je me demande... admettons qu'on pèse le contre... le pour et le contre, la technologie Bluetooth nous permettrait peut-être de protéger plus la vie privée, mais est-ce que c'est la meilleure technologie? Parce qu'au départ... mais vous n'en avez pas parlé beaucoup dans votre présentation, mais, au début de votre présentation, vous avez parlé... il existe d'autres technologies. Est-ce que c'est la moins pire des technologies? Est-ce que c'est la meilleure ou est-ce qu'il y en aurait d'autres, des technologies? Puis on s'entend que la technologie, ici, là, ce n'est pas une manne, là, c'est toujours complémentaire et un outil qui permet d'être plus efficace, simplement. Qu'est-ce que vous auriez à dire là-dessus?

• (11 heures) •

M. Dupont (Benoit) : Bien, je pense que, dans le contexte plus restreint des applications de notification, donc, qui doivent être installées sur des téléphones mobiles et intelligents, c'est certain que c'est assez binaire, les choix : c'est soit le Bluetooth, soit le GPS. Je pense que le choix a été fait, à mon avis, à bon escient dans le contexte de la protection de la vie privée dans lequel on opère au Québec. On n'est pas en Chine, là. Donc, je pense que, le Bluetooth, c'est la seule option qui est disponible.

Mais mon propos n'est pas de dire qu'on ne devrait pas choisir le Bluetooth plutôt et choisir le GPS parce que c'est un peu plus fiable — ceci dit, il y a des problèmes aussi avec le GPS selon où vous êtes — c'est simplement de dire : Comprenons aussi les limites de cet outil-là et essayons d'imaginer comment on pourrait les surmonter. Et ce que j'entends dans les propos de beaucoup de personnes qui sont les... qui se font les avocats de ces applications, est une tendance à minimiser les défis techniques ou les erreurs, le taux d'erreurs va générer le Bluetooth, et je pense qu'il faut vraiment... en faisant ce choix-là, il faut vraiment qu'on soit conscients de ces limites-là et qu'on les intègre dans notre façon d'imaginer l'utilisation et le déploiement de certaines de ces applications parce qu'on va devoir aussi gérer les effets iatrogéniques, c'est-à-dire les effets négatifs d'indiquer à des gens qu'ils sont peut-être contaminés alors qu'ils ne le sont pas du tout et d'indiquer à des gens qu'ils ne sont pas contaminés alors qu'ils le sont, infectés, et qu'ils vont propager la maladie, et qu'ils l'apprendront plus tard, et qui vont...

Donc, il faut vraiment comprendre assez finement les limites de ces technologies, mais je n'ai pas de technologie de remplacement à proposer, malheureusement, et je pense que, sur les appareils, téléphones mobiles présentement à la disposition de 85 % de la population, c'est à peu près l'option unique, je pense, si on exclut d'emblée le GPS.

Mme Boutin : O.K., je vois. Peut-être que je me trompe, là, mais... puis j'essaie de rendre ça de manière assez concise et claire, il y a l'enjeu des données, quels types de données on va collecter. Bon, on s'entend, le gouvernement ne veut pas collecter de données personnelles, et, pour rassurer Mme la députée de Saint-Laurent, les données, toutes les données qui sont sensibles au gouvernement vont toujours être stockées par le gouvernement, encryptées et protégées, c'est très important. Mais, dans le cadre de cette application-là, la seule donnée qui pourrait provenir du gouvernement, c'est un identifiant généré par la Santé publique, là, c'est le modèle un petit peu comme le fédéral.

Donc, il y a le volet données puis la gestion des données, puis il y a le volet de l'appareil lui-même, là, la technologie Bluetooth. Est-ce qu'il y a des mesures d'atténuation? Ou qu'est-ce qui peut être mis en place, le maximum, pour essayer d'atténuer les effets négatifs et s'assurer d'une protection de la vie privée au maximum?

Est-ce que c'est au niveau des infrastructures technologiques? Une gouvernance? Toutes ces réponses? Un suivi d'évaluation? On se pose toutes ces questions-là.

M. Dupont (Benoit) : Bien, je pense que c'est... Vous venez... Enfin, je pense que vous connaissez déjà un petit peu la réponse, c'est-à-dire, c'est la mise en place d'une infrastructure de gestion qui soit... qui permette un encadrement serré de ce type de technologie là. Mon propos sur le Bluetooth... ce n'est pas une menace à la vie privée, c'est plutôt une question d'efficacité. Pour la vie privée, c'est l'encryptage des données, très robuste, les données quand elles circulent et les données quand elles sont aussi au repos, c'est-à-dire quand elles sont stockées dans des serveurs, qui y a accès, et d'avoir aussi une surveillance et des audits réguliers sur la façon dont ces données-là sont utilisées.

Et peut-être une initiative, là, qui m'apparaît intéressante, qui a été utilisée par les autorités françaises quand elles ont déployé StopCovid, c'est qu'elles ont lancé un processus de chasse aux bogues, c'est-à-dire qu'elles ont ouvert le code et elles ont invité tous les pirates informatiques bienveillants, pas les pirates qui travaillent pour des puissances étrangères et qui voudraient déstabiliser notre société, mais des hackers — il y en a beaucoup qui travaillent dans le secteur privé, au Québec comme ailleurs — en disant : Bien, testez notre application, vous avez un mois, on va vous donner des primes si vous trouvez des vulnérabilités — il y en a une vingtaine qui ont été découvertes — parce que ça permet d'élargir au-delà des autorités et de l'expertise gouvernementale, qui est, par définition, limitée, pour bénéficier, justement, d'abord d'une expertise plus profonde et, deuxièmement, aussi d'une plus grande confiance de la part de la société, en disant : Bien, voilà, il y a des hackers qui ne sont pas connectés avec le gouvernement qui ont testé l'application et qui pensent qu'elle est probablement pas parfaite, mais les erreurs habituelles ou les plus fréquentes d'autres applications ont été vérifiées, et elles n'existent pas dans cette application-là, et cette application... Donc, vous avez un processus transparent de vérification dans... qui est, à mon avis... qui rajoute une couche supplémentaire de confiance, au-delà de tout le travail... Et ce n'est pas pour dénigrer le travail des autorités comme le centre de cybersécurité ou le Centre canadien pour la cybersécurité, je pense que c'est complémentaire, mais ça élargit un peu le débat et ça permet également... parce que toutes les applications... alors, quelques applications sur lesquelles ont détecté des problèmes de sécurité, tous ces problèmes-là ont été détectés par des tierces parties, c'est-à-dire des gens qui n'étaient pas impliqués dans le développement de ces applications ni du côté industriel ni du côté gouvernemental, et ça, il faut en tenir compte aussi. Il y a plein de gens qui sont capables de contribuer, justement, à s'assurer que ces applications sont robustes.

Mme Boutin : Dernière question, parce que mes collègues en ont : Est-ce que-vous savez si, justement, Santé Canada a fait ça? Parce que le code est ouvert, là, sur GitHub, ils l'ont publié. Est-ce que vous savez si c'est une initiative...

M. Dupont (Benoit) : J'ai essayé de le vérifier, mais je n'ai pas trouvé d'information parce que c'est un processus qui doit utiliser une procédure particulière et des plateformes. À ma connaissance, non, mais il est possible qu'ils aient informellement invité des hackers à participer à la révision du code.

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

Mme Lecours (Les Plaines) : Merci beaucoup, M. le Président. Tout d'abord, merci beaucoup pour votre présentation, ça suscite effectivement beaucoup de questions.

Moi, c'est le côté vraiment comportemental, j'aime beaucoup vos réflexions, ce serait intéressant d'y trouver, justement, des solutions. Vous parlez... Un des obstacles à l'efficacité, c'est l'utilisation de façon active. Ce que vous dites, ce que j'en comprends, puis corrigez-moi si je me trompe dans ma compréhension, c'est que, bon, les gens... On va parler où le téléchargement s'est fait et qu'il y a eu... voyons, du débranchement, en fait, si tu télécharges l'application, ton utilisation peut être aussi dans les opportunités de dire : J'ai une notification, je vais... moi, je ne vais pas nécessairement me faire tester parce que je sais un peu ce que j'ai fait dans les dernières semaines puis de la façon dont je me suis comportée, mais je vais me retirer pendant deux semaines. Est-ce que, pour vous, c'est une personne qui est inactive, ça? Non?

M. Dupont (Benoit) : Non, ça, c'est une personne, au contraire, qui est très active puisqu'elle utilise l'application selon les intentions de ces concepteurs.

Mme Lecours (Les Plaines) : ...n'est pas allée se faire tester.

M. Dupont (Benoit) : Non, elle n'est pas allée se faire tester, mais elle se met en retrait, en confinement, donc elle a tenu compte... donc elle a activé... elle utilisé son application, elle a vérifié quand elle avait reçu une notification et elle a agi en fonction des recommandations de la Santé publique, c'est-à-dire de s'isoler socialement.

Moi, l'utilisation active, c'est quelqu'un qui va télécharger l'application, qui va l'utiliser pendant 24 heures, qui va regarder son téléphone, qui va commencer à avoir, peut-être parce que son téléphone est un modèle plus ancien, de l'instabilité dans son système, donc qui ne pourra plus accéder à d'autres applications, ou qui va trouver ça finalement trop contraignant, ou qu'il a un iPhone et qu'il doit déverrouiller l'écran de son iPhone à chaque fois pour que l'application soit active et qui, au bout de 24 heures, va trouver que les bénéfices sont inférieurs aux

inconvenients, et puis il va arrêter d'activer l'application à chaque fois qu'il sort en dehors de chez lui, et donc il aura l'application téléchargée sur son appareil, mais, l'application n'étant pas lancée, elle ne pourra pas, en fait, remplir ses fonctions.

Mme Lecours (Les Plaines) : Toujours dans le même volet, vous dites... vous avez mentionné que, notamment, en Australie, il y a deux fois plus de jeunes, maintenant, qui sont en contact avec la COVID et deux fois moins, je vais dire, de conscientisation, O.K.? C'est ce qu'on vit ici aussi, hein, vous le savez comme nous tous. Pourtant, c'est eux qu'on voudrait aller chercher avec, notamment, une application comme celle-là, si elle était mise de l'avant, parce que c'est leur modèle, c'est leur façon de vivre, les plus jeunes que moi — je vais dire «que moi» — l'utilisent beaucoup plus. Donc, de quelle façon on pourrait, selon vous, les conscientiser à l'importance, si on décide d'y aller avec un téléchargement, et d'une bonne utilisation? Comment est-ce qu'on pourrait faire ça?

• (11 h 10) •

M. Dupont (Benoît) : Bien, je pense que, comme de la manière dont on a agi jusqu'à maintenant, avec des campagnes de marketing social ou de sensibilisation du public massives, parce qu'une fois qu'on a une application... je pense que mon collègue Gingras, hier, avait appelé ça des «bêbelles technologiques», là, mais l'application, en soi, elle n'est rien si elle ne s'articule pas dans un ensemble beaucoup plus... un effort coordonné, synchronisé de promotion des comportements vertueux auprès de certains publics qui sont plus difficiles à rejoindre, ou qui ont de la... parfois, qui ont moins confiance dans les messages des autorités de Santé publique, ou qui sont... on va revenir à mon propos sur les biais cognitifs aussi, qui se sentent invulnérables, donc qui ont des biais de myopie, de simplification face au risque et qui font... et qui s'estiment... ils estiment que le contenu du message est tout à fait légitime — et d'ailleurs c'est propre à tous les humains, ce n'est pas uniquement les jeunes — mais ça s'applique aux autres et pas à moi parce que moi, je suis protégé, et ça, on le voit dans tous les domaines de gestion des risques, que ça aille dans la préparation contre les désastres naturels, les inondations, les gens qui évacuent en dernier les rues inondées, et tout ça. C'est la même dynamique où les gens ont de la difficulté à intégrer les messages d'avertissement et de gestion de risques quand ça les concerne à eux, même s'ils reconnaissent tout à fait la légitimité du contenu du message pour l'ensemble de la population.

Donc, il y a des stratégies à mettre en oeuvre, de communication, qui sont ciblées pour essayer de surmonter un petit peu cet obstacle, pour aider les gens qui en ont particulièrement besoin, justement, de prendre conscience et de les pousser, de les aider, de façon persuasive et non pas coercitive, à utiliser ces applications-là.

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

M. Provençal : Merci, M. le Président. Merci beaucoup pour votre présentation. Vous avez quand même soulevé différents éléments. Un des points sur lesquels je m'interroge, là, c'est le niveau d'adhésion qu'une population peut avoir versus un outil technologique. Croyez-vous que cette adhésion-là est en lien avec le niveau d'efficacité qu'on peut lui attribuer et aussi en lien avec la confiance que l'outil peut donner, une confiance ou une sécurité que cet outil-là peut donner à la personne qui va l'utiliser?

M. Dupont (Benoît) : C'est probablement l'un des facteurs qui va jouer. Je ne suis pas certain que ça soit le seul, mais c'est certainement l'un de ces facteurs. Et je pense que les usagers sont un peu comme nous tous ici, ils ont du mal à voir directement comment le seul fait de télécharger cette application va permettre de combattre et de faire repousser ou de faire redescendre le niveau d'infection. On nous le dit, mais ça reste très abstrait. Les mécanismes très concrets par lesquels on va y arriver restent quand même assez... je ne dirais pas nébuleux, mais très abstraits. Et donc je pense que c'est difficile pour les gens de comprendre le lien direct entre le téléchargement de ces applications et un effet positif, que ça soit sur la société ou sur eux-mêmes et leur entourage immédiat. On comprend que c'est l'objectif qui est recherché, mais comment on va y arriver? Ce n'est pas évident. Donc, je pense que c'est un des facteurs, effectivement, qui joue et qui a de la... qui explique pourquoi, dans tous les pays démocratiques, on a des taux de téléchargements qui sont beaucoup plus faibles que ce qu'on pourrait imaginer dans une situation de pandémie mondiale dans laquelle l'économie menace de s'effondrer, donc il y a une urgence, une urgence manifeste.

Mais je vais faire encore une analogie avec le domaine de la santé, vous savez, dans le domaine des transplantations d'organes, il y a... bien que des gens aient eu une seconde chance, une seconde vie, il y en a toujours 40 % qui ne prennent pas leurs médicaments antirejet, bien qu'ils aient eu une deuxième chance. Donc, il y a toujours quand même ce facteur... pas d'irrationalité, mais de biais qui fait en sorte que, même dans une situation d'urgence, plein de gens vont avoir des comportements qu'on s'explique difficilement de façon rationnelle, mais ça, c'est parce qu'on est humains.

Le Président (M. Bachand) : ...il reste moins d'une minute.

M. Provençal : Merci.

M. Lévesque (Chapleau) : Oui, il reste moins d'une minute, donc rapidement, là, vous avez parlé des hackers en France qui ont participé, dans le fond, à améliorer l'application, est-ce que vous avez connaissance d'autres endroits dans le monde ou peut-être même au fédéral si ça aurait été fait, ça, pour améliorer les applications? Et est-ce

que... Disons qu'on décidait d'aller de l'avant avec une application ici, au Québec, est-ce que ça devrait être fait aussi ou il y aurait d'autres étapes qui devraient être faites pour, justement, maximiser l'efficacité des applications?

M. Dupont (Benoit) : À ma connaissance — mais, encore une fois, il y a tellement d'activités dans ce domaine-là que c'est quasiment difficile de maintenir ses connaissances à jour au fil du temps, là — à ma connaissance, moi, la France, c'est le seul pays qui a mis en place une démarche très structurée, qui est une démarche qui existe dans d'autres domaines applicatifs, là, logiciels. Est-ce qu'on devrait l'envisager au Québec? Moi, je pense que oui, mais en plus, évidemment, des mesures qui sont déjà proposées.

Le centre de cybersécurité devrait avoir du temps pour passer à travers l'application. Je pense qu'il y a le Centre canadien pour la cybersécurité qui est peut-être... qui a peut-être plus de ressources que le centre de cybersécurité, à l'heure actuelle, donc il pourrait aussi certainement, de façon complémentaire, être mis à contribution. Et il y a, au Québec, aussi une industrie de la cybersécurité qui est très développée, et donc il y a plein d'entreprises québécoises qui ont une expertise qui pourrait certainement être mise à contribution pour aider aussi à s'assurer que l'application, qui a été conçue par des experts des applications et pas des experts de la sécurité, soit conforme, et soit respectueuse, et soit suffisamment protégée.

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

Mme Rizqy : Merci beaucoup, M. le Président. Bonjour, merci d'être avec nous aujourd'hui. Vous avez soulevé beaucoup d'éléments fort importants, notamment l'obstacle à l'efficacité. J'aimerais y revenir, car vous soulevez, à juste titre, le phénomène de faux positif et de faux négatif. Alors, par exemple, nous sommes ici, dans cette salle. Si, par exemple, on a des gens qui sont en haut au deuxième, ils pourraient... Si tout le monde télécharge, aujourd'hui, la technologie, si une personne en haut est testée positive, nous, on pourrait recevoir une notification alors qu'on est à distance, on n'est pas au même niveau, et ça pourrait faire aussi en sorte qu'on va tous avoir une invitation d'aller se faire tester. Lorsqu'on est dans une urgence sanitaire, en pleine crise, on sait, par définition, les ressources sont limitées, et on l'a vu au mois de mars et au mois d'avril, que c'était très difficile d'avoir accès aux tests. Est-ce qu'il pourrait y avoir aussi un étau d'étranglement au niveau de la capacité de tester et de tester les bonnes personnes?

M. Dupont (Benoit) : C'est certain que ça va générer des tests additionnels. Donc, est-ce que là... Ça va dépendre, évidemment, de la capacité à offrir ces tests ou pas, mais c'est certain que ça va contribuer, et puis il faut l'intégrer dans la planification, justement, des capacités de test qui sont offertes ou qui sont planifiées.

Mais, a contrario... Vous évoquez l'augmentation du nombre de tests, mais il y a aussi, a contrario, le fait qu'il y a toujours cette population de 40 % des non symptomatiques, asymptomatiques, qui ne vont jamais aller se faire tester bien qu'ils soient porteurs de la maladie et qui, donc, vont aussi faire... créer des faux négatifs de façon telle que la propagation ne pourra pas être arrêtée, probablement, si on ne teste que les gens qui ressentent des symptômes. Alors, je ne suis pas... Je vais m'arrêter là parce que je...

Mme Rizqy : Au contraire, allez-y, parce que c'était la deuxième partie de ma question, faux positif et faux négatif, parce que disons que nous ne sommes pas avec la personne qui est infectée, alors nous, on irait se faire tester parce que nous avons accès à un téléphone intelligent, on a l'application, alors qu'une personne qui est dans une communauté plus vulnérable, qui n'a pas accès à Internet et qui... Habituellement, lorsqu'on est dans les quartiers plus défavorisés, c'est aussi, par conséquent, un quartier qui, souvent, est densément peuplé, et souvent, si on prend toujours l'exemple de Montréal-Nord, 30 % qui n'ont pas nécessairement accès à Internet de façon régulière. Alors, eux pourraient se retrouver avec un risque d'infection plus élevé et très, très loin dans la chaîne de commandement et de prise d'action pour le test, alors encore plus loin dans la chaîne pour avoir accès à la santé, est-ce que je me trompe?

M. Dupont (Benoit) : Disons que mon propos est de dire que, sans des politiques... et, encore une fois, je m'aventure sur un terrain qui est un peu miné pour moi parce que je ne suis pas épidémiologiste, mais sans politique de testage extrêmement agressive... L'application ne va pas se substituer à une politique de testage de toutes les populations, y compris celles qui sont plus fragiles et plus défavorisées.

Mme Rizqy : ...revenir aussi... Vous avez donné l'exemple très précis de l'Australie, qui, eux, avaient l'application et toujours ce que nous, on a toujours, au Québec, la recherche, disons-le, par l'équipe manuelle, donc, de santé publique, qui appelle : Avec qui avez-vous été en contact lors des dernières journées? Par la suite, on appelle les gens, mais aussi, au Québec, on remplit une fiche, sur Internet, des gens avec qui qu'on a été en contact.

Vous avez mentionné, dans votre propos, que ça avait même interféré avec l'équipe de santé publique, l'application, et, par conséquent, ils ont dû l'abandonner. Alors, j'aimerais juste voir avec vous... Nous, ici, au Québec... Tantôt, vous avez dit : On a le choix entre Bluetooth, GPS, et je n'ai pas d'autre option à vous donner. Mais l'Australie a gardé l'option de statu quo, n'est-ce pas?

M. Dupont (Benoit) : ...je n'ai pas d'autre option technique à vous donner, mais il est clair que l'Australie... Et d'ailleurs je n'ai pas eu le temps de terminer là-dessus, mais Singapour a fait la même chose, c'est-à-dire que

Singapour avait été un des premiers pays à développer une application de notification, et, très rapidement, ils ont déchanté parce que, un, malgré la confiance et malgré la discipline de la population, les taux de téléchargement ont été très en deçà des objectifs attendus, et, deuxièmement, les résultats étaient très décevants aussi. Donc, le chef de projet de l'application de notifications de Singapour a déclaré publiquement, «on the record», que ce n'était pas la solution ni maintenant ni à l'avenir, certainement, et que le traçage manuel et les tests à très grande échelle restaient, selon lui, la seule avenue pour contrôler l'infection.

• (11 h 20) •

Mme Rizqy : Il n'y a pas non plus un risque... Lorsqu'on parle de totalitarisme numérique, et là je vais vers Singapour parce que vous le mentionnez, qu'effectivement ils ont abandonné l'application qui utilisait le Bluetooth, mais ils sont allés vers ce que moi, j'appelle souvent la grenouille dans l'eau, là, tranquillement, on monte la température jusqu'à tant que ça bout, puis là, de toute façon, elle est cuite. Dites-moi, Singapour, ils ne sont pas allés jusqu'au bracelet?

M. Dupont (Benoit) : Oui, Singapour utilise le bracelet pour les personnes...

Mme Rizqy : Infectées?

M. Dupont (Benoit) : ...en quarantaine. Donc, on vous donne un bracelet... D'ailleurs, Hong Kong aussi, maintenant. Quand on arrive à Hong Kong, on doit porter un bracelet quand on est en quarantaine, pendant la période de quarantaine, pour être localisé et s'assurer qu'on ne quitte pas son domicile. Donc, effectivement, les pays asiatiques, que je ne cherche pas à citer en exemple pour s'inspirer de... mais ont choisi d'aller, après avoir testé les applications, vers des démarches beaucoup plus intrusives. La Corée du Sud passe à travers toutes les transactions de cartes de crédit et tous les déplacements des téléphones intelligents des personnes qui sont testées positives. Donc là, on est encore dans une autre réalité, je pense, qu'on n'est pas du tout près de voir s'implanter au Québec.

Mme Rizqy : Mais j'imagine que votre avis, ce n'est surtout pas une avenue souhaitable pour nous, au Québec.

M. Dupont (Benoit) : Non, rassurez-vous.

Mme Rizqy : Parfait. Merci. Aussi, j'aimerais revenir sur les superpropagateurs. Est-ce que vous avez réfléchi à ces superpropagateurs, comment, au fond, on pourrait s'assurer d'avoir... de mieux circonscrire, en fait, la démarche qui devrait être suivie par la Santé publique?

M. Dupont (Benoit) : Bon, encore une fois, je suis criminologue, moi, je ne suis pas épidémiologiste, donc je ne peux pas vous faire un exposé sur les superpropagateurs, mais je m'y intéresse parce que ça a un impact sur des applications et sur la surveillance. Ce que j'en comprends, c'est... encore une fois, on revient toujours aux tests, c'est-à-dire que le seul moyen de les découvrir, c'est probablement de les tester. Et, encore une fois, on ne sait même pas quelles sont les caractéristiques qui font que certains individus sont des superpropagateurs alors que d'autres ne le seront pas. Donc, je pense que, là, on est dans un domaine «zone grise» de la recherche, où on a encore... on a des indices de schémas de propagation, mais on a encore très peu d'information sur les déterminants qui vont faire en sorte que je vais être un superpropagateur et vous, vous n'allez pas transmettre la maladie.

Mme Rizqy : Je vais m'éloigner un petit peu de l'application qui est souhaitée par le gouvernement puis regarder davantage ce que l'industrie fait en parallèle. En ce moment, rien n'empêche l'industrie de développer leurs propres applications, de faire du croisement de données, et quand... et je dis «quand» et non pas «si», lorsqu'il y a des fuites de données, à l'heure actuelle, c'est quoi, les conséquences pour ces entreprises au Québec?

M. Dupont (Benoit) : Au Québec et dans le reste du Canada, ce n'est plutôt rien.

Mme Rizqy : Alors, je comprends que... Parce que vous auriez peut-être une recommandation à cet effet pour qu'on ait des lois avec plus de mordant, notamment, peut-être aussi pour les administrateurs des entreprises, un peu à l'instar... comme, par exemple, lorsqu'on a mis, au niveau... une responsabilité criminelle en matière de pollution dans nos lois environnementales ainsi que dans le Code criminel, parce qu'à un moment donné les entreprises, pour eux autres, là, ça coûtait moins cher de polluer que de payer une amende, alors ils prenaient la décision de tout simplement polluer, et, lorsqu'ils ont compris qu'ils pouvaient faire face, à titre d'administrateurs, à des obligations criminelles, tout à coup, le comportement de ces entreprises a changé. Pensez-vous que c'est quelque chose qu'on devrait observer et faire plus tard une recommandation au niveau fédéral?

M. Dupont (Benoit) : Ça peut être une mesure dans l'arsenal. Je pense qu'il y en a d'autres qui sont déjà en discussion, inspirées du GDPR européen, donc des amendes pouvant aller jusqu'à 4 % des revenus annuels. Je pense qu'il y a un projet de loi qui a été déposé ici même, au Québec, qui va être discuté assez rapidement. Ça, c'est une mesure intéressante parce que quelques milliards ou quelques dizaines de millions d'amendes, quoiqu'on en pense, ce n'est pas anodin pour une entreprise et surtout pas pour ses actionnaires. Et donc il y a beaucoup de P.D.G.

d'entreprises, aux États-Unis et en Europe, qui ont été victimes de ces vols de données là, qui se sont vu imposer des amendes considérables et qui ont perdu leur emploi.

Donc, je pense que ça commence avec des amendes, déjà, considérables, la sensibilisation des dirigeants, des hauts dirigeants, des administrateurs aussi. Ça peut être un élément, mais je pense qu'il y a... Les amendes considérables sont aussi assez efficaces, commencent à montrer qu'on est sérieux, maintenant, dans l'encadrement de ces incidents.

Mme Rizqy : Merci. En terminant, vous avez commencé votre propos en disant : Il existe plein de technologies, notamment les drones, reconnaissance faciale. Pensez-vous qu'au Québec nous sommes dus pour avoir une vraie consultation publique sur toutes ces nouvelles technologies qui, de toute évidence, à chaque jour, enfreignent notre droit à la vie privée?

M. Dupont (Benoit) : Je pense qu'on devrait avoir une consultation permanente parce que ces technologies évoluent à un tel rythme qu'une consultation ponctuelle dans le temps aurait de nombreux avantages, mais serait quasiment désuète après six mois. Et donc on devrait avoir une... Et je pense qu'on a déjà une commission de l'éthique dans les sciences et technologies, une commission d'accès à l'information, mais qui peut-être n'ont pas les ressources suffisantes pour pouvoir consulter à grande échelle et pour pouvoir entretenir des équipes de recherche capables de nous tenir informés un peu de ces nouvelles tendances et de leur impact sur la société et sur notre vie quotidienne.

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

M. Nadeau-Dubois : Merci, M. le Président. Merci, M. Dupont, d'être avec nous cet avant-midi. J'ai peu de temps, je vais aller droit au but. À peu près tout le monde qui est venu nous voir depuis deux jours s'entend sur le fait que ces applications ne pourront pas protéger les gens qui sont les plus vulnérables à la COVID-19, c'est-à-dire les gens les plus âgés et les populations plus défavorisées, pour la raison simple que ces gens-là ont statistiquement moins de chances d'avoir un téléphone intelligent, encore moins un téléphone récent, comme l'exige l'application fédérale dont on discute, actuellement. Par contre, il y a un contre-argument qui est venu à quelques reprises, et c'est de dire : Mais on peut quand même aider ces gens-là par la bande, puisque, si dans d'autres groupes de la société, il y a moins de contagion à cause de l'application, par la bande, disons, de manière collatérale, on va finir par mieux protéger ces gens-là. En vous basant sur l'exemple de l'Australie, que vous avez évoqué dans votre témoignage, qu'est-ce que vous pensez de ce contre-argument?

M. Dupont (Benoit) : Je pense que ça reste extrêmement spéculatif. Et, pour revenir à votre question, je ne suis même pas certain que ces applications puissent adéquatement protéger les gens qui ne sont pas vulnérables, donc...

M. Nadeau-Dubois : Pourquoi?

M. Dupont (Benoit) : Bien, parce qu'il y a trop de variances, trop de variables qui ne peuvent pas être intégrées dans les modélisations et qui font en sorte que les modélisations statistiques, c'est une chose, la réalité, c'est autre chose. Et je pense que ces applications vont détecter quelques cas, quelques dizaines de cas, tout en occupant une bande passante de ressources publiques qui est considérable, et je ne suis pas certain que les bénéfices dépassent les inconvénients.

M. Nadeau-Dubois : Autrement dit, non seulement on ne protégera assurément pas les plus vulnérables, mais il est même fort probable qu'on ne protège pas mieux les moins vulnérables.

M. Dupont (Benoit) : C'est ça.

M. Nadeau-Dubois : Donc, on ne protège pas vraiment personne de plus.

M. Dupont (Benoit) : Non, mais on a l'impression de faire quelque chose, on a l'impression d'agir, et je pense qu'on est dans une crise majeure, et donc toute aide et toute contribution potentielle, je pense, est bienvenue. Mais, sur le papier, pour l'instant, dans les pays qui ont de l'avance sur nous, ces contributions restent... j'ai dit «modestes», mais on pourrait dire... on pourrait utiliser des adjectifs même un petit peu plus... un peu moins ambitieux.

M. Nadeau-Dubois : Donc, c'est moins que modeste.

M. Dupont (Benoit) : C'est moins que modeste.

M. Nadeau-Dubois : Merci.

M. Dupont (Benoit) : On pourrait dire «anecdotique», peut-être.

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

M. Ouellet : Merci beaucoup, M. le Président. Moi non plus, je n'ai pas beaucoup de temps. Je voudrais savoir, M. Dupont, est-ce que, selon vous, les Québécois et Québécoises ont suffisamment d'information pour être en mesure, avec un consentement éclairé... être capables de prendre la décision de dire : Oui, une application de traçage est une bonne chose?

M. Dupont (Benoit) : Oui, je pense qu'on a quand même un débat qui se fait, au Québec, comparativement à d'autres provinces canadiennes ou d'autres pays, qui est relativement transparent. Je pense qu'on a une expertise, aussi, au Québec, qui est... qui s'est manifestée depuis hier, et avant aussi, dans la presse et dans des éditoriaux assez détaillés. Donc, je pense que la population québécoise est probablement l'une des mieux informées sur ce type de phénomène, à l'heure actuelle.

Si on prend l'exemple de l'Alberta, où l'application a été déployée très rapidement, très tôt, il y a eu très, très peu de débats publics. D'ailleurs, on en entend très peu parler, de cette application-là, maintenant. Donc, je pense qu'au Québec on a quand même... on mène un exercice salutaire et je pense que la population doit recevoir des informations en quantité suffisante pour prendre une décision éclairée, oui.

M. Ouellet : Plusieurs personnes sont venues nous dire que ce n'était pas fiable, qu'il y avait un risque. Et, si le gouvernement décide d'aller de l'avant après ses sondages et ses consultations qui lui dit que la population du Québec va télécharger l'application, quelle serait, selon vous, la chose à faire, minimalement, pour que, si le gouvernement va de l'avant avec cette application, on protège les droits des citoyens, on protège la sécurité des données, mais surtout on leur donne un vrai sentiment de sécurité?

• (11 h 30) •

M. Dupont (Benoit) : Bien, on en a déjà parlé, et je pense que les autres personnes qui ont présenté devant la commission ont déjà mentionné... je pense que des... une révision externe de l'application pour s'assurer que la sécurité est optimale, un encadrement juridique robuste pour s'assurer que les données ne sont pas exploitées de façon abusive ou seront détruites quand on n'en aura plus besoin, mais... je pense, des campagnes de communication à très grande échelle, c'est-à-dire d'investir autant en recherche sur la manière de communiquer l'utilisation optimale de cette application, et de convaincre, et de persuader la population de l'adopter que des budgets en recherche pour développer l'application elle-même. Je pense que l'un ne va pas sans l'autre. Donc, c'est de concevoir l'application comme un écosystème, un écosystème dans lequel il y a énormément de parties en mouvement, qu'on doit imaginer de façon très complexe plutôt que de penser que la simple mise à disposition d'une application va résoudre tous nos problèmes.

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

M. Ouellette : Merci, M. Dupont. Je pense qu'on se questionne aussi depuis deux jours et... Qu'est-ce qui ferait qu'au Québec... Partout ailleurs, à date, dans le monde... Puis souvent les décisions politiques sont basées sur l'expérience, sur ce qui se fait de bien à certaines places. On a souvent entendu, dans les deux derniers mois : Bon, bien, dans tel pays, ils ont réussi, dans tel autre pays, le déconfinement a mieux réussi qu'ailleurs, etc.

Je vous écoute puis j'écoute les autres experts qu'on a eus depuis hier, et, à date, la technologie... vous avez utilisé «anecdote». Je pense que la technologie n'est pas fiable, ou on n'a pas le... on n'a pas trouvé encore la bonne technologie pour répondre à une certaine problématique. Qu'est-ce qui pourrait faire que... Et, je comprends, vous nous avez dit tantôt : Il faut que le gouvernement donne l'impression qu'il agit. Ça donne l'impression qu'on a solutionné un problème, mais votre expertise nous dit qu'on n'a rien sur le marché pour le solutionner, le problème. Donc, c'est un miroir qu'on va envoyer aux citoyens. Je ne sais pas ce que... s'il y a quelque chose que vous pourriez rajouter là-dessus, mais, mon degré de confiance, après vous avoir écouté, dans la technologie, je pense qu'il vient de baisser encore.

M. Dupont (Benoit) : Juste pour être bien compris, là, je ne mettais pas forcément le gouvernement au pilori. C'est... nous tous voulons faire quelque chose face à l'impuissance qu'on ressent dans un tel contexte de pandémie, là. Les entreprises privées, les OSBL, les chercheurs, on veut tous découvrir le moyen miracle d'essayer de combattre et de contrôler la maladie.

La technologie la plus efficace jusqu'à présent, c'est un système de santé publique qui est robuste, qui est bien financé et qui est capable d'agir localement, de façon très agile, pour pouvoir contraindre et contrôler la maladie. Il y a des pays qui sont arrivés à la contrôler de façon démocratique, sans avoir de technologies très sophistiquées mais en ayant des employés de la Santé publique, une coordination des divers ministères, des politiques de tests qui impliquent aussi le secteur privé de façon extrêmement coordonnée et ambitieuse. Il y a plein de moyens. Ce sont des politiques publiques plus que des technologies, et les technologies, à mon avis, ne peuvent pas toujours se substituer aux politiques publiques. Des fois, c'est une technologie très rudimentaire, qui est l'humain, qui va pouvoir aider à contrôler cette maladie-là. Et, les pays comme la Nouvelle-Zélande, qui sont arrivés à des cas zéro ou deux à trois cas par mois, ce n'est pas une technologie miracle qui les a aidés, c'est tout un tas de mesures, de politiques publiques.

Le Président (M. Bachand) : Merci beaucoup, Pr Dupont, de votre présence ici avec nous.

Je suspends quelques instants. N'allez pas trop loin, parce qu'on pourrait peut-être sauver quelques minutes, là, pour la séance de midi. Alors, je suspends les travaux quelques instants. Merci.

(Suspension de la séance à 11 h 34)

(Reprise à 11 h 36)

Le Président (M. Bachand) : À l'ordre, s'il vous plaît! Merci. La commission reprend ses travaux.

Le député de René-Lévesque ne sera pas présent à cette séance, alors, s'il y aurait consentement de la commission, on pourrait répartir le temps entre le député de Gouin et le député de Chomedey. Consentement? Merci beaucoup.

Alors, il me fait plaisir de recevoir monsieur le Pr Gambs, professeur en informatique de la Chaire de recherche du Canada en analyse respectueuse de la vie privée et éthique des données massives de l'Université du Québec à Montréal. Alors, merci beaucoup. Vous avez 10 minutes de présentation, après ça on aura un échange avec les membres de la commission. La parole est à vous. Merci.

M. Sébastien Gambs

M. Gambs (Sébastien) : Bonjour. Tout d'abord, merci de m'avoir invité. Mon expertise à moi — je suis informaticien — elle est surtout sur les aspects vie privée et sécurité, donc je vais essayer d'aborder surtout ces aspects-là.

Donc, d'abord, pour rappeler le contexte, on appelle ça une application de notification d'exposition, qui fait plutôt rapport à la finalité, ou de traçage de contacts, qui fait rapport aux moyens. On est, je pense, c'est bon de le rappeler, dans un contexte où on va demander à la majorité de la population d'installer une application qui va collecter des données, donc je pense que le niveau de sécurité qu'on devra attendre de cette application-là est le maximum, je dirais quasiment celui qu'on attendrait d'une infrastructure critique, et donc il y a des enjeux importants, en plus de ceux qui ont déjà été discutés, en termes de sécurité et de vie privée.

Une des choses, je pense, qui est importante, qui a déjà été abordée, c'est que, dans le contexte où on va vouloir être capables de mesurer l'efficacité de l'application et de faire la reddition de comptes, ça a déjà été abordé dans quelques interventions, mais je pense que c'est important de se doter, a priori, de critères mesurables qui pourront permettre, au bout de quelques mois, de dire si l'application a atteint ou pas ses objectifs, que ce soit en termes de vie privée ou d'efficacité.

Donc, comme vous l'avez évoqué, j'ai vu que le Québec a déjà dit qu'il n'irait pas avec la géolocalisation, ce qui est vraiment une bonne chose parce que, parmi les technologies possibles, je dirais que c'est à la fois la pire en termes d'efficacité, parce que votre position GPS, elle est très peu précise si vous êtes dans une zone avec des bâtiments, en plus on ne peut pas la prendre si vous êtes à l'intérieur, dans le métro, et en plus c'est très intrusif pour la vie privée.

Donc, comme, pour l'instant, la consultation ne porte pas sur une application particulière, je vais venir sur celle du fédéral, qui a été mise sur la table comme une application potentielle. Donc, du point de vue de la vie privée, elle est un peu mieux parce que, déjà, elle utilise le Bluetooth, donc il y a moins de données collectées. Dans les points, en termes de vie privée, positifs, quand on regarde la conception de l'application, on essaie quand même de minimiser les données, donc on va envoyer des codes aléatoires mais pas d'identifiant direct. On essaie, aujourd'hui, d'avoir une certaine souveraineté de l'utilisateur sur les données, donc les codes restent stockés sur le téléphone, et c'est lui-même, quand quelqu'un a été testé positif, qui peut, par son application, récupérer la liste des codes testés positifs et faire directement, localement, sur son téléphone, le calcul de la notification d'exposition à savoir s'il est à risque ou pas. Donc, ça, c'est plutôt bien pour la vie privée.

• (11 h 40) •

Les choses sur lesquelles, je pense, il faut porter attention, c'est que je pense que le terme «anonyme» est un peu trop fort, dans le sens où même si le risque de réidentification est faible, il existe encore, et d'ailleurs ça a été relevé par le commissariat à la vie privée du Canada dans un avis qu'il a fait sur l'application Alerte COVID. En particulier, le Bluetooth, à la base, est fait pour des communications à courte distance, mais on l'a détourné en essayant de mesurer la proximité. Et donc ce que font la plupart des applications, c'est qu'elles demandent à envoyer des métadonnées, qui sont votre type de téléphone et la force de votre signal, en plus de ce code aléatoire dont je parlais tout à l'heure, et on pourra arriver à des situations où on pourra essayer de tracer quelqu'un ou tracer son téléphone parce que cette information-là, cette métadonnée est stable dans le temps. Donc, ça, ça pourrait être une source de réidentification potentielle.

Une autre chose que j'ai vue en regardant l'application fédérale, c'est que, quand vous avez téléchargé l'application, votre adresse IP est enregistrée, et, quand vous allez... quand vous êtes testé positif et que vous envoyez les codes aléatoires qui permettront aux autres contacts d'être notifiés, eh bien, votre adresse IP est aussi enregistrée. Donc, potentiellement, on pourrait faire un lien entre qui a téléchargé l'application à tel moment et la personne qui a été testée positive.

Une des choses aussi que je voudrais mentionner, c'est que cette appli va demander à ce que le Bluetooth des appareils tourne en permanence. Et rien que la semaine dernière, par exemple, on a eu une faille de sécurité, découverte par des chercheurs chinois, qui permettait de voler leurs listes de contacts et leurs SMS à partir d'une faille Bluetooth. Une faille plus sérieuse, qui a été patchée, qui date de février, c'était une faille qui permettait d'exécuter du code arbitraire, donc de prendre le contrôle du téléphone, en février. Donc, il faut que... je pense, dans le contexte où la population doit être informée avant de consentir, il faut qu'elle soit au courant qu'en activant le Bluetooth il peut aussi y avoir des risques de sécurité.

En termes de vie privée, un des enjeux qui peut être possible, aussi, c'est que... ça a été abordé hier, mais au niveau du traçage cyberphysique qui est parfois utilisé dans les centres commerciaux, où on essaie de suivre les déplacements de votre téléphone à partir des données émises par les signaux wifi ou les signaux Bluetooth, il pourrait y avoir aussi un risque, seulement d'un attaquant qui est motivé, parce qu'il faudrait qu'il soit capable de mettre des capteurs un peu partout dans la ville, de suivre un téléphone à partir des données Bluetooth qui ont été émises, donc ça pourrait être par les métadonnées dont je parlais tout à l'heure.

Une autre chose qui pourrait arriver et qui a été — je pourrais vous envoyer la référence — identifiée comme étant des scénarios d'attaque, quelle que soit la technologie utilisée, donc, ça a été évoqué par la Quadrature du Net hier, ça serait des attaques du type l'attaque d'entretien d'embauche. C'est une attaque très simple où vous avez quelqu'un que vous hésitez à embaucher, vous prenez un téléphone dédié, vous installez l'application, vous le faites rentrer en contact avec cette personne, vous isolez le téléphone ensuite puis vous attendez de voir s'il y a une notification qui est faite ou pas. Si c'est le cas, eh bien, ça veut dire que la personne a été testée positive.

Une autre attaque qui est reliée à la sécurité, c'est une attaque que j'appellerais de déni de service. Donc, supposons que je pense avoir les symptômes et que je vais sûrement aller me faire tester bientôt, ce que je pourrais vouloir faire, c'est essayer de causer du tort. Donc, les raisons pourraient être variées. Supposons que j'ai un restaurant en face de mon restaurant et où je voudrais aller dans la salle, faire interagir mon téléphone avec les employés du restaurant, eh bien, si je suis testé positif, ensuite ils vont devoir se mettre en quarantaine et le restaurant va fermer.

Dans l'exemple que les Français avaient imaginé dans les scénarios, c'était même plus loin, ils disaient que, supposons qu'il y a un contexte de guerre où on veut empêcher un navire d'appareiller, on pourrait aller près de ce navire-là avec quelqu'un qui est positif, faire que tous les marins attrapent ce contact-là dans la liste et puis ensuite bloquer le... Donc là, on est peut-être dans des scénarios un peu extrêmes, mais donc il peut y avoir des risques aussi, et ça, c'est indépendant de la technologie. Donc, que ce soit le GPS, que ce soit la géolocalisation, c'est des scénarios d'attaque qui pourraient arriver.

Donc, je pense qu'une des choses qui est vraiment importante, quelle que soit l'appli qui est choisie, si jamais la consultation amène à une appli, c'est vraiment la transparence. Donc, c'est revenu dans les débats, donc, la transparence, ça passe par plusieurs éléments. Ça passe par l'ouverture du code source, mais ce n'est pas suffisant. Ça passe par une documentation pour le grand public, qui est claire, ce qui est le cas... Donc, le fédéral le fait, actuellement, mais ce qui manque, par exemple, c'est des documents de spécifications techniques qui sont à un niveau... Donc, un code source, c'est bien, mais c'est des milliers de lignes de code. Donc, même pour un informaticien, c'est plus intéressant, parfois, d'avoir un document clair, qui explique comment fonctionne l'application. Donc, ça, je pense que c'est une clé qui est nécessaire.

S'il y a des audits de sécurité, ce qui me semble, aussi, nécessaire, il faudrait que les audits soient publics, à mon sens, pour que d'autres experts puissent éventuellement prendre connaissance des failles et rajouter leur expertise. Et donc, à mon sens, il faudrait qu'il y ait vraiment une volonté... Donc, on parlait de «security»... de «hackathon» de sécurité, tout à l'heure, c'est aussi une très bonne alternative.

Et je pense qu'une des choses qu'on ne réalise pas, aussi, c'est que l'écosystème de l'application est relativement complexe. Donc, si je prends l'exemple de l'appli fédérale, Shopify a refusé de venir ici. Mais, au-delà de Shopify, je pense qu'il aurait fallu avoir les services numériques canadiens qui ont participé au développement, BlackBerry, qui, de manière pro bono, a aidé à la sécurité de l'application et aussi appelé Google au niveau de l'API qu'ils ont mis en place. Parce qu'il y a des soupçons, dans les articles scientifiques qui sont sortis les dernières semaines, sur le fait que, même si l'API d'Apple et Google se base sur un protocole qui, à la base, est plus respectueux de la vie privée, il y a quand même des métadonnées qui sont collectées dans certains pays. Et, en plus de ça, si j'allais même plus loin, bien, on parlait, tout à l'heure, des serveurs d'infonuagique, le fédéral fait affaire avec Amazon Web Services pour stocker les données qui vont être collectées. Donc, même eux, je viendrais leur demander d'expliquer comment fonctionne le stockage des données dans le cadre de l'application. Donc, si une appli est choisie, je pense qu'il faudrait que tous ces acteurs-là soient aussi auditionnés. Je ne sais pas si ce serait dans le cas d'une commission comme ici ou dans le cadre d'autres approches.

Et une dernière chose sur laquelle je voudrais insister, c'est le glissement de finalité. Donc, à mon sens, c'est un risque important. Donc, cette application-là, si la population québécoise y adhère, donc si cette application est lancée, je pense que le risque qu'on commence à voir des employeurs qui commencent à demander de voir le score de risques ou certains centres commerciaux qui disent : Bien, vous ne pourrez rentrer que si vous avez un score de risque faible, c'est un risque qui est important. Donc, à mon sens — ça a été repris, je pense, ce matin par la Commission d'accès à l'information et d'autres individus, donc d'autres personnes qui ont été entendues — ça serait de mettre dans la loi directement une interdiction non seulement d'utiliser l'application pour d'autres finalités, mais même de mettre des amendes qui décourageraient à le faire. Donc, on parlait ce matin, si vous êtes dans un groupe vulnérable, que votre employeur vous demande de voir le score de risque, quelle est la probabilité que vous allez

vraiment refuser de répondre à son injonction si le fait de pouvoir payer votre loyer à la fin du mois dépend de votre travail, alors que, si la loi fait qu'il pourrait y avoir des conséquences financières importantes, je pense que ça découragerait les glissements de finalité. Donc, voilà, c'était mon intervention.

Le Président (M. Bachand) : Merci beaucoup. Je me tourne vers le gouvernement. Mme la députée de Jean-Talon, s'il vous plaît.

Mme Boutin : Merci beaucoup de votre présence, c'est vraiment extrêmement intéressant et très pertinent également.

Moi, si je vous entends, là, soudainement, j'ai quasiment envie que, finalement, on remette nos téléphones cellulaires puis qu'on arrête, parce qu'on est, actuellement, tout le monde ici, je pense, et la population en général à l'international est à risque. Nous sommes à risque si on utilise... on écoute de la musique dans une voiture, on a... Moi, j'active le Bluetooth parce que je mets de la musique un peu partout, j'ai mon wifi, j'utilise Google Maps parce que je n'ai aucun sens de l'orientation, alors j'imagine que moi, personnellement, comme plusieurs personnes, on est déjà à risque en continu dans la société.

M. Gambs (Sébastien) : Il y a beaucoup de personnes qui refusent d'activer le Bluetooth, donc ce n'est pas non plus si rare que ça que les gens n'activent pas le Bluetooth. Et, quand vous avez votre appli qui communique avec votre voiture, par exemple, elle le fait de manière ponctuelle, donc, effectivement, un attaquant qui viendrait à ce moment-là pourrait éventuellement profiter de la vulnérabilité, mais là, avec l'application, le Bluetooth va être activé en permanence.

Donc, souvent, on parle de surface d'attaque. La surface d'attaque, elle va être toute la journée pour ceux qui activent le Bluetooth, elle ne va pas être...

Mme Boutin : Donc, dès qu'on active tout le temps le Bluetooth, nous sommes toujours à risque, qu'on ait l'application ou non. C'est vraiment une question, là, que je me pose, là, très sérieusement, là. Si je le laisse activé, mon Bluetooth, puis je vais au centre d'achats, je suis toujours à risque, dans le fond?

M. Gambs (Sébastien) : Vous serez à risque aussi, effectivement. Mais il y a quand même pas mal de monde qui refusent d'activer leur Bluetooth justement à cause de ces risques-là et qui ne le font qu'au cas par cas. Donc, je connais des gens... peut-être que ce serait intéressant de faire un sondage ou de trouver des données probantes, mais il y a des gens qui refusent d'activer le Bluetooth tout simplement à cause de ces enjeux-là de sécurité.

Mme Boutin : Je pose cette question-là parce que... c'est sûr, c'est un petit peu en dehors du cadre de l'application elle-même, mais c'est une question qu'on devrait se poser au niveau de la société, également, là. Toutes les applications... puis, tu sais, la littératie numérique des gens, on manque peut-être, aussi, d'information. Puis moi, j'aime la technologie, mais, quand même, on se pose ces questions-là puis on se dit toujours qu'il y a un risque à prendre. Dès qu'on met... on utilise une technologie, il y a un risque. C'est de balancer l'efficacité, l'utilité versus le risque d'atteinte à la vie privée dans toutes nos décisions.

M. Gambs (Sébastien) : Mais souvent la plupart des applis actuelles qui utilisent le Bluetooth le font de manière ponctuelle. Donc, vous allez démarrer votre appli, le Bluetooth s'active à ce moment-là. Là, il faut quand même se rendre compte que l'application de traçage de contacts va avoir le Bluetooth activé en permanence, donc le temps où vous êtes vulnérable va être plus important.

Mme Boutin : Puis est-ce que vous savez s'il y a beaucoup d'attaques de ce genre, en général, ou... C'est peut-être une question... Moi, je n'ai pas la réponse, là.

M. Gambs (Sébastien) : Il y en a eu beaucoup, ces dernières années, sur Bluetooth. Donc, il y a vraiment des vulnérabilités critiques d'exécution de codes parce que Bluetooth, c'est un protocole qui est encore relativement récent et qui a commencé à être beaucoup utilisé ces dernières années. Donc, il y a des objets connectés, par exemple, et là, en fait, ça a amené les chercheurs à regarder cette technologie, et il y a eu beaucoup de failles trouvées. Donc, c'est assez significatif, ces dernières années.

Mme Boutin : Tu sais, quand on utilise, dans le fond, des applications de notre plein gré, que ça soit, tu sais, des applications qui sont par le privé, bien, c'est un peu notre responsabilité à nous. Mais moi, je comprends que le gouvernement... et je prône pour que le gouvernement, lorsqu'elle met en circulation des applications, soit responsable, qu'il y ait un encadrement qui soit légal, une imputabilité, un encadrement technologique, une infrastructure technologique autant pour protéger les données, tu sais, être conscient de ça, là, encrypter, avoir le moins de collectes de données personnelles possible et tout et au niveau de l'appareil.

Vous, quelles seraient vos recommandations qu'on pourrait... les choses qui pourraient être mises de l'avant pour cette application-là, l'application, tu sais, Bluetooth, qui pourraient être considérées, même pour toute autre application? Qu'est-ce qui peut être... des mesures qui pourraient être mises en amont par une entité gouvernementale au niveau technologique et au niveau de la gouvernance, au niveau de la sécurité? Est-ce qu'il y a des groupes d'experts, le groupe de cyberdéfense pourrait faire des tests?

M. Gambs (Sébastien) : Oui, donc, c'est déjà revenu un peu dans ce que j'ai dit, mais il faudrait déjà qu'il y ait des audits par des groupes de cyberdéfense. La suggestion de Benoit, qui me précédait, de faire appel aussi à de l'industrie de cybersécurité serait important. Le fait de faire appel à des volontaires dans un... de sécurité, me semble important. Donc, le fait, avant de lancer l'application, de laisser la chance aux experts et aux entités qui ont l'expertise de faire une évaluation de la sécurité me semblerait vraiment important.

Mme Boutin : Et est-ce que vous seriez pour — je pense que c'est vous qui avez parlé de ça, oui — peut-être un projet pilote ou un test, mettre en place une... bien, je n'aime pas le mot «infrastructure», mais un processus d'évaluation au départ et en continu? Et comment on pourrait le faire, sur quels critères? Évaluation au niveau de la sécurité, de l'efficacité, est-ce que c'est quelque chose qui serait pertinent?

• (11 h 50) •

M. Gambs (Sébastien) : Donc, il y a... le projet pilote, je pense que ça serait important pour l'efficacité. Donc, au-delà de la sécurité, on a beaucoup discuté de l'efficacité, et je pense que ça serait intéressant, d'avoir un... Alors, peut-être que, si jamais l'appli fédérale est choisie, on peut peut-être considérer que l'Ontario est un projet pilote en soi, mais, si une autre appli est développée, ça pourrait être de choisir une zone, une ville, une région du Québec pour déployer l'application et mesurer si elle est vraiment efficace et, si on constate que l'efficacité n'est pas au rendez-vous, bien, de ne pas déployer l'application.

Au niveau de la gouvernance, c'est revenu aussi, mais je pense que d'avoir un comité de personnes de différentes expertises, qui ont vraiment un pouvoir, je pense, dans leurs recommandations, qui est suivi par le gouvernement... donc pas juste un avis consultatif. Je ne sais pas quelle serait la meilleure structure pour mettre ça en place, mais, si jamais le comité lève l'alarme et dit : Il y a quelque chose qui ne va pas, on n'atteint pas les objectifs, qu'on puisse débrancher. Alors, ça me semble aussi quelque chose de vraiment important.

Mme Boutin : Je vous remercie. Je pense que mes collègues ont quelques questions, mais je vais juste dire, c'était important pour nous de consulter, puis on est les seuls qui le font, en fait, puis on a l'avantage d'être... je ne voudrais pas dire «en retard», mais d'être un peu plus frileux, donc de prendre plus le temps. Merci.

Le Président (M. Bachand) : M. le député de Chapleau.

M. Lévesque (Chapleau) : Oui, merci, M. le Président. Merci beaucoup de votre présentation. Donc, vous avez parlé de, bon, la question de Bluetooth, des données IP, de certains scénarios catastrophes, également, puis de l'application fédérale. Donc, peut-être pour reprendre un peu la question de ma collègue de Jean-Talon, qui disait : Qu'est-ce qu'on peut faire, disons, pour les applications à venir?, mais qu'est-ce que... disons, si on prend l'exemple de l'application fédérale, qu'est-ce qu'on pourrait faire pour l'améliorer, disons qu'on décidait d'aller avec celle-là ou avec celle de l'Ontario? Donc, qu'est-ce que... avez-vous des éléments, des pistes de solutions pour éviter, justement, les scénarios catastrophes dont vous faites mention, la perte d'un navire militaire ou autre?

M. Gambs (Sébastien) : Bien, le problème, c'est qu'il y a certaines des attaques que j'ai mentionnées qui sont indépendantes de la technologie, donc il y a certaines attaques qu'on ne pourra pas éviter, quelle que soit la façon dont on fait le système.

Une des choses, je pense, où on peut prêter attention, c'est... donc, si jamais l'application fédérale est choisie par le Québec, il y a aussi une gestion des mots de passe à usage unique qui sont gérés par le système de santé québécois, et donc il faut faire attention, aussi, à comment ça, ça va être mis en place. De ce que j'ai vu en Ontario, ils ont demandé d'avoir une information supplémentaire qui est ajoutée, qui pourrait éventuellement leur permettre de déterminer si une personne qui a été testée positive a choisi... a consenti à envoyer ses contacts ou pas. Donc, je rappelle que le consentement de la personne est un pilier fondamental de la vie privée, et donc même une personne qui est testée positive a le choix de ne pas remonter ou pas ses contacts. Et donc une infrastructure déployée où il y aurait une possibilité éventuelle de savoir si une personne a choisi de remonter ou pas ses contacts, pour moi, me semblerait problématique parce qu'on pourrait être tentés de dire : O.K., est-ce que cette personne-là qui a été testée positive, c'est vraiment un bon citoyen, elle a vraiment «uploadé» ses contacts ou est-ce que qu'elle a choisi de ne pas les «uploader» pour une raison qui peut lui être spécifique?

Donc, je pense que la façon dont le provincial générerait les codes à usage unique, comment ça s'arrimera avec le fédéral, serait un sujet... Encore une fois, comme certains experts ont dit, je pense qu'une fois qu'une appli est choisie il faudrait faire revenir les experts en sécurité en vie privée par rapport à cette appli-là, parce que, là, on est beaucoup dans le spéculatif, on ne sait pas si une appli va être choisie, quelle appli va être choisie.

M. Lévesque (Chapleau) : Non, c'est clair. Vous avez parlé de, justement, la protection de la vie privée puis protection des renseignements personnels, peut-être qu'en tant qu'informaticien avez-vous peut-être analysé, là, puis soyez bien à l'aise, le cadre juridique, là, notamment la Loi concernant le cadre juridique des technologies de l'information, sur certains points de protection. Est-ce qu'il y a des éléments, si jamais vous avez eu l'occasion de le voir, qui pourraient être ajoutés dans ce cadre juridique là? Ou même vous avez eu l'occasion de voir le projet de loi n° 64 puis peut-être vous avez même des recommandations générales de par...

M. Gambs (Sébastien) : Oui, je peux rajouter. Alors, il faut que je dise à l'avance que je suis Français d'origine et je suis revenu au Québec il n'y a que quatre ans, donc je ne connais pas aussi bien la loi que... j'ai vu

qu'il y a Pierre-Luc Déziel et Céline Castets-Renard qui pourront intervenir là-dessus, mais une des choses que je vois, effectivement, et c'est revenu dans les discussions, c'est qu'il n'y a pas de mordant en termes d'amende. Donc, le fait de pouvoir donner des pouvoirs de sanction plus importants, ça pourrait aider aussi.

M. Lévesque (Chapleau) : Dans le projet de loi n° 64, il y a...

M. Gambs (Sébastien) : Il y a aussi... le fait de donner plus de ressources à l'autorité de protection des données, donc à la CAI, pour être capable, aussi, d'exercer ses missions me semble aussi fondamental.

M. Lévesque (Chapleau) : C'est un peu ce qu'elle nous disait. Dans le projet de loi n° 64, d'ailleurs, il y aura des sanctions, là, pécuniaires, financières en lien avec ça. Donc, ça, c'est un bon point, effectivement.

Vous avez parlé, notamment, aussi de la question des tiers, de l'employeur qui pourrait demander ou exiger, là, bon, d'avoir l'application, d'avoir les résultats à l'employé. Donc, vous avez parlé de deux mesures législatives. Par décret, ce serait possible de le faire. Est-ce que ce serait une voie qui serait envisagée, à ce moment-là, si ça, effectivement, donne la protection? Et est-ce qu'on ajouterait, à ce moment-là, disons, des mesures pécuniaires, financières, quelques peines à ce niveau-là?

M. Gambs (Sébastien) : Je pense que c'est important d'ajouter les mesures pécuniaires, sinon j'ai peur qu'un employeur, finalement... s'il n'y a pas de mesure contre lui, il ne se sentira pas obligé de respecter. Donc, effectivement, je pense que la loi ou le décret devrait inclure ça comme un dispositif pour éviter tout glissement de finalité. Et le glissement de finalité, il pourra arriver dans six mois. Donc, supposons qu'une appli soit choisie, qu'elle soit déployée, que la population y adhère, mais qu'il y a une cinquième, 10^e vague, à ce moment-là, les employeurs pourraient se dire : O.K., bien là, tout le monde a l'appli, on va demander d'avoir accès au score de risque pour...

M. Lévesque (Chapleau) : O.K. Excellent. Merci, M. le Président.

Le Président (M. Bachand) : Merci. Autres questions du côté ministériel... gouvernemental, pardon? Mme la députée des Plaines, oui.

Mme Lecours (Les Plaines) : Merci beaucoup, M. le Président. Merci de votre vision, vos éclairages. Vous êtes, évidemment, un spécialiste en cybersécurité. Par contre, je vais vous amener sur un autre terrain qui est un peu plus le côté comportemental. Bon, dans un premier temps, vous dites : On ne sera pas à l'abri d'attaques, advenant l'adoption d'une application comme celle qui existe actuellement, là, mais qu'on n'a pas de choix de fait. Par ailleurs, on n'est déjà pas à l'abri d'attaques, si je comprends bien.

M. Gambs (Sébastien) : Bien, si, le Bluetooth, vous l'avez désactivé sur votre téléphone, par exemple, une grosse partie des attaques que j'ai mentionnées...

Mme Lecours (Les Plaines) : Je vais le désactiver, là.

M. Gambs (Sébastien) : ...ou si vous utilisez une application qui active le Bluetooth quand vous allumez l'application, vous êtes à l'abri des attaques que j'ai mentionnées sur le Bluetooth.

Mme Lecours (Les Plaines) : Mais pourquoi je vous dis «du côté humain», est-ce que... si on essaie de faire le contrepois entre les impacts possibles mais les bienfaits également, une application comme celle qui est présentée, qui est sur la table, est-ce qu'effectivement ce pourrait être important et complémentaire à tout point de vue humain, actuellement? Tout le traçage humain qui se fait, selon vous, est-ce que c'est quelque chose qui est acceptable?

M. Gambs (Sébastien) : Bien, est-ce que ça peut être... Je pense que tout le monde est d'accord que ça serait un outil complémentaire, mais pas la panacée. Est-ce que... Donc, si vous me demandez de faire l'exercice d'équilibrer les bénéfices en termes de santé et les risques de sécurité, je pense qu'il faudrait que j'aie une spécification d'appli beaucoup plus détaillée et qu'on soit plusieurs experts de sécurité à se mettre autour de la table pour être capables de faire l'exercice. Donc là, de manière abstraite, c'est sûr que cet exercice devrait être fait, mais on a les questions sur l'efficacité, donc cet exercice ne va pas être facile à faire parce que certaines choses vont être difficiles à mesurer. Quelle serait vraiment l'efficacité de l'appli si elle est déployée à large échelle? C'est revenu dans plusieurs interventions. Donc, il faudrait faire cet exercice, mais sans spécification d'appli...

Mme Lecours (Les Plaines) : Mais je comprends que vous êtes d'accord avec moi sur le fait que faire... actuellement, on ne fait appel qu'à la mémoire des gens, là.

M. Gambs (Sébastien) : Donc, je pense qu'effectivement le bénéfice principal de cette appli, ça serait de pouvoir tracer des contacts dans un contexte, par exemple, de déconfinement massif, où on commence à avoir beaucoup d'interactions, des contacts de gens, par exemple, qu'on croise dans le métro, qu'on ne se souviendrait pas.

Donc, ça, c'est, je pense, vraiment le plus par rapport au traçage manuel traditionnel. Le moins, c'est quand même qu'on déploie à large échelle et donc que les enjeux de vie privée, ce n'est pas une personne, mais c'est multiplié par toute la population.

Le Président (M. Bachand) : ...M. le député de Beauce-Nord, s'il vous plaît.

M. Provençal : Merci, M. le Président. Par rapport à tout ce que vous avez dit, là, selon vous, là, à quel endroit va se situer le point d'équilibre entre la protection de la santé publique puis le respect de la vie privée? Ça se situe où, là? Tu sais, on travaille beaucoup, dans notre vie, avec des graphiques, là, avec des points d'équilibre, mais, pour vous, là, par rapport à ce que vous nous avez tout exposé, ça se situe où?

M. Gambs (Sébastien) : Donc, encore une fois, sans... Ça se situe où par rapport à quels critères ou quelles mesures? Sans avoir une application spécifique, c'est difficile pour moi de répondre.

Donc, si, par exemple, il y avait eu... supposons qu'il y a 20 pays dans le monde où on sait que ce genre d'appli permet de sauver des millions de vie, là je serais dans une situation où on aurait déjà des preuves de l'efficacité, où effectivement je pourrais essayer de mesurer, dire : O.K., il y a des enjeux de vie privée, mais on a des données probantes démontrables qui montraient que cette application-là avait eu un impact important.

Dans les conditions actuelles, moi, étant chercheur en vie privée et en sécurité, je peux vous amener les problèmes potentiels que je vois. Je ne suis pas un épidémiologiste, un peu comme Benoit le disait, donc l'impact positif sur la santé publique, je n'ai pas vu d'étude de pays où ça a vraiment fonctionné pour l'instant, donc je ne me sens pas forcément à l'aise de répondre à cette question-là.

M. Provençal : Merci.

Le Président (M. Bachand) : Merci. Autres questions? Il reste une minute. Non? Ça va?

M. Provençal : Oui, merci beaucoup, M. le Président.

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

• (12 heures) •

Mme Rizqy : ...consentement, on pourrait peut-être prendre la minute pour l'attribuer aux deux autres groupes, aux députés indépendants.

Le Président (M. Bachand) : Ça a été fait, ça a été fait.

Mme Rizqy : Ah! parfait. Merci d'être présent avec nous. J'ai l'impression, quand j'écoute les questions qui vous sont posées, qu'on essaie de banaliser le fait de la violation de la vie privée en disant : Bien, de toute façon, on est déjà tous à risque, alors que l'application qui est déjà offerte par le gouvernement fédéral, vous l'avez clairement mentionné, que, là, à ce moment-là, je vais citer, là, notre surface d'attaque, elle est permanente, et donc 24 heures par jour, sept jours sur sept, tant et aussi longtemps qu'on a l'application sur notre téléphone. Est-ce exact?

M. Gambs (Sébastien) : Oui.

Mme Rizqy : Donc, lorsque certains collègues mentionnent : Ah! mais, de toute façon, j'ai déjà des applications sur mon cellulaire, il faut faire attention, parce que ces applications, lorsque le Bluetooth est activé, c'est lorsqu'on est sur l'application. À moins qu'on n'est pas sur l'application, à ce moment-là, notre surface d'attaque n'est pas, à ce moment-là...

M. Gambs (Sébastien) : Oui, la plupart des applications qui utilisent le Bluetooth fonctionnent comme ça. Il faut aussi être conscients qu'il y a des gens, justement, pour des enjeux de sécurité et de vie privée, qui refusent d'activer le Bluetooth, donc, toute appli qui va leur demander d'activer le Bluetooth, ils vont le refuser. Alors, quel pourcentage c'est de la population? Je pense, ça serait intéressant, si un intervenant sociologue pourrait compléter ça, d'avoir une idée de combien de personnes activent ou pas le Bluetooth, je n'ai pas ces chiffres-là. Mais ces personnes-là, en fait, essaient de limiter leurs risques en évitant d'activer le Bluetooth. S'ils installent l'application, ils vont avoir le Bluetooth qui est activé, donc ils peuvent le faire en connaissance de cause en fonction des bénéfices qu'ils voient ou pas et de l'information qu'ils auront sur les risques de vie privée et de sécurité, mais d'un coup leur surface d'attaque est passée de quasiment rien à, effectivement, une surface importante.

Mme Rizqy : Il y a quand même, ici, une certaine forme de méprise quant à notre compréhension collective de quand est-ce qu'on est sous attaque et quand est-ce qu'on ne l'est pas avec la technologie Bluetooth, et ça amène... et vous mettez le point, je trouve... justement, avoir plus de données à cet effet, qui qui l'utilise, qui qui ne met pas le Bluetooth. Mais tous les groupes qu'on a entendus jusqu'à présent nous parlent du consentement libre et éclairé. Quel est notre degré de compréhension de la littératie numérique au Québec?

M. Gambs (Sébastien) : Pareil, je pense, ce serait une question pour une sociologue ou un sociologue du numérique, mais je pense que la littératie numérique est effectivement un... Je ne sais pas, je pense que je ne suis pas assez bien... je ne suis revenu qu'il y a quatre ans au Québec, donc je ne pourrais pas dire, mais je pense que les débats publics comme on a contribué à améliorer la littératie numérique et je pense qu'au fur et à mesure que les gens vont améliorer cette littératie, il y en a qui choisissent ou pas de désactiver le Bluetooth en fonction des risques et des failles de sécurité.

Je pense que Desjardins a aussi contribué à éveiller les consciences. Donc, malheureusement, pour améliorer la sensibilité de la population, parfois il faut des scandales de vie privée. Donc, j'espère qu'on ne sera pas avec une application de traçage de contacts, dans un cas où on va déployer cette application-là, et il va y avoir des failles de sécurité importantes. Mais, le niveau de littératie, je pense qu'il va quand même s'améliorer au fur et à mesure qu'on a des débats et qu'on informe le public.

Mme Rizqy : Oui, encore faut-il que les débats soient tenus en temps opportun. Et vous citez l'exemple de Desjardins, et c'est bien que vous faites le parallèle, parce que, autant cette consultation publique que celle que nous avons faite pour Desjardins, il a fallu que les groupes d'opposition, on talonne le gouvernement pour les avoir, parce qu'à chaque fois elles nous ont été refusées, et ce n'est pas faute d'avoir déposé des motions, notamment par mon collègue, des pétitions de la population, puis on est quand même en plein milieu de l'été pour ce type de consultation. Mais là je m'égare un peu, alors je vais revenir.

Faillles de sécurité, failles de prendre le contrôle, et puis vous avez mentionné Apple et Google qui collectent des métadonnées. Alors, pour le commun des mortels, c'est quoi, la conséquence parce qu'Apple et Google peuvent collecter des métadonnées?

M. Gambs (Sébastien) : Ils pourraient, par exemple, savoir votre localisation ou savoir l'usage que vous avez fait de l'application.

Mme Rizqy : Et j'imagine que, là, c'est qu'eux... elles ont un objectif, ces entreprises, qui est d'abord et avant tout faire du profit pour leurs actionnaires. Est-ce que ces données collectées pourraient servir à du croisement de données afin de nous vendre d'autres produits ou mieux comprendre nos comportements?

M. Gambs (Sébastien) : Donc, c'est sûr que c'est des données qui pourraient s'ajouter au profilage. Après, je pense qu'il faut différencier Apple et... Google est vraiment sur la publicité ciblée. Donc, Google, la plus grande partie de son chiffre d'affaires dépend de la publicité ciblée, Apple est plutôt sur la vente de matériel. Donc, les deux peuvent avoir des objectifs un peu différents.

Les travaux que je mentionne sont très préliminaires, mais ils essaient de... En fait, je pourrais vous envoyer l'article, mais, l'article, ce qu'il mentionne, c'est qu'ils ont regardé plusieurs applications déployées dans plusieurs pays européens et dans le monde et ils se sont rendu compte que les enjeux de sécurité et de vie privée ne venaient pas forcément de l'application développée par l'État, mais potentiellement de données qui fuyaient de l'interface Google, Apple, qui n'étaient pas forcément bien documentées dans la documentation qu'Apple et Google ont. Donc, en fait, ils ont écouté les téléphones puis ils ont vu qu'il y avait des données qui sortaient du téléphone.

Donc, je pense que ça serait important aussi, au-delà d'avoir le développeur de l'API, d'avoir aussi des représentants, si jamais une appli choisit d'appeler Google, parce que c'est leur API sur lequel se repose l'application. Donc, c'est une partie de l'écosystème, puis je pense que c'est vraiment important pour avoir une vision large de tous les enjeux de sécurité et vie privée, et je pense que ça serait intéressant de les avoir aussi à la table des auditions.

Mme Rizqy : Merci beaucoup. Je vais céder la parole à ma collègue.

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

Mme Nichols : Merci, M. le Président. C'est définitivement, là, plusieurs points de droit, là, qui rentrent en ligne de compte, autant le droit de la commercialisation, on va avoir le droit de la propriété intellectuelle, le droit de la protection de la vie privée, puis, je pense que vous en avez fait mention, il y a sûrement des personnes compétentes qu'il faudra consulter, parce que la plupart ont des intérêts fort, fort différents, puis parfois même vient la notion du conflit d'intérêts. Il y aura des personnes, certainement, autour de la table ou autour... qui auront des enjeux bien précis. Pour certaines... mais je vais utiliser le terme «bébelle», parce que ça a été utilisé par quelqu'un qui est venu nous faire une présentation, mais certains ont des enjeux pécuniaires importants dans tout ça puis c'est souvent eux qui sont les plus forts, d'où notre grande inquiétude dans tout ça.

Plus je vous écoute, plus je comprends que, peut-être, les personnes les mieux protégées sont celles qui n'ont pas accès à la technologie. Je ne sais pas si vous aviez une réaction...

M. Gambs (Sébastien) : En fait, même si vous avez un téléphone intelligent, je pense qu'on peut choisir d'aller dans les réglages et de désactiver ou activer une certaine fonctionnalité. Donc, effectivement, si on n'a pas... Même si je travaille en vie privée, je suis loin d'être un pessimiste et de dire : Il faut aller dans une grotte et ne plus utiliser la technologie. Je pense qu'il faut profiter des... on parlait de littératie, peut-être augmenter la littératie pour que chacun soit conscient des risques et qu'il puisse aller régler. Donc, on peut avoir un téléphone intelligent mais

refuser certaines fonctionnalités. Donc, par exemple, la géolocalisation, on est d'accord que ce n'est pas une bonne idée de la collecter, et je pense que beaucoup de personnes, maintenant, si on installe une app qui leur demande la géolocalisation, si, par exemple, c'est une app de jeu, vont dire : Pourquoi est-ce que cette app me demande la géolocalisation? Est-ce que j'en ai vraiment besoin?

Donc, il y a possibilité, même si on a la technologie, d'aller voir comment on peut se protéger un peu mieux. C'est sûr qu'on peut être tracé de tellement de manières dans notre société actuelle que se protéger de tout, ça devient quasiment impossible. On peut être tracé par des caméras qui font la reconnaissance faciale, on peut être tracé par des poubelles intelligentes qui vont récupérer les signaux wifi de notre téléphone. Ça, c'était le cas au Royaume-Uni. Donc, effectivement, on peut... mais on peut limiter, je pense, nos risques en essayant d'avoir un meilleur contrôle sur les objets et les réglages des objets qu'on a.

Mme Nichols : Il y a définitivement beaucoup de pédagogie à faire, là, autour de tout ça, puis je pense que c'est important, aussi, que nos citoyens, avant d'utiliser une application... mais on ne sait pas laquelle, moi, je n'ai pas vu d'application sur la table, mais avant d'utiliser n'importe quelle application qui sera en lien avec la pandémie, ou en lien avec la COVID, ou pour des mesures préventives, je pense qu'il y aura de la pédagogie à faire, justement, sur tout ce qui entoure l'utilisation de ce logiciel-là. Parce que souvent, le politique, on va dire : Bien, cette application-là va venir sauver des vies. Bon, est-ce que cette application-là va sauver des vies? Moi, j'aimerais bien vous entendre sur cet aspect.

M. Gambs (Sébastien) : Ça, sans avoir de données probantes, c'est difficile, mais c'est le même... Moi, des fois, je fais des conférences sur l'anonymisation de données et j'ai déjà eu, effectivement... dans des contextes où je parlais devant des médecins, je parlais d'anonymisation de données médicales, et les gens nous disaient : Bien, c'est bien beau de vouloir anonymiser, mais il y a des études qu'on ne pourra pas faire, et il y a des gens qui vont mourir parce qu'on n'aura pas accès aux vraies données. Mais qu'est-ce qui se passe si ces données fuient, par exemple, et que votre assurance médicaments s'amuse à changer votre prime à partir de ces données ou qu'est-ce qui se passe si ces données fuient et que, dans ces données, il y a des données qui permettent d'usurper votre identité?

Donc, il y a... je pense qu'il y a un compromis à trouver entre les deux, mais, l'argument, je pense qu'il a été soulevé une fois ou deux hier, sur il y a des gens qui vont mourir si on n'utilise pas l'appli. Il faut faire attention. Il faut faire attention aussi, parce qu'on parlait hier... je pense, c'était Yves Gingras qui parlait du coût de cette appli. Il y a aussi là... Donc, il y a la question de l'efficacité, il y a la question du coût, et, si jamais cet argent-là, il pouvait être investi dans d'autres mesures qui permettraient peut-être de sauver autant de vies, il faut aussi prendre ça en compte dans la balance.

Donc, je pense que l'argument... c'est difficile, en plus, pour moi, en vie privée, quand on me dit l'argument : Des gens vont mourir parce que vous avez anonymisé les données ou des gens vont mourir parce que la technologie n'est pas utilisée. Je le comprends mais je pense que c'est à prendre en balance avec les coûts de la solution, l'argent qui aurait pu être utilisé dans d'autres contextes, les autres risques en termes d'usurpation d'identité ou d'impact sur les personnes.

• (12 h 10) •

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

M. Nadeau-Dubois : Merci, M. le Président. Merci, monsieur, d'être avec nous cet avant-midi. Combien de temps j'ai, M. le Président?

Le Président (M. Bachand) : 3 min 50 s... 3 min 40 s, maintenant, excusez.

M. Nadeau-Dubois : Quel luxe! Un argument qu'on entend parfois de manière générale — je ne l'attribue à personne en particulier — c'est l'argument suivant : On a déjà tous Facebook, on a déjà tous un téléphone intelligent, on est déjà tous à risque, alors c'est-tu... on s'expose-tu vraiment plus avec une application de traçage et est-ce que le jeu n'en vaut pas la chandelle, puisqu'il y a des vies, nous dit-on, qui pourraient être sauvées? Qu'est-ce que vous pensez, comme expert en cybersécurité, de ce type de raisonnement qui dit : Puisqu'on est déjà à risque, on peut bien prendre encore plus de risques?

M. Gambs (Sébastien) : Moi, j'avoue que ce n'est pas un superargument parce que, en fait, on a une chercheuse américaine qui a une notion qui s'appelle l'intégrité contextuelle où, en fait, en fonction du contexte, on a des attentes différentes. Donc, peut-être que vous avez une page Facebook et vous êtes prêt à partager beaucoup de données avec vos amis, mais ça, ça veut dire que, dans un contexte particulier, vous êtes prêt à donner plein de données, mais ça n'empêche pas que, par exemple, je m'attends à ce que mon médecin, lui, ne partage pas mon dossier médical avec des compagnies pharmaceutiques. Je m'attends aussi... si vous avez des discussions entre collègues dans un cadre particulier, dans un café, et que vous discutez à bâtons rompus, vous vous attendez aussi à ce que ce que vous dites dans ce contexte-là ne sorte pas de la sphère privée. Donc, on peut être exposé à beaucoup de données dans un contexte de réseau social, mais s'attendre à ce que, par exemple, l'État ou une compagnie aient des engagements très forts en termes de vie privée par rapport à nos données.

M. Nadeau-Dubois : Autrement dit, c'est un raisonnement qu'on peut qualifier de très faible.

M. Gambs (Sébastien) : Je pense que ça ne tient pas compte de toutes les attentes des personnes en fonction du contexte.

M. Nadeau-Dubois : Parfait. Toutes choses étant égales par ailleurs, si j'ai le même téléphone avec les mêmes applications et les mêmes fonctionnalités, qu'il n'y a pas d'application... une application comme Alerte COVID, l'application fédérale, et le même téléphone, toutes choses étant égales par ailleurs, avec l'application Alerte COVID, lequel... est-ce qu'il y a une différence dans la vulnérabilité de ces deux téléphones-là à des attaques?

M. Gambs (Sébastien) : Bien, le fait que... si vous n'utilisiez pas le Bluetooth avant et qu'Alerte COVID vous fait utiliser le Bluetooth, comme je l'ai dit tout à l'heure, vous ouvrez la porte à des failles de sécurité Bluetooth.

M. Nadeau-Dubois : Parfait. Sur la technologie Bluetooth, en terminant, est-ce que c'est une technologie qui a été inventée pour mesurer avec précision des distances?

M. Gambs (Sébastien) : Pas du tout. À la base, c'est une technologie de communication courte distance entre téléphones. Donc, par exemple, si vous avez une PS4, c'est ce qui va permettre à votre manette de parler avec la console. Donc, c'est vraiment un usage détourné qu'on en fait, de mesurer la proximité. Je ne dis pas que c'est impossible, mais il va y avoir... je ne suis pas venu sur la discussion des faux positifs et faux négatifs, mais il va y avoir des gens, on aura l'impression qu'ils sont proches de nous alors qu'ils étaient loin, et puis, à l'inverse, des gens qui seront à côté de nous, mais à cause d'une vitre, finalement, on ne...

M. Nadeau-Dubois : Est-ce qu'on peut dire que la technologie... Est-ce qu'on peut affirmer que la technologie Bluetooth est fiable pour mesurer la distance avec certitude?

M. Gambs (Sébastien) : Avec certitude, non, mais ça, ça me semble... Je pense qu'il faudrait... Je n'ai pas les chiffres en tête, mais il faudra aller voir les études les plus récentes sur le taux de faux positifs, faux négatifs. Mais je pense que, n'importe quel contexte technologique, c'est rare qu'on ait de la certitude. Mais, clairement, non, on ne peut pas savoir avec certitude, en particulier le type de téléphone que vous avez et qui... métadonnée envoyée est envoyée... parce qu'en fonction de deux téléphones différents, la puissance du signal ne sera pas la même et...

M. Nadeau-Dubois : Donc, si je résume votre propos, vous êtes plutôt certain qu'il y a des risques associés à la technologie Bluetooth et plutôt dubitatif qu'il y a une fiabilité dans la mesure de distance. Est-ce que je résume bien votre propos?

M. Gambs (Sébastien) : Oui, mais je mettrais quand même un bémol en regardant les dernières études pour savoir quels sont les taux de faux positifs et négatifs dans la mesure de distance, mais c'est sûr que ça ne sera pas parfait.

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

M. Ouellette : Merci, M. le Président. Vous savez, quand on reçoit des experts puis qu'effectivement on pose des questions, on s'intéresse au sujet du jour. Puis effectivement, Mme la députée de Jean-Talon, merci d'avoir posé la question tantôt, qui était une question un peu plus personnelle, mais j'ai vu que, suite à la réponse, on a tous regardé nos téléphones puis on est plusieurs à avoir désactivé le Bluetooth, le temps de comprendre, sur l'heure du midi, là, où est-ce qu'on est à risque puis où est-ce que notre surface d'attaque est là 24 heures par jour, parce que ça va nous le dire. Ça fait que, juste là-dessus, merci, vous avez fait l'éducation de plusieurs députés de la commission aujourd'hui.

Vos premiers commentaires aujourd'hui, vous avez dit que ce qui n'a pas été abordé depuis le début de la commission auprès des experts, vous avez parlé de critères mesurables, des critères mesurables en reddition de comptes ou des critères mesurables... J'aimerais ça vous entendre un peu plus.

M. Gambs (Sébastien) : ...reddition de comptes. Donc, par exemple, s'il y a... si le gouvernement choisit d'aller avec une application, je pense que ce sera important de dire : O.K., comment est-ce qu'au bout de deux mois on va savoir si l'application a atteint sa cible? Ça va être quoi qu'on va mesurer? Est-ce qu'on va mesurer le nombre de personnes qui ont été notifiées par cette application-là? Est-ce qu'on va mesurer le nombre de personnes dont on a sauvé les vies, ce qui va être difficile? Donc, c'est vraiment quel va... On parlait de la gouvernance avec ce comité consultatif. Quels sont les critères que le comité consultatif va pouvoir regarder pour mesurer si l'application a été un succès ou un échec?

M. Ouellette : On a parlé de comité consultatif en reddition de comptes. Vous nous avez parlé qu'il faudrait que leurs recommandations puissent être exécutoires, aussi. Donc, il faut que ça soit prévu dans un processus législatif, que le comité d'experts, bien, il ne sera pas là juste par parure, parce qu'il faut bien paraître ou parce que... On regarde un peu ce qui se passe ailleurs. Des fois, les décisions ou les recommandations sont longues, ou tu as juste un pouvoir de recommandation, mais, dans la vraie vie, ce n'est pas applicable. Donc, c'est des choses qu'il faut prévoir dans notre processus législatif.

M. Gambs (Sébastien) : Je pense... Enfin, je suggérerais de faire ça. Après, j'avoue ma méconnaissance du système québécois, je ne sais pas à quel point c'est possible de mettre en place un comité qui a des avis exécutoires versus consultatifs.

M. Ouellette : L'autre chose que vous nous avez dite aussi, c'est que, dans le cadre d'un processus législatif, normalement, il y a des consultations. Les consultations d'aujourd'hui, c'est une chose. Si le gouvernement décidait d'aller vers un processus législatif, vers une loi, il va y avoir des consultations particulières. Dans les consultations particulières, à la lumière de ce que vous avez regardé de l'application canadienne, entre autres, puis ce sera en fonction de regarder aussi du choix du gouvernement qui sera fait en fonction des valeurs québécoises, ce serait important... Si c'était l'application canadienne, en consultations particulières, vous exigeriez, si vous aviez le pouvoir, que BlackBerry, Shopify, les développeurs, les bénévoles qui l'ont développée, Google, Amazon viennent expliquer leur partie ou leur créneau de participation dans ce qui va être imposé aux citoyens du Québec.

M. Gambs (Sébastien) : Oui. Je ne sais pas si «exiger» serait le mot, mais je leur demanderais fortement de venir expliquer les enjeux et...

M. Ouellette : Non, mais c'est quelque chose qui est important pour vous, là, parce que...

M. Gambs (Sébastien) : Ça me semble... parce que, comme je disais, l'écosystème des applications est complexe. Souvent, on voit une app comme un objet sur notre téléphone, mais il y a beaucoup d'acteurs en arrière-plan.

M. Ouellette : Merci.

Le Président (M. Bachand) : Merci infiniment de votre présence aujourd'hui. Sur ce, la commission suspend ses travaux jusqu'à 14 heures. Merci.

(Suspension de la séance à 12 h 18)

(Reprise à 14 h 01)

Le Président (M. Bachand) : À l'ordre, s'il vous plaît! Bon début d'après-midi. Bienvenue à tous. La Commission des institutions reprend ses travaux. Je demande, bien sûr, à toutes les personnes 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 sur leur acceptabilité sociale dans le cadre de la lutte contre la COVID-19.

Cet après-midi, nous entendrons les personnes et les groupes suivants : le représentant du Comité consultatif en cybersécurité, le directeur du Groupe de recherche sur la surveillance et l'information au quotidien, M. Pierre-Luc Déziel, l'Association québécoise des technologies et M. Steve Waterhouse.

Alors, il nous fait plaisir de recevoir en visioconférence le Dr Debbabi, du Comité consultatif en cybersécurité. Alors, docteur, bienvenue, un grand plaisir de vous voir, d'être avec vous aujourd'hui. Je vous rappelle, vous avez 10 minutes de présentation, après nous aurons un échange avec les membres de la commission. Alors, la parole est à vous.

M. Mourad Debbabi

(Visioconférence)

M. Debbabi (Mourad) : Merci beaucoup, M. le Président. C'est un plaisir pour moi d'être avec vous aujourd'hui et d'avoir l'opportunité, donc, de partager avec vous certaines des informations importantes sur ce dossier important, surtout dans les circonstances actuelles où on a cette pandémie.

Donc, ces applications-là, c'est un outil technologique qui peut s'avérer extrêmement important, il peut aider à briser la chaîne de propagation du virus. Et ça demande de le faire de manière sécuritaire, donc il y a certains principes, je dirais, qui sont fondamentaux, qu'il faut observer quand on conçoit, ou on développe, ou on déploie des solutions technologiques qui permettent de tracer les personnes infectées et d'alerter ceux qui ont été en contact avec ces personnes-là.

D'abord, il y a des principes simples. Il faut impliquer, dans le développement de ces applications, des experts en cybersécurité et des experts dans la confidentialité de la vie privée. Ces experts-là... parce que ce n'est pas... de développement de logiciel, c'est aussi un effort où on doit regarder de très près la protection des informations personnelles collectées, la protection de ces applications, ainsi que protéger contre des attaques éventuelles de géolocalisation, de divulgation d'informations personnelles, etc.

Parmi les principes, donc, d'une part, il faut impliquer les experts dans le développement et le déploiement. D'un autre côté aussi, une fois que ces applications-là sont développées, il faut les faire évaluer par des experts

indépendants en cybersécurité et en confidentialité de la vie privée. Et, comme j'ai dit tout à l'heure, il y a des principes très, très simples, qui sont fondamentaux, qu'il faut observer quand on développe ce genre d'application.

Parmi ces principes-là, j'ai mentionné l'examen par des experts indépendants. Ça, c'est quelque chose qui est extrêmement important. Ça valide la conception, ça valide qu'on est protégés contre des attaques, surtout quand on sait que ces infrastructures technologiques là relèvent des infrastructures critiques. On peut penser que, si quelqu'un, par exemple, attaque une solution technologique comme celle-là, on peut amener beaucoup de gens à faire des tests, on peut amener beaucoup de gens à être en confinement ou en quarantaine, donc il faut accorder une certaine attention aux aspects sécurité et aux aspects confidentialité de la vie privée.

Deuxième principe fondamental, je dirais, il faut que la conception de ces applications soit simple, dans le sens où il ne faut pas que le modèle sous-jacent, technologique soit alambiqué ou complexe parce que, d'abord, ça va complexifier aussi l'étape de vérification et l'étape d'examen pour valider que ces applications n'auront pas de répercussions sur les aspects sécurité et de confidentialité de vie privée.

Troisième principe, il faut qu'il y ait une fonctionnalité minimale, c'est-à-dire il ne faut pas aller au-delà de l'objectif de cette application-là, c'est-à-dire il ne faut pas qu'à la volée on essaie de collecter d'autres informations qui ne sont pas nécessaires à l'objectif en question. Il faut aussi minimiser la collecte des données, et donc il ne faut pas collecter des données personnelles ou des données qui permettent d'identifier une personne, ce qu'on appelle les PII, les «personally identifiable informations». Et, si jamais on doit récolter de l'information sensible, de préférence, il faut que cette information, elle réside sur le dispositif, sur le téléphone, ou sur la tablette, ou sur l'ordinateur de la personne à qui appartient cette information, donc il ne faut pas partager cette information. Et, quand il est question de partager, on partage de l'information, mais pas nécessairement de l'information sensible. Donc, il faut minimiser la collecte des données.

Et, cinquième principe, je dirais, c'est la gouvernance des données de confiance. Donc, quand on collecte de l'information sensible, on ne peut pas la stocker. S'il faut la stocker quelque part, une partie ou un fragment de cette information-là, il faut que l'autorité en question soit une autorité de confiance, par exemple une agence gouvernementale, qui peut être soumise à un contrôle public. Donc, il ne faut pas que ça soit une tierce personne, ou une industrie, ou quelque chose comme ça.

Sixième principe fondamental, la cybersécurité de ces applications. Donc, quand on développe des applications comme ça, avec une infrastructure, comme j'ai mentionné, qui relève de l'infrastructure critique du pays, donc, il faut attacher beaucoup d'importance aux aspects sécurité, la protéger, protéger ce déploiement-là contre toutes sortes d'attaques, des attaques qui permettent de voler des informations sensibles, des attaques qui permettent de géolocaliser des personnes ou de divulguer l'identité des personnes qui sont infectées, etc.

Aussi, septième principe, je dirais, une conservation minimale de l'information. Donc, quand on conserve de l'information, il ne faut pas aller au-delà du besoin, donc il faut faire une rétention minimale de cette information. Évidemment, il faut aussi sécuriser des consentements de toutes les parties qui sont impliquées.

Et, 10e principe, il faut prévoir un dispositif d'extinction de ces applications. On les met en place pour combattre la pandémie, mais, une fois que cela est terminé, il faut prévoir un dispositif d'extinction de ces applications.

Donc, ça, c'est les 10 principes fondamentaux. On les a articulés dans une publication qui émane d'un groupe que je dirige avec d'autres collègues au Canada. On est à peu près 140 chercheurs, au Canada, qui se sont structurés dans une organisation qui s'appelle le Consortium national de cybersécurité, et ce consortium a été créé pour fédérer toutes les forces vives en recherche en développement dans le domaine de la sécurité... de la cybersécurité et de la confidentialité de la vie privée. Donc, on avait fait une publication quand on a vu qu'il y a beaucoup d'applications qui commençaient à sortir, et certaines de ces applications-là ne respectent pas les principes de sécurité et de confidentialité de vie privée. Donc, on avait fait une publication, il y a à peu près, je dirais, un mois et demi, dans laquelle nous avons alerté le public, et les agences, et les autorités compétentes sur l'importance des 10 principes que je viens d'articuler, notamment l'examen par des experts indépendants, la conception simple, le fonctionnement minimal, la minimisation des données, la gouvernance des données de confiance, la cybersécurité, la conservation minimale des données, la protection des données et métadonnées dérivées, et la divulgation et consentement appropriés, et finalement le dispositif d'extinction.

• (14 h 10) •

Maintenant, dans la deuxième partie de cette intervention, je vais parler très brièvement de deux classes ou deux catégories d'applications qu'on a vues, qui ont émané ou qui ont été proposées. D'abord, il y a des applications qui reposent sur la technologie GPS. Donc, on utilise la technologie GPS pour localiser les personnes, et l'information qu'on récolte, elle est soumise à des algorithmes d'intelligence artificielle, et d'apprentissage automatique, et d'apprentissage profond, et c'est avec ça qu'on essaie de découvrir quels sont les gens qui ont été exposés au virus et les avertir en conséquence. La deuxième catégorie, c'est une catégorie d'applications qui reposent sur les technologies de type Bluetooth, et donc avec une conception simple et minimale.

Donc, si on compare les deux technologies très rapidement, les technologies GPS, c'est un choix qui est discutable ou peut-être pas très judicieux pour ce type d'application parce qu'il y a des implications sérieuses en matière de confidentialité de vie privée, d'une part, mais, d'autre part, aussi des implications, je dirais, négatives du côté de l'efficacité de ces applications. Comme on sait, le GPS a une granularité d'à peu près 10 mètres, donc la précision de la localisation, elle est dans un intervalle de 10 mètres, et on sait très bien que, pour le virus, la distance minimale requise, elle est de l'ordre de deux mètres. Déjà, au départ, les technologies de type GPS n'ont pas la précision nécessaire pour ce genre d'application.

Deuxièmement, on sait que le GPS... on a tous expérimenté ça quand on utilise notre GPS, on a des problèmes quand on est dans des immeubles qui sont d'une certaine hauteur, assez grande, ou d'une hauteur conséquente, on perd souvent le signal GPS. Et, en général, dans ce genre d'agglomération, on a des buildings qui sont assez élevés, on a aussi une densité de population qui est élevée. Ça, c'est une autre raison pour ne pas recourir à la technologie GPS.

Par ailleurs, on a vu aussi que ces applications qui utilisent les technologies GPS utilisent ce qu'on appelle les algorithmes d'intelligence artificielle ou d'apprentissage automatique. L'apprentissage automatique, c'est un outil, définitivement, qui est merveilleux et qui peut donner d'excellents résultats, mais, pour ce type d'application, il pose un peu de problèmes parce qu'il nécessite le partage d'informations sensibles, et aussi on n'a pas une visibilité. En général, les algorithmes d'apprentissage, surtout l'apprentissage profond, c'est des boîtes noires, et on ne sait pas toujours expliquer les résultats qui sortent de ces algorithmes.

Le Président (M. Bachand) : Dr Debbabi, je vais devoir vous arrêter là, parce qu'on doit débiter la période d'échange avec les membres de la commission.

M. Debbabi (Mourad) : Parfait.

Le Président (M. Bachand) : Merci beaucoup. On débute avec la députée de Jean-Talon. Merci beaucoup.

Mme Boutin : Bonjour, M. Debbabi. Merci beaucoup d'être présent. Je connais un petit peu votre travail et puis je connais aussi votre crédibilité en la matière. Mais je vous laisserais terminer avant de poser mes questions, parce que ça va aller un petit peu dans ce sens-là. J'aime bien que vous compariez, là, Bluetooth puis GPS, parce qu'on a plusieurs questionnements, nous-mêmes, dans la commission, par rapport à l'efficacité, les risques sous-jacents également.

M. Debbabi (Mourad) : Merci beaucoup, Mme la députée de Jean-Talon. Donc, c'est vrai que, brièvement, j'avais mentionné quelques inconvénients de la technologie GPS. Je pense que c'est une excellente technologie pour nous orienter, nous guider quand on prend une route, ou quelque chose comme ça, dans des contextes de navigation, mais, pour... Je pense, j'avais mentionné certains des inconvénients qui font en sorte qu'elle n'est pas nécessairement appropriée, que ce soit d'un point de vue efficacité ou d'un point de vue de confidentialité de la vie privée.

En contrepartie, les applications qu'on a vu sortir, que ce soit en Europe ou bien au Canada et au Québec, c'est des applications basées sur Bluetooth, une conception très, très simple, un échange minimal d'information avec... Il y a eu pas mal de publications qui expliquent le fonctionnement de ces applications-là. Et on a vu aussi qu'il y avait beaucoup d'évaluations — il y avait de la sécurité et de la confidentialité de la vie privée — qui démontrent que ces applications-là ont un risque minimal et qu'elles sont, jusqu'à un certain degré, à un très grand degré, sécuritaires et respectent la confidentialité de la vie privée.

Mme Boutin : J'ai une question par rapport aux principes, parce que j'ai vu la publication avec les 140 chercheurs et les 10 principes puis... Entre les deux, entre la technologie GPS ou la technologie Bluetooth, laquelle des applications respecte le plus les principes? Je vais poser la question différemment. Est-ce que l'application qui a été proposée par le Canada, qui est, bon, celle un petit peu Bluetooth... est-ce qu'elle respecte un maximum de principes? Et puis, sinon, quels principes devraient être plus mis de l'avant ou qu'on aurait... qu'il ne faudrait surtout pas oublier?

M. Debbabi (Mourad) : C'est une excellente question, Mme la députée de Jean-Talon. Donc, en fait, la publication des 140 chercheurs, elle émanait... Quand on a vu certaines publications qui sont sorties sur des applications qui utilisent la technologie GPS, c'est ça qui nous a amenés à rédiger le document qui a été partagé. Et donc je pense que les gens qui ont développé des applications qui reposent sur la technologie GPS avaient une expertise indéniable en matière d'intelligence artificielle, d'apprentissage automatique, mais je ne pense pas qu'ils ont associé à cet effort de développement conséquent des experts de sécurité, donc il y avait certains principes qui n'étaient pas respectés. Par exemple, il y avait une exposition de l'information sensible. J'avais mentionné que la technologie GPS, c'est un choix qui est discutable et pas nécessairement qui va dans le sens de l'efficacité. Donc, il y avait beaucoup de principes qui n'étaient pas respectés, que ce soit sécurité, confidentialité, efficacité.

D'un autre côté, l'application qui a été développée au Canada, en fait, elle a été influencée par l'effort qui a été fait en Europe avec l'application DPT. Il y a beaucoup de publications à cet égard-là. Il y a un consortium de développeurs et de chercheurs européens qui ont articulé une architecture qui était très, très bien analysée côté sécuritaire, très, très bien analysée côté confidentialité de la vie privée, avec une architecture simple, très, très simple qui collecte une information minimale, qui n'est pas nécessairement sensible, qui laisse le contrôle aux gens sur leur mobile, et, je pense, elle respecte la majorité des principes que j'ai mentionnés, les 10 principes.

Mme Boutin : J'ai une question par rapport à l'efficacité, parce que c'est un questionnaire qui revient dans les médias et même ici, au sein de la commission, parce que, bon, il n'y a pas de rapport officiel ou d'étude très sérieuse qui a été encore publié, il y en a peut-être en rédaction en ce moment. Mais admettons qu'un outil comme une application Bluetooth, comme le fédéral, était adoptée en complément et qui était... bon, on mettrait toutes les

mesures de sécurité autour puis on respecterait les principes, mais qui aurait un taux d'adhésion relativement important, est-ce qu'un outil comme ça pourrait avoir un effet positif sur le contrôle de la pandémie ou sur l'identification des contacts? Est-ce que ça faciliterait le rôle de la... Ça pourrait faciliter le rôle de la Santé publique, qui fait une identification manuelle, actuellement. Est-ce que ça pourrait faciliter leur rôle, s'il y avait une adhésion suffisante, selon vous?

M. Debbabi (Mourad) : Ça, c'est une très, très bonne remarque. Je pense qu'une prémisse de la réussite de cette technologie-là, c'est le niveau d'adoption. Donc, pour être... pour avoir un impact réel et positif, il faut qu'il y ait une large adoption. Mais, dans les chiffres que j'ai vus circuler, donc, on est déjà à quelques millions, peut-être, au Canada, j'ai vu, par exemple, qu'en Allemagne, aussi dans certains pays européens, il y avait une adoption qui est très, très large, et, je pense, dès le moment où on atteint le niveau des millions d'utilisateurs de ces applications-là, on commence à avoir un certain retour sur l'investissement, donc on commence à être efficaces et à contribuer... Je ne pense pas que cette technologie à elle seule va limiter la propagation du virus, mais, définitivement, elle contribue de manière significative à briser la chaîne de propagation du virus.

Mme Boutin : J'ai une dernière petite question avant de laisser la parole à mes collègues. On a une autre préoccupation, collectivement, ici, c'est sur la sécurité de la technologie Bluetooth. On s'est même questionnés, on a regardé nos téléphones cellulaires, à savoir peut-être qu'on est en train de se faire pirater. Premièrement... Puis moi, j'ai entendu, bon, dans les médias ou d'experts, que les failles ont été réglées. Mais moi, je ne suis pas une experte de Bluetooth. J'aimerais vous entendre là-dessus. Puis qu'est-ce qui pourrait être mis en place, aussi, pour s'assurer d'une sécurité... on s'entend qu'en cybersécurité, on le sait, le risque zéro n'existe pas, mais, pour minimiser les risques...

M. Debbabi (Mourad) : Très bonne question. Premièrement, l'information qui est échangée par les applications de type Bluetooth, l'information, elle n'est pas du tout sensible, elle est censée être publique. Et quelqu'un qui intercepte cette information-là ne pourra pas nécessairement extraire beaucoup de choses de cette information. D'un point de vue utilité, il n'y a pas beaucoup d'information là-dedans. C'est une séquence de nombres, qui est, en fait, le résultat d'une opération de chiffrement, qu'on appelle un hachage. Donc, ça génère une séquence de chiffres, on ne peut pas faire grand-chose avec ça. Elle n'a de sens que pour celui qui possède la clé, et la clé, elle est à l'intérieur du téléphone, dans une zone qui est très, très sécurisée du système d'exploitation, que ce soit Android ou que ce soient les types de téléphones de type iPhone. Et, si on a la clé et on a ces informations échangées d'identification, les identifiants de proximité variable, là, on ne pourra pas... on pourra faire quelque chose, mais la clé n'est pas distribuée, donc on ne pourra pas faire grand-chose avec cette information, l'information, elle est publique. Je pense que le risque sécuritaire, il est vraiment minime avec l'usage de la technologie Bluetooth.

• (14 h 20) •

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

M. Lévesque (Châteauguay) : Merci, M. le Président. Merci, M. Debbabi, d'être ici avec nous, là, cet après-midi.

J'aimerais peut-être reprendre certains de vos principes clés, fort intéressants, forts pertinents. Le premier, d'abord, là, vous émettez, donc, le principe comme quoi il faudrait qu'il y ait des experts autant en cybersécurité qu'en, dans le fond, protection de la vie privée et protection également de renseignements personnels, autant dans le développement que le déploiement d'applications. Est-ce que vous avez vu, de par vos recherches, certaines applications, dans le monde, qui auraient suivi ce protocole-là ou ce principe-là? Donc, disons qu'il y a eu le développement, dans le fond, de cette application-là et que ça a pu être déployé par la suite... Sinon, qu'est-ce qui aurait dû être fait? Puis comment, dans le fond, vous auriez vu ce développement-là?

M. Debbabi (Mourad) : Merci beaucoup, M. le député de Sherbrooke. La question est très pertinente. Donc, pour les exemples...

M. Lévesque (Châteauguay) : Un peu plus à l'est... à l'ouest, c'est-à-dire, l'ouest. L'autre ouest, oui.

M. Debbabi (Mourad) : L'application... Deux exemples que j'ai en tête. L'application qui a été développée, par exemple, en Europe, DPT, là, il y a un document qui a été publié, on voit qu'il y a un consortium très riche en expertise. Il y avait des experts de sécurité et il y avait des expertes de confidentialité de vie privée. Et j'ai fait, personnellement, la lecture du document où on détaille la conception et on articule les différents détails techniques de l'application, on sent que ça a été fait par des professionnels, et il y a énormément de détails qui ont été très, très bien pensés.

Le deuxième exemple que je mentionne, c'est l'application canadienne, qui a été élaborée par Google et Apple avec le concours de firmes canadiennes comme BlackBerry, Shopify, etc. C'est une application, dès le départ, donc on avait pensé très, très bien aux aspects sécurité, aux aspects confidentialité de la vie privée. Comme j'ai mentionné, l'architecture, elle est très, très simple, et on avait pris des précautions additionnelles. Par exemple, il y a eu une évaluation par les effectifs de sécurité de la compagnie BlackBerry. Il y a aussi une évaluation qui a été faite par le Centre canadien de cybersécurité, qui est une autorité importante en expertise en termes de cybersécurité et de confidentialité de vie privée.

Par ailleurs, il y avait aussi plein d'agences, des commissaires à la vie privée, que ce soit dans des provinces ou que ce soit au niveau fédéral, qui ont regardé de très près les aspects confidentialité de la vie privée et sécurité de ces applications-là, et, jusqu'à un certain degré, la majorité, ils ont émis des avis favorables. J'ai vu aussi des analyses très techniques par des experts indépendants qui ont... qui révèlent quelques faiblesses, mais qui ne sont pas des faiblesses, je dirais, à haut risque. Comme vous le savez, on ne peut pas arriver à une sécurité à 100 % ou à confidentialité de vie privée à 100 %, il y a toujours un risque résiduel. Mais, à la lumière de ce qui a été fait comme efforts, à la lumière des évaluations et analyses qui ont été faites, on arrive à la conclusion qu'il y a... ça a été très, très bien pensé, et le risque résiduel est assez minime.

M. Lévesque (Chapleau) : Un risque assez minime. Nous avons également un expert, hier, qui nous parlait, lors du développement de l'application en France, que des hackers avaient eu... disons, des hackers amis, là, qui avaient eu la possibilité d'améliorer l'application. Est-ce qu'en plus des différents experts que vous mentionnez ce serait une voie, également, à emprunter, de permettre à certains hackers de venir améliorer ou d'aller chercher des failles dans l'application?

M. Debbabi (Mourad) : Certainement. Mais en fait, quand je dis «des experts qui évaluent», il y a deux types d'évaluations. On peut évaluer en faisant, par exemple, l'examen de l'architecture, les protocoles qui sont utilisés. On peut évaluer en regardant le code, on lit le code source de ces applications-là. Il y a des outils, aussi, automatiques qui permettent de trouver des failles, etc., dans du code. On peut aussi évaluer en attaquant l'application qui a été développée, et c'est à ça que vous faites référence. Mais, moi, quand je dis, par exemple, «une évaluation de la sécurité et de la confidentialité», j'inclus aussi l'effort qui consiste à attaquer l'application pour éventuellement découvrir des vulnérabilités et les réparer.

M. Lévesque (Chapleau) : Peut-être une dernière question, là, sur les points 7 et 8, là, conservation minimale de données, protection des données et métadonnées dérivées, et le 9 également, divulgation et consentement appropriés. Est-ce que vous considérez... J'imagine que vous avez regardé également, là, la réglementation puis, peut-être, le cadre législatif qui encadre ce type d'application. Est-ce qu'actuellement vous considérez que c'est pertinent? Est-ce qu'il y aurait des éléments à ajouter pour répondre, dans le fond, de façon favorable à ces trois principes clés que vous avez mis dans la liste?

M. Debbabi (Mourad) : Je pense que l'information qui est collectée, elle est très minimale. Et, comme j'ai mentionné, les identifiants de proximité variable, c'est des chiffres qui n'ont pas de sens si on n'a pas la clé. La clé, elle est gardée de manière sécuritaire au sein... dans une couche qui est très, très bien protégée du système d'exploitation de chaque téléphone ou ordinateur.

La seule, je dirais, information qui est sensible, c'est l'adresse IP de la personne qui se connecte au serveur fédéral, et cette information-là, elle est au sein... Premièrement, elle n'est pas associée à d'autres informations, donc, en tant que tel, elle ne pose pas de problème. Et, en outre, elle est chez une autorité de confiance, qui peut être... qui peut recevoir aussi des audits publics, etc., donc je ne pense pas que c'est quelque chose qui est très, très grave, de ce point de vue là.

M. Lévesque (Chapleau) : Un autre de vos principes clés. Parfait. Merci, M. le Président.

Le Président (M. Bachand) : Il vous reste une minute, Mme la députée des Plaines.

Mme Lecours (Les Plaines) : Merci, M. le Président. Très rapidement, une question d'explication. Votre prédécesseur aux auditions nous parlait de l'application en Europe, où les jeunes ont décroché, et ce qu'il expliquait, c'est que...

(Interruption)

Mme Lecours (Les Plaines) : ... — eh mon Dieu! Il y a une réverbération — ce qu'il expliquait, c'est que l'application vient en interférence avec d'autres, donc ils décident tout simplement de décrocher. Pouvez-vous m'expliquer davantage... Et comment est-ce qu'on pourrait faire, surtout si vous dites qu'elle doit être minimale, comment est-ce qu'on pourrait faire pour contrecarrer cette réalité?

M. Debbabi (Mourad) : Je me suis... Selon moi, là, je ne comprends pas la problématique de l'interférence avec votre application. Et vous avez mentionné les capacités de décrocher... C'est une application qui est très petite, qui est très, très stable, qui tourne sur un téléphone, donc, si le téléphone fonctionne bien, il n'y a pas de problème. Il fait quelques connexions avec le serveur provincial et le serveur fédéral. Ce n'est pas une connexion qui est fréquente, ce n'est pas une connexion qui est intense. Il n'y a pas un volume important de données qui est échangé, c'est des informations très, très minimales. Donc, je ne vois pas où est le risque d'interférence, où est le risque de problème avec ça, c'est vraiment une application légère. Et c'est l'avantage d'avoir un design qui est simple, c'est qu'il n'y a pas de risque d'interférence, il n'y a pas de risque de mal fonctionnement. Si le téléphone se porte bien, de l'autre côté, du serveur, aussi, ce n'est pas quelque chose qui est coûteux en bande passante ou qui est coûteux parce qu'il y a beaucoup de trafic qui circule, etc. Je ne vois pas de risque à cet égard.

Le Président (M. Bachand) : Merci beaucoup. Je cède maintenant la parole à la députée de Saint-Laurent.

(Interruption)

Mme Rizqy : Je crois que l'écho est par chez vous, Pr Debbabi. Je ne sais pas si ça va être corrigé. Ah! maintenant, on entend mieux. Alors, bonjour et bienvenue parmi nous.

Plusieurs de nos invités ont mentionné qu'en fait c'était une des pires solutions, et vous, vous dites que c'est la plus minime. Pouvez-vous, s'il vous plaît, distinguer pourquoi que vous, vous trouvez que ça peut être quand même sécuritaire, cette application?

• (14 h 30) •

M. Debbabi (Mourad) : Pourquoi elle est sécuritaire? Comme j'ai mentionné, ça a été examiné de manière minutieuse par des experts qui ont une très grande crédibilité, notamment le Centre canadien de cybersécurité, qui est une instance hautement respectable en matière de cybersécurité, ça a été examiné par des ingénieurs de sécurité de plusieurs clients, notamment la firme, par exemple, BlackBerry, ça a été examiné par des chercheurs indépendants. Ça a été bien pensé, même, au départ, d'un point de vue sécurité, et c'est très clair, donc, quand on lit les documents qui détaillent le design de cette application-là, on voit très clairement que beaucoup d'aspects ont été très, très bien pensés.

Par ailleurs, il y a plusieurs commissaires... Est-ce que vous m'entendez?

Mme Rizqy : ...à quelle application vous faites référence? Celle de l'alerte du fédéral?

M. Debbabi (Mourad) : Oui, oui.

Mme Rizqy : O.K. Est-ce que vous pouvez nous dire quand il y a eu la dernière défaillance?

M. Debbabi (Mourad) : Est-ce qu'il y a eu une défaillance?

Mme Rizqy : Oui, la semaine dernière.

Le Président (M. Bachand) : Juste avant, le technicien me demande, s'il vous plaît, de baisser le volume de vos haut-parleurs, Dr Debbabi, peut-être que ça pourrait aider à la non-réverbération.

M. Debbabi (Mourad) : O.K.

Le Président (M. Bachand) : Merci infiniment. Désolé, Mme la députée.

Mme Rizqy : Quand y a-t-il eu une défaillance avec le système qui a été lancé par le fédéral?

M. Debbabi (Mourad) : Moi, je suis au courant de quelques risques résiduels...

Mme Rizqy : Non, je vous demande quand est-ce qu'il y a eu une dernière défaillance.

M. Debbabi (Mourad) : Je ne suis pas au courant d'une défaillance de cette application.

Mme Rizqy : La semaine dernière, en fait.

M. Debbabi (Mourad) : Mais quel genre de défaillance? Moi, je ne suis pas au courant de ces défaillances.

Mme Rizqy : Bien, j' imagine qu'au centre de cybersécurité vous faites des suivis, non? Parce que, là, on n'a pas eu l'occasion d'avoir des rapports... un rapport de votre part, et vous faites quand même des affirmations assez importantes. Alors, c'est pour ça que j'essaie de bien comprendre vos affirmations, si elles sont factuelles avec la réalité en date d'aujourd'hui.

On est... Il y a eu des défaillances avec l'application qui a été téléchargée. On a vu qu'il peut y avoir des brèches, et même un des invités ce matin nous parlait qu'il y avait des trous, qu'il était possible aussi de pouvoir faire encore de la réidentification. Est-ce que, ça, vous l'avez vérifié?

M. Debbabi (Mourad) : Oui, oui, j'ai regardé ces aspects-là, oui.

Mme Rizqy : Parce que c'est plusieurs... On parle de réidentification, là, donc ce n'est pas des données qui sont anonymes. Et, en date du 31 juillet, le commissaire à la vie privée fédéral a mentionné aussi que c'est une probabilité, là, qu'on peut réidentifier.

M. Debbabi (Mourad) : Bien, il y a deux risques qui sont sous-jacents. Mais ça, c'est des vulnérabilités. Ce n'est pas des attaques qui ont réussi, c'est des vulnérabilités. Donc, il y a deux vulnérabilités. Notamment, il y a l'identification, qui est un risque. Il y a l'identification...

Mme Rizqy : La semaine passée, il y a eu une brèche, donc il y a eu une attaque. Mais, bon, tantôt...

M. Debbabi (Mourad) : Moi, je suis au courant de vulnérabilités et non pas d'attaques.

Le Président (M. Bachand) : S'il vous plaît...

M. Debbabi (Mourad) : Il y a deux vulnérabilités. Il y a l'identification. Si on est dans une zone où il y a très peu de gens, isolée, donc, effectivement, on peut identifier la personne, mais ça, c'est un risque qui est très, très résiduel. Deuxième risque qu'on voit, si on a énormément de téléphones et on les déploie à plusieurs intersections, on peut faire un traçage des personnes, une identification avec un traçage, mais ça, c'est un scénario qui est extrêmement peu probable.

Mme Rizqy : La fuite chez Desjardins, c'était un scénario peu probable, et c'est arrivé, alors vous comprendrez que, nous, notre objectif, c'est de voir toutes les possibilités, et c'est pour ça qu'on pose ces questions. Alors, vous comprendrez que, même quand qu'il y a un petit trou, malheureusement, l'être humain, comment est-il, il va vouloir exacerber ce trou.

Mais, si vous permettez, vous avez aussi affirmé que les données, au niveau fédéral, étaient hébergées de façon sécuritaire chez un tiers de confiance. Le tiers de confiance auquel vous faites référence, est-ce que vous parlez bien d'Amazon Web Services?

M. Debbabi (Mourad) : Oui, oui, oui.

Mme Rizqy : C'est quand, la dernière fois qu'il y a eu une fuite de données chez Amazon?

M. Debbabi (Mourad) : Ça, c'est une bonne question. En fait...

Mme Rizqy : En fait, là, on a parlé de 100 millions de détenteurs de cartes de crédit. Un ancien employé a été capable de hacker et d'avoir accès à 100 millions de cartes de crédit américaines et aussi canadiennes. Est-ce que c'est toujours un tiers de confiance, alors que...

M. Debbabi (Mourad) : En effet, il y a deux réponses à cela. Moi, je suis un expert de sécurité. Je vois quotidiennement des dizaines de milliers d'attaques. Il n'y a aucune institution dans le monde qui n'est pas attaquée. La question... est-ce qu'on va être attaqué ou pas, c'est juste une question de temps.

La question, maintenant : Est-ce qu'on a la capacité de répondre? Est-ce qu'on a la capacité de détecter? Est-ce qu'on a la capacité d'atténuer? Maintenant, supposons... prenons le pire scénario que vous êtes en train d'énumérer, supposons qu'Amazon est attaqué. Qu'est-ce qu'on va découvrir? On va découvrir les adresses IP de gens qui se sont connectés et peut-être des clés de chiffrement. Qu'est-ce qu'on peut faire avec ça? Vous savez très, très bien que nos téléphones reçoivent une adresse IP qui est... qui n'est pas statique, qui est souvent dynamique, parce que les fournisseurs d'accès Internet, ils ont des adresses dynamiques qui sont allouées par un protocole DHCP, donc on ne peut pas remonter à la personne facilement, à moins d'avoir une autre base de données, peut-être gouvernementale, où on associe les adresses IP avec des personnes. Donc, je pense, honnêtement, le risque, il est résiduel et très, très minime, à mon sens.

Mme Rizqy : Hier, nous avons reçu la Quadrature du Net, et, au contraire, ils nous affirmaient que, souvent, les gens, lorsqu'ils téléchargent, sont soit à la maison, parce qu'ils sont confinés, soit au travail et que l'adresse IP, à ce moment-là, n'était pas dynamique, mais statique, et par définition on était capable de relocaliser les gens de façon plus efficace.

Mais j'aimerais juste continuer pour... parce que je ne veux pas tomber non plus dans un argumentaire, j'aimerais revenir à certains fondamentaux assez importants. Vous dites qu'on serait en mesure de casser les chaînes avec cette application-là. Mais, dans le monde, on a des exemples concrets, vous l'avez aussi mentionné, si elle était téléchargée par des millions de personnes. Singapour, ce sont des millions de personnes qui ont téléchargé l'application, est-ce que ça a été utile, chez eux?

M. Debbabi (Mourad) : Premièrement, je ne travaille pas avec des organisations de santé, mais, dans les lectures que j'ai faites, ils mentionnent que ça a contribué beaucoup au contrôle de la pandémie dans ces pays-là, notamment la Corée du Sud, notamment le Singapour, et aussi on parlait d'un effet qui est très positif, par exemple, en Allemagne.

Mme Rizqy : Parce que ce que nous, on a lu, et ce que les rapports disent, c'est qu'au contraire de ce que vous venez d'affirmer, au Singapour, c'est exactement le contraire, des millions ont téléchargé, et le gouvernement, les autorités publiques ont clairement mentionné que ça a été pas efficace, et ils ont arrêté complètement l'utilisation, et ils sont allés dans une force beaucoup plus... dans une façon beaucoup plus intrusive avec le bracelet électronique pour ceux qui ont la COVID-19, et l'Australie a complètement abandonné cette pratique, même chose pour la Norvège. Est-ce que vous avez un exemple concret où est-ce que ça a été un franc succès?

M. Debbabi (Mourad) : Je n'ai pas d'informations qui émanent d'organismes de la santé.

Mme Rizqy : Bien, je vous remercie beaucoup. Je n'aurai pas d'autre question, M. le Président.

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

Mme Nichols : Je n'ai pas d'autre question.

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

M. Nadeau-Dubois : Merci, M. le Président. Vous faites certaines affirmations... Bien, d'abord, bonjour, merci d'être avec nous. J'ai peu de temps, je vais aller droit au but. Vous faites certaines affirmations qui sont plutôt surprenantes, Pr Debbabi, et qui détonnent avec ce que plusieurs autres experts nous ont dit depuis 48 heures. Vous parlez notamment de taux d'adoption qui seraient satisfaisants à plusieurs endroits dans le monde. La totalité des experts qui sont passés ici, y compris M. Bengio, qui était, jusqu'à tout récemment, un fervent partisan de ces applications, soutiennent le contraire, nous disent qu'au contraire c'est une des faiblesses plutôt généralisées, le fait qu'il y ait un faible taux d'adoption. Vous dites qu'en Allemagne le taux est satisfaisant. Quel est le taux en Allemagne?

M. Debbabi (Mourad) : Dans les lectures que j'ai faites, c'était dans l'ordre de millions.

M. Nadeau-Dubois : Mais il y a 83 millions de personnes en Allemagne. Moi, les chiffres que j'ai, qui sont issus de la CBC, une source quand même crédible, parlent de 15 millions de téléchargements sur 83 millions de citoyens, ce qui donne donc un taux d'adoption d'à peu près 16 %. Est-ce que vous jugez que c'est un taux satisfaisant, ça, 16 % d'utilisation?

M. Debbabi (Mourad) : Je pense qu'une population de 15 millions... Je ne regarde pas le droit acquis à la population, mais 15 millions, c'est quand même... c'est beaucoup, c'est vraiment beaucoup. 15 millions de population, c'est beaucoup.

M. Nadeau-Dubois : ...c'est parce que vous comprendrez que les 15 millions, dépendamment de la grosseur de l'échantillon et surtout de la grandeur du territoire, là, 15 millions de personnes, ça ne veut rien dire en soi. L'important, c'est la probabilité qu'ont ces 15 millions de personnes là de se rencontrer et de s'échanger de l'information via l'application. Mais 15 millions de personnes qui l'ont téléchargée, si on ne nous dit pas c'est sur combien de gens et sur quel territoire, ça ne veut strictement rien dire.

M. Debbabi (Mourad) : Selon moi, quand on parle d'une population de 15 millions, c'est un segment qui est très significatif.

M. Nadeau-Dubois : M. Debbabi, 15 millions sur combien?

M. Debbabi (Mourad) : Et il faut comprendre...

M. Nadeau-Dubois : C'est parce que, si je vous dis : Il y a 15 millions de personnes en Amérique du Nord, allez-vous être satisfait?

M. Debbabi (Mourad) : On parle d'un pays, on ne parle pas d'un continent, pour commencer. Deuxièmement, parmi les 80 millions dont vous parlez, il y en a certains, par exemple, qui n'ont pas de téléphone, il y en a certains qui...

M. Nadeau-Dubois : Est-ce que vous avez ces informations-là cet après-midi avec nous?

M. Debbabi (Mourad) : Pardon?

• (14 h 40) •

M. Nadeau-Dubois : Vous me présentez un argument. Avez-vous les statistiques pour appuyer cet argument?

M. Debbabi (Mourad) : Non. La seule information sur laquelle je me base pour faire cette affirmation, c'est que 15 millions ou dès que ça atteint l'ordre des millions, pour moi, c'est un ordre qui est significatif.

M. Nadeau-Dubois : Des statisticiens sont venus nous expliquer que ce qui est important, ce n'est pas la quantité de gens qui l'ont, c'est la probabilité statistique que deux personnes qui l'ont se rencontrent, puisque c'est la condition pour que l'application fonctionne, et que les clés d'identification soient échangées via le protocole Bluetooth. Là, vous soutenez, devant nous, cet après-midi, qu'en fait ce n'est pas cette proportion-là qui est pertinente, seulement la quantité de gens qui l'ont téléchargée. Est-ce que je vous comprends bien?

M. Debbabi (Mourad) : Ce que je suis en train de dire...

M. Nadeau-Dubois : ...qu'il y a des millions que c'est un haut taux d'adoption. 15 millions de personnes en Chine, par exemple, ce serait marginal.

M. Debbabi (Mourad) : Premièrement, les 15 millions, ce n'est pas en Chine, les 15 millions, c'est en Allemagne, c'est par rapport à 80 millions, et 16 %, 16 % de la population, pour moi, ce n'est pas négligeable. Ça, c'est un. Deux, on n'a jamais dit que cette solution-là, c'est la seule solution qui va permettre de combattre contre la pandémie, mais tout effort, tout effort...

M. Nadeau-Dubois : Et ce n'est pas ce que je soutiens non plus.

Le Président (M. Bachand) : Le temps est écoulé, désolé. M. le député de René-Lévesque, vous avez la parole. Merci beaucoup. Vous avez la parole, M. le député.

M. Ouellet : Oui, j'attendais d'apparaître. Oui, merci beaucoup, M. le Président. Donc, à mon tour de pouvoir vous questionner... Ça va-tu? Oui, je suis là? O.K., parfait. Merci.

On a entendu plusieurs experts venir nous parler de cette technologie-là, mais ils nous ont fait référence, aussi, dans la différence entre avoir téléchargé l'application et utiliser l'application. Est-ce que, dans les chiffres que vous avancez, vous avez ces informations-là pour le Canada ou du moins ailleurs, dans vos références, à savoir qu'il existe une différence entre : Je l'ai téléchargée, mais aussi : Je l'utilise, donc je la mets en application, je l'active? Est-ce que, ça, vous avez de l'information à ce sujet-là?

M. Debbabi (Mourad) : Je n'ai pas d'information à ce sujet.

M. Ouellet : O.K. Est-ce que vous êtes d'accord avec moi qu'il existe une différence entre le fait de l'avoir téléchargée et le fait de l'avoir téléchargée et mise en fonction?

M. Debbabi (Mourad) : Certainement.

M. Ouellet : O.K. Donc, lorsqu'on affirme qu'un chiffre nominal de tant de personnes qui l'utilisent... ou qui l'ont téléchargée, pardon, on peut comprendre que ce chiffre-là va peut-être être plus bas si les gens qui l'ont téléchargée ne l'ont pas mise en application, parce que c'est ça qu'on cherche à savoir au...

M. Debbabi (Mourad) : Ça, c'est une trivialité, que les gens qui utilisent, c'est un sous-ensemble des gens qui ont téléchargé, c'est une information qui est triviale. Mais la question que je pose, comme j'ai dit tout à l'heure : Quelle est l'alternative? Aujourd'hui, par exemple, sur vos ordinateurs que vous utilisez chez vous et que vous êtes en train d'utiliser, par exemple un laptop, à cet instant-là, il y a des antivirus. Quel est le pourcentage des attaques des virus qu'on intercepte avec ces outils-là? Peut-être 40 %, ce n'est pas 100 %. Il y a plein d'attaques que vous n'allez pas... que votre antivirus ne va pas être efficace. Je dirais, c'est la même chose pour cette application. Cette application-là ne réglerait pas tous les problèmes de la planète. Cette application-là, c'est un effort pour combattre la pandémie. Donc, on peut la rejeter, mais quelle est l'alternative? On va au manuel?

M. Ouellet : On est en train de se poser la question, quelles pourraient être les alternatives, mais on se pose la question aussi sur l'efficacité de telle application et qu'on n'est pas en train, avec cette application, de donner à nos citoyens, citoyennes un faux sentiment de sécurité, puisque, dans certains cas, ce genre d'application là pourrait donner de faux contacts positifs ou pourrait alarmer, dans certains cas, des gens qui auraient été en contact avec des personnes, mais ces deux personnes-là portaient un masque ou ces deux personnes-là se trouvaient à l'intérieur d'une pièce, séparées par un mur. Donc, ce n'est pas parfait, et donc on veut juste s'assurer que, si le gouvernement va de l'avant avec ça, les informations qui sont divulguées sont pertinentes, crédibles et justes, et la personne qui la reçoit va se gouverner en ce sens.

Dernière question, très rapidement. Certains spécialistes nous ont dit : Avant d'aller de l'avant, au Québec, on devrait la tester sur notre territoire. Êtes-vous d'accord qu'on devrait tester avant de déployer ça sur le territoire du Québec?

M. Debbabi (Mourad) : Et qu'est-ce que ça veut dire, tester?

M. Ouellet : Avant d'y aller de façon générale, on devrait procéder à des tests et voir si, effectivement, il y a des risques qu'on devrait colliger avant de mettre son application de façon unilatérale au Québec.

M. Debbabi (Mourad) : Je ne sais pas. Ça, c'est un choix, je pense, que les autorités auront à faire. Moi, honnêtement, de mon point de vue, c'est un effort qui peut contribuer à lutter contre la pandémie, qui n'est pas parfait. Mais, si on attend d'avoir de la perfection, la perfection n'existe pas chez les humains, n'existe pas dans les choses que l'humain fabrique. Il n'y a aucune voiture qui est parfaite, il n'y a aucune chose qu'on fait qui est parfaite. Je pense, c'est quelque chose qui est sécuritaire. Il y a beaucoup, beaucoup, beaucoup d'experts qui ont regardé ça de très près, et ce n'est pas des amateurs, c'est des professionnels du métier, et qui disent que c'est sécuritaire. Donc, il

y a des évaluations qui ont été faites. Je pense que personne dans cette salle-là ne peut affirmer que cette application ne contribue pas à la lutte contre la pandémie. On peut parler de l'efficacité jusqu'à quel degré, mais on ne peut pas dire qu'elle ne contribue pas.

Le Président (M. Bachand) : ...Chomedey, s'il vous plaît, vous avez la parole. S'il vous plaît, M. le député, allez-y.

M. Ouellette : Merci, M. le Président. Bonjour. Merci d'être avec nous autres. J'ai juste trois petites questions pour vous. Dans un premier temps, avez-vous participé à l'élaboration de la consultation en ligne du Conseil du trésor?

M. Debbabi (Mourad) : Non. Consultation sur quoi?

M. Ouellette : On est en consultations, là, et il y avait un document, il y a eu une consultation en ligne pour les citoyens, cet été, et qui a terminé au mois d'août, et qu'on semble dire qu'il y a 17 000 citoyens qui ont répondu. Il y en a 12 000 qui seraient d'accord pour l'application. Je vous demande si votre comité ou vous avez participé.

M. Debbabi (Mourad) : Moi, non. Personnellement, non.

M. Ouellette : O.K. Votre dernière rencontre avec M. le ministre Caire remonte à quand?

M. Debbabi (Mourad) : À quelques mois.

M. Ouellette : O.K. Est-ce que vous avez participé à la mise en place du logiciel fédéral Alerte COVID?

M. Debbabi (Mourad) : Non.

M. Ouellette : Et ma dernière question, le taux d'adoption ou le taux d'adhésion au Québec... Parce que vous semblez attacher beaucoup d'importance à des millions. On a parlé de l'Allemagne, on a parlé... en France, hier, on nous a dit que c'est 1,8 million sur 65 millions de population. Au Québec, le taux d'adoption, pour vous, pourrait ressembler à quoi?

M. Debbabi (Mourad) : Je n'ai pas de statistiques à cet égard, mais j'espère qu'elle va être adoptée par une grande partie de la population.

M. Ouellette : O.K. Parce que je ne vous apprendrai pas que la moitié de la population est dans la région métropolitaine.

M. Debbabi (Mourad) : Notamment, à Montréal, par exemple, la région de Montréal, ça serait bien que les gens l'utilisent. Je pense que ça peut contribuer à lutter contre cette pandémie.

M. Ouellette : O.K. Merci.

Le Président (M. Bachand) : Alors, merci, Dr Debbabi, de votre participation. Puis merci à l'équipe technique de l'Assemblée nationale qui, à la dernière heure, a pu mettre en place cette visioconférence, même s'il y a eu un petit bogue. Merci beaucoup à toute l'équipe. Merci beaucoup, au plaisir.

Alors, je suspends les travaux quelques instants. Merci.

(Suspension de la séance à 14 h 47)

(Reprise à 14 h 50)

Le Président (M. Bachand) : À l'ordre, s'il vous plaît! Merci. La commission reprend ses travaux.

Alors, il nous fait plaisir de souhaiter la bienvenue à M. André Mondoux, professeur titulaire à l'École des médias à l'Université du Québec à Montréal et directeur du Groupe de recherche sur la surveillance et l'information au quotidien.

Alors, vous avez 10 minutes puis, qui sait, peut-être plus, on ne sait pas... bien, 10 minutes de présentation, puis on verra avec la période d'échange. Bienvenue, M. Mondoux.

M. André Mondoux

M. Mondoux (André) : Merci, M. le Président. Membres de la commission, merci de m'avoir invité. Je vais dévaler une colline parlementaire, hein, mais... parce que j'ai juste 12 minutes, alors je vais prendre tout le temps.

Rapidement, je suis sociologue et professeur à l'École des médias depuis 2009. Sociologue, pour ceux qui ne s'en souviennent pas, c'est «société». Je sais que ça fait longtemps qu'on n'entend plus parler de société, de système

puis de tout ça, mais nous existons encore. Auparavant, j'ai été 20 ans journaliste en technologies. Donc, depuis les années 84, je peux dire que je navigue dans les technologies numériques. Donc, je peux dire que j'ai gagné ma vie et, rétrospectivement, l'avoir perdue un petit peu aussi avec ces technologies-là.

Je ne suis ni technophobe ni technophile. Si on avait à choisir, peut-être que je serais peut-être un peu technophile : le rapport d'ordinateurs par habitant à la maison est beaucoup trop élevé. D'une part, j'ai des rapports ambivalents avec la technique depuis le début. Dans les années 80, si vous vous souvenez — les plus jeunes, vous demanderez à vos parents — c'était la bureautique puis le traitement de texte, puis je me rappelle, à l'époque, il y avait des manuels écrits par des ingénieurs en informatique qui allaient expliquer comment faire le travail de bureau. Imaginez que ce n'était pas du tout adapté. Et c'est comme ça qu'à l'époque je commençais à écrire des livres de formation qui étaient plus adaptés à la réalité humaine. 40 ans plus tard, il y a de nouveaux manuels qui sortent puis, cette fois-ci, c'est pour le vivre-ensemble au complet. Alors, voilà qui me semble, sinon inquiétant, à tout le moins, de regarder l'héritage qui a été fait.

D'une part, ce n'est pas étonnant que, maintenant, le vivre-ensemble, la première ligne de front, c'est la santé. Alors, on va vraiment s'attaquer à la santé et à l'éducation. À la santé, maintenant, bien, c'est rendu, on l'a vu au cours des deux derniers jours, désormais tout ce qui est santé publique doit composer avec le génie informatique, il n'y a aucune formation en santé populationnelle ni en santé publique. Alors, c'est pour vous dire à quel point qu'on est rendus vraiment techniques dans nos discussions.

Et d'ailleurs, je le répète, pandémie : «pan», au complet, «démie», «demos», le peuple, ça affecte tout le peuple. Alors, n'importe quelle solution qui sera pandémique va également être pan-démique, et en ce sens, il faut faire attention, justement, comment est-ce qu'on conceptualise ça. C'est une dynamique de totalisation. Et, vous me permettez cette petite flèche, je pense que ça mérite plus que quelques réunions en quelques semaines d'intervalle durant l'été pour avoir le temps de faire des rapports. Vraiment, c'est une question qui, à mon sens, est très importante.

Donc, ce qu'il faut faire attention, c'est tous les enjeux qui vont, justement, avec le déploiement de la technique dans toutes nos vies, et c'est pour ça qu'il faut regarder... Parce qu'on parle de pandémie collective, mais, si vous regardez, depuis deux jours, tout ce qu'on parle, c'est de la technique et de l'individu, protéger les données personnelles, la vie privée, et il y a très peu... pour ne dire aucune discussion générale sur quel genre de vivre-ensemble on veut et... par l'utilisation de ces outils-là. Et ça, c'est des questions qui m'apparaissent fondamentales et qui ne sont malheureusement pas abordées.

Donc, qu'est-ce que ça veut dire, d'aborder d'un point de vue global? D'une part, aucun outil n'est isolé. Je ne vous apprend rien, n'importe quel outil s'inscrit dans un réseau des vastes ensembles de techniques, de pratiques et de ressources, que ce soit l'ordinateur, la montre, l'Internet, etc., et cette circulation... Les données, d'ailleurs, ne sont jamais toutes seules, elles circulent déjà de façon marchande. Alors, il est un peu difficile d'avoir une discussion sur la vie privée COVID-19, mais, par exemple, sur mon Facebook, mon Twitter, tout ça... Vous lirez, si vous voulez, les 2 823 pages de consentement, mais vous allez voir que vous abandonnez tous vos droits aux données. Alors, si on veut réglementer la vie personnelle, la protection des données personnelles, il ne faut pas se confiner — excusez le mauvais jeu de mots — au COVID-19, il faudrait élargir la discussion et la réflexion au vivre-ensemble lui-même.

Deuxième chose, c'est la quasi-autonomie de la technique, si vous remarquez. J'écoutais hier, lorsqu'on demandait sur l'application fédérale : Bien, qui c'est qui est responsable de ça?, ah! bien, c'est des volontaires, c'est Shopify. Ah bon? Mais qui c'est qui est responsable de ça? Personne. Pas d'imputabilité, parce que, sous-entendu : Ah! la technique est neutre, et puis c'est juste une question d'opérationnalité. D'ailleurs, le terme qu'on utilise pour ces outils-là est révélateur, des «applications». On l'a vu avec le commentaire précédent, on part avec «c'est déjà déployé», puis ensuite on va justifier parce que c'est fait en fonction de ça. D'ailleurs, à l'époque, dans les années 80-90, on parlait de solutions, des solutions informatiques, au point qu'aujourd'hui on parle de solutionnisme, c'est-à-dire qu'on va créer des problèmes pour avoir les outils pour les régler.

L'autre question qui est importante et qui touche un peu l'économie politique, on l'a vu : À qui vont aller les données? Vous voulez bien le donner aux GAFAM. Mais, bon, je vais faire un scénario de science-fiction, imaginons un président des États-Unis un peu excentrique, des services de renseignements qui voudraient fouiller, imaginons une pandémie — tiens donc! — et puis finalement les serveurs chez Amazon foutent le camp. Et puis qu'est-ce qui se passe avec ça? Certains vont dire : On devrait avoir un OSBL, mais ça reste quand même une forme de privatisation de données collectives. Et ça, il faudrait réfléchir à ça, ce sont des données qui appartiennent aux Québécoises et aux Québécois.

L'autre chose, il faudrait faire attention de ne pas donner ces outils-là à tout ce qui bouffe des données. Tout ce qui est intelligence artificielle, Spotify, ça exige des quantités massives de données. Alors, évidemment, s'ils sont collés sur une application de COVID qui récolte des données, vous les mettez dans le... ces institutions-là... ces compagnies-là, pardon, ces entreprises-là, dans la position très inconfortable qu'est Facebook en ce moment : un modèle d'affaires qui est sur la production, la circulation des données, puis en même temps on va assumer la responsabilité de ne pas faire circuler les données. Écoutez, on peut bien essayer de faire coucher le loup dans la bergerie, mais je gage que le mouton ne devrait pas fermer l'oeil de la nuit. Il faudrait faire attention, justement, là-dessus.

Quelles sont ces valeurs, justement, techniciennes? On le voit dans les discussions, ici, on parle de performance, d'efficacité, de pragmatisme, d'opérationnalité, ce qui est certes nécessaire, j'en conviens, mais certainement pas, non, suffisant, hein, parce que, d'une part, face à l'érosion de ce qu'on pourrait appeler des grandes valeurs collectives — «libarté», oserais-je dire — bien, arrive la technique qui se présente comme quelque chose de neutre. Et remarquez le vocabulaire qui est associé : «optimisation», «pragmatisme», «statistiques», «ratios». Bref, les moyens sont devenus les fins, et ça, c'est un problème qui est plus gros que la pandémie et qui est vraiment... Et je ne suis

pas tout seul, hein, dans le monde, plusieurs philosophes et penseurs se demandent la question sur est-ce qu'on ne s'en va pas vers une espèce de cul-de-sac technique, justement, d'une société qui serait trop technicienne au point de ne pas être capable de redoubler la technique pour l'adapter, justement, un peu comme les manuels de traitement de texte dans les années 80.

Cette machinisation du social, on le voit, d'ailleurs, et, même ici, on parle de gouvernance, on ne parle plus d'idées, de politiques, de vision. Non, la gouvernance, c'est l'application des règles neutres, et ça se trouve à engager un phénomène de dépolitisation. On est juste des gestionnaires d'opérations et on prend les décisions là-dessus, et, quand arrivent des finalités ou de parler de finalités, un peu comme je le fais en ce moment, on est sous l'impression d'être un chien dans un jeu de quilles : Ah! ce n'est pas la place pour parler de ça, ou etc.

Centralisation des données, bien, j'en ai parlé, il faut faire attention. Puis il y a aussi le fait : Qu'est-ce qui se passe lorsqu'on délègue nos données ou les médiations aux algorithmes? Premièrement, ça augmente la quantité d'infos : Ah! j'ai besoin d'un logiciel pour le traiter. Ça augmente la vélocité, on parle désormais d'accélération sociale et de temps réel. Je vous mets au défi de vider votre boîte de courriels une journée par semaine. Vous savez, on n'ira pas là-dedans, mais on le voit qu'on est de plus en plus dans une dynamique de temps réel, de rapidité.

Et qu'est-ce qui se passe, lorsqu'on applique la technique, justement, machinique? Parce qu'il y a plusieurs sortes de techniques. Celle qu'on parle ici, c'est la technique cybernétique, ça reproduit au même, hein : homéostasie, «homeos», même, «stasis», ma place. Ça fait que c'est pour ça, d'ailleurs, que c'est une base industrielle. Reproduire au même, c'est une industrie. Alors, appliquez ça sur Facebook, par exemple, bien, le concept d'amitié, hein, je rappelle, à l'époque, un symbole de l'amitié, c'était un morceau que je brisais en deux, le «symbolon», pour marquer que j'étais en amitié avec quelqu'un, que je suis accompli avec l'autre. Maintenant, sur Facebook, c'est un compteur, et ce compteur-là n'a qu'une seule direction : plus, plus, plus. Et c'est ça, ce que certains disaient, la technique moderne, lorsqu'elle n'est pas enchâssée, elle s'emballe. On met un outil pour mesurer, bien, l'outil va aller le plus haut possible, le plus loin possible et de façon autonome. Alors, je l'ai vu avec mes enfants, 600, 700 amis. Mon Dieu! Moi, si j'en avais 20, je me comptais chanceux. Et aujourd'hui on a des quantités industrielles. Évidemment, ce qui se sous-tend là-dessus, c'est plus d'amis, plus de données vues, plus de publicités, plus de données personnelles qui... Et voilà, on est rendus dans le modèle du GAFAM, du modèle d'affaires d'une économie qui se déploie sur le traitement, la production, la circulation et la consommation de données.

Autre caractéristique, donc, du numérique, c'est donc...

Le Président (M. Bachand) : Peut-être en conclusion, s'il vous plaît. Peut-être en conclusion.
• (15 heures) •

M. Mondoux (André) : Oui, j'y arrive. Je suis à la page 5 de mes 12, tout va bien.

Une des choses qu'on a remarquées, nous, en laboratoire, c'est les notifications. On a des applications qui sont capables de mesurer le temps ou la notification, puis on y va, hein? On a parlé d'input, output puis de boîte noire tantôt, là, il y a un nom pour ça, ça s'appelle du behaviorisme cybernétique, c'est du contrôle de comportement : la montre dit «rouge, arrête», elle dit «verte, tu y vas», «10 000 pas, calories, stop», sans se questionner, on fait confiance. Alors, ça, ça crée, encore une fois, des individus... Et plusieurs chercheurs parlent d'économie de la pulsion, temps réel, je veux avoir tout, ici, maintenant, et ce que ça donne, bien, ce n'est pas un citoyen qui a le temps de réfléchir, de prendre de la distanciation, on est justement happés.

Donc, en conclusion, M. le Président, il y a une dynamique de totalisation, qu'elle soit par la pandémie, qu'elle soit par une tendance que je dirais quasi naturelle à la technique. Joindre à ça... Regardez ce qui se passe un peu partout, aux États-Unis, en Europe, il y a une montée d'une droite que je dirais décomplexée, peut-être même extrême, dans ses moments les plus inclusifs, et ceci, dans le contexte pandémique et le déploiement d'applications biométriques, je pense que ça mérite pleinement notre souci. Merci beaucoup.

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

M. Lévesque (Chapleau) : Merci, M. le Président. Merci, Pr Mondoux. On sent la passion, on reconnaît le sociologue. Merci de votre présentation.

M. Mondoux (André) : ...j'espère.

M. Lévesque (Chapleau) : Bien, oui, j'imagine, on l'entend cet après-midi. Juste peut-être un petit rappel, là, quelques points, là, qui avaient été énoncés par le gouvernement. J'imagine que vous en avez pris connaissance également, là. Si jamais le gouvernement décidait d'aller de l'avant avec une application, il n'y aurait pas, évidemment, de géolocalisation, pas de recours à la biométrie, donc reconnaissance faciale, pas de stockage de données, dans le fond, maximiser la protection de la vie privée puis maximiser également, là, dans le fond, la protection des renseignements personnels pour les personnes, pour la population du Québec. Évidemment, ça devient... C'est églement volontaire, là, cette application-là, donc il n'y aurait pas d'obligation par rapport à ça.

Mais je serais quand même curieux... Vous opposez santé publique et technologie, du moins philosophiquement. Je serais peut-être curieux de voir comment, pourquoi, qu'est-ce qui vous a amené là dans votre cheminement, dans votre réflexion.

M. Mondoux (André) : Écoutez, depuis quand, historiquement, tout d'un coup, que le génie informatique et les statistiques deviennent des intervenants incontournables en santé? Ça, c'est un phénomène assez récent. Ça a

commencé avec la méthode Toyota, la méthode Bolduc. Ça a commencé par mesurer combien de cuillerées de patates on va mettre, de rationaliser, et on a vu aussi, malheureusement, les résultats que ça a pu donner, hein, c'est-à-dire de se fier, justement, à une espèce de gestion technique et sans mettre de l'humain dans la machine, et c'est là qu'est le bogue. C'est-à-dire que, si vous laissez l'entière de la machine, l'algorithme de regarder la production, la circulation et la consommation, elle va faire une boucle totalisante en soi et pour soi, et ça, il y a de nombreux exemples, j'en ai donné quelques-uns, mais on pourrait passer la journée à en jaser.

M. Lévesque (Chapleau) : On est d'accord, là, pour le manque d'humanisme en santé par le passé, là, ça, tout à fait, on est sur la même ligne. Vous parlez également, là, d'un outil non isolé, non pris dans le groupe. Est-ce que, justement, un outil qui serait... qui ferait partie d'un ensemble d'autres éléments en santé publique pourrait être pertinent et non pas juste comme la valorisation du technique ou du technologique, et donc comme un outil, comme un instrument, donc, qui vient en appui, mais donc l'humain reste quand même en contrôle, l'humanisme est encore là?

M. Mondoux (André) : Je vous dirais, M. Lévesque, que c'est déjà fait. Je veux dire, votre outil travaille avec l'Internet, travaille sur l'ordinateur, travaille avec le monde, vous ne pourrez pas l'isoler, d'où pourquoi... En fait, je suis moins venu ici pour vous dire des solutions, je ne suis pas un ingénieur, mais la même façon qu'on me reproche de ne pas me mêler de l'informatique, je vais peut-être avoir une petite gêne de laisser les informaticiens parler de social, par exemple. Et, je le remarque, les premiers ont beaucoup de parole, en ce moment, et pas les seconds, il faudrait ramener ça pour rééquilibrer.

Je ne suis pas technophobe, comme je vous dis, j'ai bien de la techno à la maison, mais il faut faire attention, parce que... ne pas penser l'outil isolé, il s'inscrit dans des dispositifs toujours plus grands, et ça englobe l'ensemble du vivre-ensemble. Et, ce faisant, et là je vous reparle de la question, est-ce qu'on va viser le vivre-ensemble seulement en travaillant sur les points individuels ou si on devrait aussi l'aborder par le haut? Bien, tout dépend de la philosophie, j'imagine, de politiques que vous adoptez, mais moi, je serais de ceux qui disent, bien, que l'individu produit une société à produire un individu à produire une société.

M. Lévesque (Chapleau) : D'ailleurs, sur le vivre-ensemble, c'est là où j'allais, vous m'amenez à ma prochaine question. Est-ce que, justement — puis là on va y aller dans le très pointu, du moins dans le pratico-pratique — le fait, justement, de vivre ensemble et d'avoir l'opportunité d'être notifié qu'il y a une possibilité qu'on ait été en contact avec quelqu'un qui avait la COVID-19... est-ce que, justement, ça, ça ne pourrait pas aussi faire partie du vivre-ensemble? Dire : Regardez, wow! par souci de ma société, par souci des autres êtres humains, je vais, moi, m'isoler parce qu'il y a peut-être un risque ou je vais aller faire le test parce qu'il y a peut-être un risque, est-ce que ça aussi, ça fait partie du vivre-ensemble?

M. Mondoux (André) : Oui, ce qui devrait aller plus loin, c'est-à-dire de dire : Cet outil-là, est-ce que je vais en parler seulement en termes individuels, en termes de projet individuel, en termes d'intérêt économique ou si je vais regarder ses impacts? Parce que, là, si vous partez, justement, de l'outil et vous ne décollez pas de l'outil, bien, on est au même point. Alors, moi, ce que je dis, c'est qu'il faut penser beaucoup plus large, quels sont les impacts sociaux et sociétaux. On en a parlé un petit peu avant-hier, l'accès, les inégalités, etc., mais... puis aussi le partage des informations, ça, c'est le gros point.

Vous amenez ça aux États-Unis, il va y avoir des problèmes, là. Je veux dire, le gouvernement américain, il se donne les droits quand c'est... la sécurité nationale, il... puis il va aller chercher les infos. Puis de donner ça à un OSBL, ça reste encore une forme de privatisation. Puis de le donner à des gens qui ont intérêt à ramasser des données pour faire leur modèle d'affaires, ça ne nous avance pas.

M. Lévesque (Chapleau) : ...pas de collecte de données, là, ni de...

M. Mondoux (André) : Pardon?

M. Lévesque (Chapleau) : On ne voudrait pas... Il n'y a pas de collecte de données ni de recueillement de ces choses-là.

M. Mondoux (André) : Bien, il y aura des collectes de données, au gouvernement. Ce que je dis, c'est que le stockage, la manipulation, le contrôle devraient être vus d'une ressource publique, et ça devrait appartenir aux Québécoises et aux Québécois, et de rester ici, sur le territoire. Et puis, si on y va lentement, tant mieux pour nous. Et ça pourrait aussi servir... Écoutez, on ne partira pas, mais l'«open source», les données ouvertes... On en a, des ressources, au Québec, on en forme beaucoup à l'UQAM, justement, en médias numériques pour adresser ces enjeux-là et pour avoir des intervenants qui sont capables de dire : Aïe! On va mettre du social dans la game parce que c'est important, et il y a des enjeux de surveillance, d'intégrité, et que ce n'est pas juste une question d'applications, de déploiement, de ratios puis de statistiques, ça s'inscrit dans des rapports économiques, politiques et sociaux.

M. Lévesque (Chapleau) : Je comprends votre point. Merci beaucoup. Merci, M. le Président, c'est tout pour moi.

M. Mondoux (André) : Je vous en prie.

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

Mme Boutin : Pr Mondoux, vraiment, c'est extrêmement intéressant, là. Moi, je m'inscrirais tout de suite à votre cours. Moi, dans le passé, dans mes études, j'ai fait un petit peu de... je regardais beaucoup le rapport de la sociologie de la population avec la technologie.

M. Mondoux (André) : ...à l'automne.

Mme Boutin : J'aimerais vraiment ça pour vrai, là, c'est quelque chose... je m'intéresse beaucoup à la technologie puis je pense qu'on est peut-être dus, au Québec, avoir une réflexion. Je ne sais pas si c'est le gouvernement qu'il faut qu'il ait cette réflexion-là, parce que, tu sais, le gouvernement n'est pas... on ne s'occupe pas de tout non plus, là, mais avoir une réflexion sur ça, avoir aussi plus de littératie numérique, aussi, au sein de la population, parce que ce n'est pas... on n'est pas dans le veau d'or du temps moderne, là, avec la technologie, on s'entend, mais je me pose quand même cette question. Tu sais, il faut garder un esprit critique par rapport à la technologie.

Selon vous — parce que je suis aussi technophile, mais j'ai un esprit critique puis je me questionne beaucoup — est-ce que la technologie a quand même un rôle à jouer, peut-être, comme un outil, sans être un outil central, en santé publique, que ce soit cette application-là, là, ou d'autres outils technologiques, tu sais? Votre opinion là-dessus, première question. Puis, deuxièmement, quel rôle pourrait jouer le gouvernement pour peut-être mieux encadrer, justement, l'utilisation de technologies pour soutenir la santé publique?

M. Mondoux (André) : De un, il y a une nuance importante à faire. Nous sommes homo faber, hein? Il y a une différence entre le squelette du dernier hominien puis du dernier grand singe, c'est que le deuxième, il a un silex dans la main, alors on est techniques par nature.

Là, le danger, comme disait le fameux philosophe, c'est de confondre notre destin avec celui de la technique, hein? Le compteur d'amis sur Facebook, là, il ne dit pas : Tu en as quatre, c'est le fun, non, non, 200, 300, 400, et ça devient, à un moment donné, le pouvoir du pouvoir. Et on entend des choses comme : Bien, si ça peut être déployé, on va le faire parce que c'est normal, et c'est ça qui est dangereux. C'est parce qu'on a besoin de la technique, mais il ne faut pas qu'on devienne des outils, nous autres, à la technique. Et, quand vous déployez... D'ailleurs, regardez comment est-ce qu'on définit la population à coups de machinisme, ça devient homogène, plate, statistique. Et d'ailleurs on parle maintenant de population au sens biologique, hein, il n'y a plus de disparités, et ça, ça fait... D'ailleurs, mes collègues... on commence des réflexions sur est-ce qu'il y a une forme de biopouvoir. Parce que, quand vous êtes rendus avec des montres biométriques, des téléphones qui mesurent vos... D'ailleurs, vous le savez, à l'université... la mal nommée Oral Roberts, ils ont donné des montres pour voir l'abstinence à des jeunes ados. Il fallait être optimiste. Et puis ils ont réalisé que... On va leur donner des montres puis ils vont faire de l'entraînement. Ils ont réalisé qu'après avoir eu des relations très intimes, le cœur montait, ça fait que les montres enregistraient à chaque fois qu'il y avait des gens qui faisaient l'amour. Donc, vous voyez, il y a toujours des effets pervers, ce qui nous renvoie au fait que non seulement on n'a pas la discussion qu'on devrait avoir, mais on est en train de dire : Aïe! On peut-tu au moins juste tester avant de déployer? Aïe! On est deux, trois marches, là, en deçà où on devrait être.

Votre deuxième question : Qu'est-ce que peut faire le gouvernement? Bien, c'est l'instance démocratique que nous avons, et là on pourrait avoir... il faudrait chapeauter tout ça, je ne sais pas, c'est le grand rêve d'un ministère du Numérique. Mais, comme c'est des technologies qui sont totalisantes et peut-être même totalitaires, bien, j'aimerais mieux les voir entre les mains du gouvernement qu'entre les mains opaques du privé, où il n'y pas d'imputabilité, quoi que ce soit.

• (15 h 10) •

Mme Boutin : Peut-être qu'on pourrait — puis là c'est vraiment moi qui fais une suggestion, là, je ne sais même pas si c'est le cadre pour l'avoir, mais j'aime beaucoup la conversation — peut-être qu'on pourrait intégrer plus de sociologues comme vous dans des comités d'experts, tu sais, et ne pas seulement avoir des gens qui sont des techniciens et des experts en sécurité, mais avoir des gens qui ont un regard différent sur la société puis de mieux définir le rapport avec la technologie. Parce que moi, je me pose la question, comment est-ce que, dans ce contexte-là... Là, ça va en accélérant, là, la technologie, c'est exponentiel, ça va vite, puis, tu sais, on ne vit plus en 1950, on est en 2020, puis c'est très dur parce que c'est mondial. Comment est-ce que nous, on peut conserver notre humanité là-dedans?

M. Mondoux (André) : C'est la grande question qui insuffle... D'ailleurs, on a perdu un grand joueur, Bernard Stiegler, la semaine dernière, grand penseur et collègue à moi de... sur la technique, justement, pour ramener cette espèce d'équilibre. Et il sera probablement toujours instable, mais, vous savez, quand on modélise à coups de statistiques... Je peux prendre un dé, j'ai une chance sur six de rouler un dé. Si je roule six fois, ça ne veut pas dire que je vais avoir un six, si je le roule 6 milliards de fois, ça va. Le problème avec la modélisation statistique, c'est qu'on ne vit pas à 6 milliards de lancées, on en a un à la fois, et c'est toute la différence. Parce que, quand vous avez une idéologie, une vision du monde, d'un social qui, ultimement, se fait régler par un seul algorithme qui pourrait même prévoir ce qui va arriver, bien, Houston, on a un problème, là, je veux dire, plus besoin de démocratie ou d'élections, plus besoin de rien, c'est juste des certitudes. Puis là on est rendu dans... voilà, on est rendu des «dividus», comme dans la notion de... bien, une masse populationnelle, puis c'est juste du pourcentage.

Un autre exemple, madame, aux États-Unis, on a dit : Ah! les données interceptées par la NSA, ce n'est bien pas grave, c'est juste des métadonnées. Mais c'est décourageant, ça veut dire que ce qu'on a à dire ne compte même pas. Juste avec les métadonnées et les croisements, ils sont capables d'aller chercher des formes de régulations. Puis le problème, c'est que, maintenant, quand on a des régulations sous forme de contrôle, ça ne va très bien avec la vie démocratique. À un moment donné, il y a... il faut faire attention, ça prend le premier puis ça prend aussi le second. Alors, ce n'est pas une question d'arriver avec des gros sabots, mais ça demande de la nuance, et je ne pense pas que seuls mes collègues en informatique peuvent apporter cette nuance-là, ça prend une discussion «at large» entre plusieurs champs disciplinaires.

Mme Boutin : O.K. C'est vraiment intéressant. Donc, le gouvernement, dans le fond — et même j'irais plus au-delà du gouvernement, de l'Assemblée nationale et de l'ensemble des élus qu'il représente, des citoyens — devrait peut-être y avoir un rôle, éventuellement, pour, justement, avoir... garder à l'œil... avoir un esprit critique par rapport à ça, par rapport à la technologie, par rapport à toute cette évolution-là?

M. Mondoux (André) : Écoutez, dans les modèles universitaires scientifiques, ça passe par des observations, des expériences. Nous, on en fait sur la circulation marchande, on essaie aussi de former des nouvelles générations de spécialistes. D'ailleurs, on a une réforme où on veut rentrer l'intelligence artificielle, pas pour s'opposer, pour être capables d'avoir une interface commune et de dire : Attention, là il y a un danger pour la surveillance, là il y a un danger pour ceci, et de faire ça de façon plus harmonieuse ou organique, pourrais-je dire.

Mme Boutin : Je partage votre avis, vraiment. Puis, dans le fond, tu sais, si on regarde une application, aujourd'hui, en commission, c'est bien intentionné, dans le sens... si le gouvernement considère une application comme ça, c'est, dans le fond... et plusieurs mesures qui ont été mises en place, l'objectif ultime, c'est de sauver des vies humaines, puis on se dit : Bon, quelles sont toutes les mesures qui pourraient être mises en place? Peut-être que la technologie peut aider, peut-être pas, mais c'est pour ça qu'on a ces discussions-là.

M. Mondoux (André) : Tout à fait, et aussi de dire : Bien, il faut déployer, ça va sauver des vies humaines... L'enfer est pavé de bonnes intentions, puis les vœux pieux, c'est 13 à la douzaine. Il faut aller plus loin, puis dire : O.K., et, justement, que la vie humaine, c'est aussi la vie collective.

Et, que voulez-vous, ça fait 50 ans de néoconservatisme qu'on a dans le monde et puis ça a exacerbé l'individualisme, et là, chassez le naturel, il revient au galop. La pan-démie, elle nous interroge toutes et tous, et c'est pour ça que je pense qu'il faut faire un retour sur ces valeurs ancestrales, à l'époque. Évidemment, vous aurez deviné, à la blancheur de mon visage, je suis un enfant des années 70, on est 12 012, 6 006, il faut se parler. Les valeurs collectives étaient très fortes, puis... mais je pense qu'elles sont appelées à revenir et... parce que les enjeux qu'on a sont, en ce moment... touchent là-dessus, et c'est à un moment qui est crucial parce que la tendance pour le contrôle, là, avec les libertariens, les mouvements de droite, et autres, moi, en tout cas, ça me donne quelques frissons, et je me dis : Il faut être vigilants et s'assurer que notre maison est en bon ordre et accueillante.

Mme Boutin : Merci. Est-ce la députée de Les Plaines...

Le Président (M. Bachand) : Oui. Mme la députée de Les Plaines, 1 min 30 s.

Mme Lecours (Les Plaines) : Ah! bien, très rapidement. Bien, en fait, je veux... Merci de nous faire sourire, parce que le sujet est quand même assez sérieux, mais, dans tout votre sérieux, vous nous avez fait sourire. Rapidement, j'aimerais ça que vous me parliez de fracture numérique parce que, on le sait, si on y va avec une application comme ça, il y en a qui n'ont pas de cellulaire, puis on a aussi une portion de la population âgée qui n'en ont pas et en auront probablement jamais. Mais est-ce que ce serait quand même efficient, en considérant qu'on partage aussi au-delà de cette information?

M. Mondoux (André) : C'est le gros enjeu, hein? La pandémie, on voit les chiffres, touche les populations les plus vulnérables, en commençant par les minorités économiquement vulnérables. Mais reportez-vous à, là, 20, 30, 40 ans, où, au temps qu'on avait un truc collectif comme la radiodiffusion, la télédiffusion, ça prenait un permis du gouvernement, promouvoir l'identité canadienne, mais, si vous regardez depuis deux, trois ans : Ah! gros marché national, puis débrouillez-vous, c'est la libre concurrence. Et c'est ça aussi, ça a affaibli le rôle de l'État là-dedans, et on pense que, justement, on va laisser le marché faire. Bon, je ne suis pas un fan du contrôle total du marché, mais je ne suis pas un fan de la main invisible non plus, c'est-à-dire qu'il faut arriver avec des incitatifs pour encadrer, mais, si on laisse ça aller... D'ailleurs, c'est ce qui se passe avec les élections, les médias sociaux, n'importe qui pouvait acheter de la pub puis le faire, puis «let's go». Et on est... D'ailleurs, nos efforts portent là-dessus, là, justement, on va travailler pour les prochaines élections québécoises, s'assurer, justement, qu'il n'y a pas d'interférence dans les... Il y a beaucoup d'enjeux, en ce moment, autour du numérique et qui touchent la démocratie directement. Et c'est un peu ça que je suis venu aujourd'hui... c'est de sonner cette cloche-là pour dire qu'il faut avoir des réflexions sérieuses. Puis la COVID-19, c'est juste la pointe d'un iceberg.

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

Mme Rizqy : Merci beaucoup. Merci. Bonjour et bienvenue parmi nous.

Et j'enchaîne directement avec qu'est-ce que vous venez de terminer, la démocratie, les élections. J'imagine que vous avez regardé ou, peut-être, vous avez pris connaissance de hacks où est-ce qu'on voyait clairement comment que ces entreprises, ces géants du Web pouvaient, grâce, d'abord, aux métadonnées qui... tellement... on parle de métadonnées, c'est tellement loin et abstrait, dans le commun des mortels, mais ça leur a permis quand même à faire du croisement de données pour orienter des élections.

M. Mondoux (André) : Oui, puis il faut être réalistes, hein? Vous savez, la sécurité informatique, je dis toujours, c'est comme l'histoire des deux personnes qui ont marché toute la journée en forêt puis ils sont fatigués, ils enlèvent leurs souliers près d'un ruisseau pour se rafraîchir puis il y a un ours qui sort, qui court après les deux, puis là les deux sautent, puis il y en a un qui est ralenti parce qu'il met son soulier, puis son chum lui dit : Aïe! Tu penses-tu que tu vas courir plus vite que l'ours? Non, mais je vais courir plus vite que toi, par exemple.

Alors, la sécurité, c'est toujours cette espèce de compromis qu'il faut faire. Là-dessus, mon collègue précédent, je lui donne raison là-dessus. La perfection n'existe pas, sauf que, non plus, il ne faut pas arriver avec... plonger dans le vivre-ensemble avec des considérations qui sont juste du génie... de l'ordre du génie informatique. Il n'y a pas de place pour les valeurs, les discussions, la démocratie là-dedans, c'est le déploiement d'un algorithme annoncé. Pour moi, c'est potentiellement catastrophique si ce n'est pas enchâssé et encadré.

Mme Rizqy : J'ai... puis ça, c'est vraiment mon opinion à moi personnelle, et je vais distinguer le gouvernement du Québec versus le gouvernement fédéral, dans les dernières années, je trouve que, lorsqu'on regarde à l'agenda, les rencontres privées entre les GAFAM et les élus fédéraux, c'était pratiquement indécent, on pouvait prendre le calendrier, c'était littéralement un jour sur deux, alors que le commun des mortels, des citoyens qui paient leurs impôts, contrairement à eux, ont peine et misère, des fois, à rejoindre leurs propres élus. Est-ce qu'on s'est éloigné, vraiment, de l'essentiel?

M. Mondoux (André) : Moi, je pense que oui, parce qu'on est pris dans les moyens qui sont incontournables. Je vais vous paraphraser mon frère : Les moyens mènent à tout, à condition qu'on en sorte. C'est un peu ça aussi.

Mme Rizqy : Et ces mêmes géants du Web, qui frappent aux portes du gouvernement fédéral, Google et Apple ont frappé pour l'alerte COVID.

M. Mondoux (André) : Ah oui, et ils vont frapper encore. D'ailleurs, le mot d'ordre, ça va être «no-touch technology». Non, non, là, je vous le dis, ça va être le gros déploiement. Regarde, ça ne touche pas, c'est sans fil, etc. Évidemment, ils sont en train de rechanger le langage, le «pitch marketing», si je peux dire, de persuasion pour s'adapter à la COVID.

Mme Rizqy : Et j'ai l'impression que le gouvernement fédéral, dans l'urgence, toujours sous le prétexte de l'urgence, a confondu «agir» et «s'agiter» en déployant rapidement l'Alerte COVID, sans avoir eu des discussions avec le gouvernement du Québec, malgré, d'ailleurs, des propos tenus par le premier ministre Legault, lorsqu'il a dit : J'ai peut-être des réticences, ça prendrait peut-être une consultation. Est-ce que je me trompe, mais la santé, c'est quand même notre juridiction à nous, et que peut-être qu'on aurait mérité être consultés, et que...

M. Mondoux (André) : Et c'est la première chose que mes collègues en sciences po m'ont dit avant de partir : Depuis quand le fédéral se mêle de santé? Alors, voyez-vous, que... C'est pour ça, comme disait l'autre : La technologie n'est ni bonne ni mauvaise, mais elle n'est surtout pas neutre. Vous vous organisez avec ça puis ça décrit bien. Alors, ça, c'est un des enjeux aussi, parce qu'effectivement, c'est ça que je vous dis, c'est totalisant. C'est très difficile, une fois qu'on met la cravate dans les rouleaux, les souliers vont y passer, si on ne fait pas attention.

• (15 h 20) •

Mme Rizqy : Et ces mêmes personnes qui frappent aux portes des gouvernements, qui ont des discussions derrière les portes closes, bien, évidemment, ce sont des sociétés en droit, là, qui sont, pour nous, étrangères et donc, par conséquent, ne sont pas sous notre juridiction. Donc, on n'ira pas faire signifier à San Francisco, à Los Angeles, par huissier : Venez à nos commissions. Et vous avez sûrement remarqué qu'elles sont absentes, malgré qu'on a vraiment tenté d'avoir, notamment, les volontaires de Shopify, qui sont à l'emploi de Shopify, et donc sous la gouverne de Shopify, alors ils sont absents du débat. Ça laisse quoi, ça, comme goût, pour nous? En tout cas, moi, ça me laisse un goût très amer. Mais il me semble que c'est arrogant, non?

M. Mondoux (André) : Bien, écoutez, c'est... Je blaguais en disant que la société, c'est rendu un concept un peu vétuste, parce qu'on le prend pour acquis, c'est devenu un système, c'est devenu un objet de modélisation, alors qu'en fait ce que c'est, c'est un petit... qui est vivant puis qui est toujours en train de s'adapter.

Moi, j'ai... les bras me tombent quand, premièrement, une entreprise privée dont le modèle d'affaires gère des données va faire l'application pour tout le monde. Bon, bien, déjà, là, moi, ça allume, ce n'est plus jaune ou rouge, là, c'est mauve. Je veux dire, je ne la comprends pas celle-là.

Mme Rizqy : ...conflit d'intérêts?

M. Mondoux (André) : Bien, potentiel, là, je veux dire. Et je ne comprends pas aussi cette volonté de penser qu'on va aller au privé. On n'a pas de ressources, au gouvernement, le privé va faire la job pour moins cher. En temps de crise, je peux vous dire une chose, là, chaque fois qu'il y a eu du privé puis du collectif, en temps de crise, c'est le capital qui a gagné, ce n'est pas les intérêts publics, là, donc il faut... et là on est en temps de crise, et alors... voilà.

Des voix : ...

Le Président (M. Bachand) : J'ai indiqué à la députée combien de temps qu'il lui restait, tout simplement.

Mme Rizzy : On peut continuer, là.

M. Mondoux (André) : Je me doutais que ce n'était pas un signe de non-agression.

Le Président (M. Bachand) : Non, non, absolument pas, là, absolument pas.

Mme Rizzy : Parfait. Et là j'aimerais vous amener sur quelque chose. Tous nos experts nous ont parlé du consentement qui doit être libre et éclairé. Pouvez-vous nous parler de la fabrication du consentement?

M. Mondoux (André) : Ah mon Dieu! Oui. Écoutez, le consentement, tout le monde consent à utiliser les applications : Clic, clic, clic, oups! J'ai-tu dit oui, moi, là? Une recherche faite par mes collègues à Carnegie, il y a à peu près cinq, six ans... Si on lisait tous les contrats d'utilisation des sites Web, des applications, ça serait 130 jours ouvrables de travail par année. Donc, il y a un problème, là. Non, le consentement, et surtout dans les données, est volontaire et involontaire.

Nous, on a fait des recherches, on a pris à peu près, je ne sais pas, moi, une cinquantaine d'applications puis on a regardé le contrat d'utilisation. La plupart, c'est : On prend vos données, c'est à vous, mais nous, on a le droit de les prendre, puis on le donne à des tierces parties, puis on n'est pas responsables. Bien là, il n'y a plus personne qui est responsable, on se ramasse avec des volontaires chez Shopify, puis on a un outil qui est important, que tout le monde dit : Ça va sauver des vies humaines, mais ça se fait de façon anonyme par une boîte privée en Ontario. Puis, au Québec, je ne sais pas, on en a, des ressources, là. Je veux dire, on a des universités, on en forme, nous autres, à l'UQAM, là, puis il y en a ailleurs aussi, je veux dire...

C'est pour ça que je pense que ça prendrait — je reviens sur les propos de madame — une initiative concertée globale. Puis, oui, il va y avoir des compromis de part et d'autre. Puis, bon, évidemment, je fais le jeu en ce moment, là, je me mets complètement de l'autre bord, mais c'est ça que ça prend pour arriver à un juste milieu. Et il n'y aura pas de solution unique, et c'est ce qui me fait peur, moi, avec le génie informatique, il ne marche pas dans la nuance, c'est binaire, c'est oui ou c'est non, alors que, dans le social, c'est vivant, c'est en devenir et c'est toujours réorganisation.

Mme Rizzy : Et au niveau du consentement, c'est que, aussi, je me pose la question : Est-ce que des fois il n'y a pas un risque d'avoir des faux consentements, par exemple, lorsqu'on utilise des sondages? D'ailleurs, les sondages, premièrement, il faut avoir accès à Internet, plusieurs des Québécois n'ont pas accès à Internet, et aussi c'est à quel moment qu'on sonde. Si vous sondez en plein milieu des vacances, durant les périodes de la construction, ça se peut qu'il y ait du monde qui ont d'autres affaires à faire, puis ça se peut qu'ils disent : Moi, c'est la saison du camping, ça fait que laissez-moi tranquille. Est-ce que je me trompe, mais ça peut être un danger de gouverner avec des sondages?

M. Mondoux (André) : Bien, écoutez, c'est un outil à deux tranchants, hein, je veux dire, ça le prend pour avoir le pouls, mais, si on le fait juste par sondage, on n'est pas guère inspiré ou guère inspirant.

J'aimerais revenir, par exemple, sur un point qu'on n'a pas mentionné dans le déploiement des outils. Pensons aux trolls, M. Lévesque. On a vu ça aller, hein? À un moment donné, on a dit : On va faire un truc avec l'intelligence artificielle. Microsoft, il y a quelques années, les gens se sont mis dessus puis ils l'ont transformé en raciste puis en nazi en trois jours. Alors, ce que je veux dire, c'est qu'il peut y avoir très bien des trolls qui vont dire : Je vais vous en faire, moi, des COVID, juste pour s'amuser, pour le fun, hein? Liberté! Je suis émancipé. Il n'y en a plus, de valeurs collectives, on va aller s'amuser, et là qu'est-ce qu'on fait, là? Et c'est là que notre ouverture sur le consentement devient une vulnérabilité. Mais, pour ça, il faut prendre en considération que ce n'est pas juste un individu, une application, c'est une collectivité, puis, dans cette collectivité-là... elle est comme mondiale. Mais, si jamais il y a du monde qui décide que, aïe! on va aller cibler cette application-là, c'est une autre source de problèmes. Mais personne n'en a parlé, de ça, là, les trollings, le hacking, les faux, puis il n'y a aucune façon d'aller chercher ça, là. Et d'ailleurs on s'y fait prendre. Pas plus tard qu'avant-hier soir, je regardais ça, une discussion, je me dis : «My God!» Ça se peut-tu, d'être obtus comme ça? Je fouille un petit peu, puis c'est du monde qui veulent juste brasser. C'est rendu un... Alors, c'est triste, mais il faut composer avec ça, parce que vous comprenez que, quand toutes les valeurs sont devenues relatives, bien, c'est ça, oui, je m'amuse à rire de toutes les valeurs, et c'est le trollisme, hein, qui est là.

Mme Rizzy : Est-ce que le droit à la vie privée commence à devenir relatif ou banal?

M. Mondoux (André) : Écoutez, la vie privée, quand toutes nos données personnelles sont pompées, quand on est rendus... Beaucoup de gens parlent d'économie de la pulsion, hein, maintenant. Alors, on rentre dans l'intimité, quand on a des montres qui vont nous chercher mon taux de sucre, mon battement cardiaque, et ça va aller en s'accroissant. Alors, là... Puis l'idée de vie privée, c'est inséparable de c'est quoi, la vie publique aussi, on ne peut pas prendre un sans parler à l'autre, ça va... un est l'extension de l'autre. Alors, il faut ré-regarder puis il faut regarder ça, et surtout, il faudrait régler...

(Interruption) Aïe! Je vais... technicien, je m'excuse, je vais vous devoir un micro.

On peut bien parler du COVID, mais il y a plusieurs autres applications qui font aussi... qui touchent la vie privée, dont la circulation marchande. Il se véhicule plus de données personnelles en circulation marchande que, probablement, par l'application de COVID-19, et ça, c'est... Il n'y a plus personne... Le problème, c'est : Qui c'est qui va réglementer une compagnie à San Francisco, à Hong Kong? Puis, avec la véritable mondialisation, bien, c'est ça, les États sont rendus des États techniciens, on va gérer le commerce, hein, puis... mais on n'a pas de jurisprudence, on n'a pas de juridiction.

Mais là, en ce moment, ça nous ramène... La pandémie, là, c'est le retour de l'autre. Ici, c'est un grand A, la nature, mais ça nous débouche sur ça, pan-démie, tout le monde, le peuple, et c'est ça qui est en jeu en ce moment.

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

M. Nadeau-Dubois : Merci, M. le Président. M. Mondoux, merci d'être avec nous cet après-midi pour réfléchir avec nous sur ces enjeux-là, qui sont importants, puis qui ne disparaîtront pas de si tôt.

Un argument qu'on entend souvent chez les promoteurs de ces applications, et on l'a entendu formulé de différentes manières dans les derniers jours, on nous a dit, et même les promoteurs le reconnaissent : Il n'y a pas de données probantes ou de données même expérimentales qui nous permettent d'affirmer avec certitude que la technologie Bluetooth fonctionne et que les applications qui fonctionnent à partir de cette technologie sont fiables. Il n'y a personne qui a osé venir nous dire : On le sait, c'est sûr, ça marche, voici l'expérience, en laboratoire ou dans le réel, qui a fonctionné. Mais ce qu'on nous dit, c'est : Même si on ne sait pas vraiment si ça fonctionne, puisqu'on va peut-être sauver des vies, ça vaut la peine d'essayer, et...

Une voix : Faites-moi confiance.

M. Nadeau-Dubois : ...oui, et faites-nous confiance. Qu'est-ce que ce raisonnement-là, qu'on nous a exposé fréquemment... qu'est-ce que ça vous dit sur notre rapport à la technique?

M. Mondoux (André) : Bien, ça me dit de... Premièrement, on n'en a pas parlé ici, mais il y a combien de millions qui circulent, en ce moment, pour l'intelligence artificielle, qui demande beaucoup de données? Alors, évidemment, tout ce qui touche la circulation des données va toucher ces intérêts économiques là. Ça se prépare dans le monde en ce moment, et, au Québec en particulier, on a des ressources de très bonne réputation. Alors, ça bouge beaucoup là-dedans. Alors, ça, ça va faire une pression. Et l'idée, c'est que, si on laisse le marché décider par lui-même, bien, ça ne va pas aider la démocratie, je ne pense pas.

M. Nadeau-Dubois : Mais qu'est-ce que ça vous fait penser, qu'on a un débat sur le fait d'autoriser ou non un outil technologique dont on n'a aucune idée de... si même l'outil en question fonctionne?

M. Mondoux (André) : C'est ça. Bien, c'est pour ça qu'on appelle ça une application.

M. Nadeau-Dubois : On débat de l'appliquer avant de même avoir une certitude si l'outil fonctionne.

M. Mondoux (André) : C'est ça. Bien, c'est ça, le mythe de la neutralité de la technique, je pars en disant : C'est une application, elle est déjà déployée, ça fait que je regarde où c'est que ça accroche, au lieu de dire : Je devrais-tu déployer ça? Ça va-tu faire ça? Quelles sont les valeurs que je vais mettre dedans? Plutôt que de le déployer puis dire : Bien, regarde, je vais avoir le réel qui va apparaître... Puis une fois que le réel, il a apparu, à coups de chiffres, puis tout ça, là, on ne peut plus s'obstiner contre ce réel-là, là, c'est une rationalité instrumentale.

M. Nadeau-Dubois : Autrement dit, on procède à l'envers. On met les... On installe des moyens, puis ensuite on tente de leur trouver des fins.

M. Mondoux (André) : Bien, et... enfin, qui restent dans l'ordre du moyen. On a été efficaces, on a eu tel taux, ça marche-tu ou ça ne marche pas. C'est vraiment étonnant que la faisabilité devient pratiquement secondaire ou encore... Je veux dire, moi, ça me dépasse. Je veux dire, mon collègue Yves Gingras l'a très bien positionné hier, je veux dire, faites des tests, puis regardez... puis regardons. Je veux dire, on n'est pas... on n'a pas le couteau sur la gorge encore, là.

M. Nadeau-Dubois : ...

• (15 h 30) •

Le Président (M. Bachand) : Merci. Désolé, M. le député, je dois passer la parole au député de René-Lévesque. Désolé, M. le député de Gouin.

M. Nadeau-Dubois : ...

Le Président (M. Bachand) : Pardon?

M. Nadeau-Dubois : Je ne vous avais pas entendu.

Le Président (M. Bachand) : Il n'y a aucun souci. M. le député de René-Lévesque.

M. Ouellet : Merci. À mon tour de vous saluer. J'ai eu l'opportunité d'avoir un sociologue dans mon caucus, et, oui, c'est divertissant et stimulant. Le collègue de Bonaventure, qui est sociologue de formation et ancien enseignant, peut, effectivement, des fois... — on dit-tu «sociabiliser»? — sur la situation...

Cela étant dit, j'aimerais avoir un échange avec vous. Tout le long de cette commission, il y a des gens, puis le collègue de Québec solidaire en faisait mention tout à l'heure, qui sont venus nous dire : Bien, ce n'est pas fiable à 100 %. On n'est pas sûrs qu'on mesure la bonne chose. Il y a des gens qui sont venus nous dire : Faites attention, si vous voulez mesurer, ça prend un cadre législatif spécial parce qu'il y aurait peut-être atteinte à la vie privée. Il y a des gens qui sont venus dire : Oui, mais il faudrait aussi qu'on analyse, ou qu'on décortique, ou qu'on monitorise cette application-là avant, pendant et après pour savoir si on fait la bonne chose.

D'un autre côté, c'est ce qu'on entend aujourd'hui, d'un autre côté, le gouvernement a une consultation qui semble indiquer que les Québécois, en tout cas les 17 000 qui ont répondu, la majorité semble dire : Ça nous tente. Et on apprend, dans les médias, de par la bouche du ministre de la Transformation numérique, qu'on va sonder aussi la population pour savoir si on est intéressés ou pas, si les Québécois sont intéressés ou pas de télécharger l'application.

Ce que je veux vous dire, c'est que, même si on a un débat bien intelligent, ici, puis qu'on décide, ensemble, en commission, de dire : Voici ce que ça prendrait pour que ça fonctionne, si j'entends le gouvernement nous dire : Peu importe si les Québécois et les Québécoises le veulent, «we go for it»... Tout le monde nous a dit que, pour que ça fonctionne, il faut qu'il y ait le plus de monde qui l'utilise. On n'est pas devant un faux dilemme, à savoir qu'il y a des gens qui veulent l'utiliser sans avoir tout saisi la portée et sa complicité, parce que c'est dans l'air du temps, et on veut tous se protéger de la COVID. Le gouvernement, qui ne met pas nécessairement toutes les recommandations, parce qu'il pourrait en choisir quelques-unes, mais selon sa volonté, et la nécessité que, pour que ça fonctionne totalement... en sachant tout ça, il faut qu'il y ait le plus de gens qui l'utilisent, qu'est-ce qu'on fait?

M. Mondoux (André) : Là, vous tombez dans l'ordre du politique, et votre collègue sociologue a dû bien lire Weber, *Le savant et le politique*. Il y a des zones où, effectivement, je peux m'exprimer comme citoyen, ce que je ne ferai pas ici, mais je vais parler comme sociologue, bien, c'est des décisions qui relèvent du politique. Certains, comme Habermas, parlent de tyrannie de la majorité, hein, la démocratie, que ça peut être parfois ça, aussi. On en a un exemple avec notre voisin du Sud, qui a une base très fiable, et on voit ce que ça donne aussi.

Donc, écoutez, «damned if you do, damned if you don't», mais je pense que ce qui serait pire, c'est de dire... ça serait de déployer un ou l'autre sans avoir fait de choix, de débat. Au moins, on n'a pas nivelé par le bas. Et puis ça a l'air un peu cucul comme truc, mais, moi, c'est ce que je pense de la présence... Et aussi, de la part de la science, nous, on vous dit ce qu'on observe, ce qu'on voit. Bien sûr, c'est dans notre champ, on n'a pas les mêmes vecteurs, les mêmes responsabilités que vous avez, comme parlementaires et personnes politiques, alors c'est pour ça qu'on peut se permettre d'être un peu plus puristes, si je peux dire. Mais ces nuances-là sont de l'ordre du politique, justement, je dirais... de l'ordre de la politique et pas nécessairement du politique.

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

M. Ouellette : Merci. C'est vrai que c'est rafraîchissant, mais je vous dirais que vous êtes une espèce en voie de disparition. On en a trouvé un à l'Assemblée nationale, il en traîne quelques-uns à l'UQAM. Puis je vous dirais, suite à votre exemple de tantôt, qu'il y en a qui enlèvent leur montre aussi, je vous dirais ça juste comme ça.

J'ai comme l'impression qu'on souffre... la société, aujourd'hui, souffre du syndrome de la banalisation. J'ai comme l'impression... Là, on l'a entendu entre nous autres, là, le gouvernement s'enlign... parce qu'ils ont fait une consultation de 17 000 personnes, il y en a 12 000 qui ont dit qu'ils étaient pour. Ça fait que, sur la foi de ces 12 000 là, là, le gouvernement, là, il s'enlign pour nous donner, en complémentaire, une application «top-notch» qu'eux autres ont décidé que c'est l'application parfaite, parce qu'il y a une problématique, puis ils vont avoir fait de quoi. Le reste, là, bien, les sociologues qu'on a, au Québec, et la société, il va falloir qu'ils prennent ça pour acquis parce que ça va avoir été décidé que c'était la meilleure chose pour eux autres. Et ça va chialer une couple de jours, après ça on va tomber dans la banalisation.

Ça me fait réaliser cet aspect-là, aujourd'hui, de vous écouter puis de vous entendre. Je veux dire, c'est sûr qu'au niveau... à notre niveau, au niveau de la législation, nous autres, bien, il faut penser... une décision qu'on prend ici a un impact sur la vie de 8 millions de personnes, c'est ça. Je vous dirais que, quand tu commences à y penser, là, c'est peut-être un peu plus lourd qu'on prend certaines décisions sans regarder le vivre-ensemble puis dire : Ah! ça va passer, ça va passer. Je ne sais pas si vous...

M. Mondoux (André) : Bien, vous savez, on parle de taux d'adoption, alors 12 000 sur 8 millions, ça donnerait un chiffre aussi...

M. Ouellette : Mais ça, c'est un chiffre politique.

M. Mondoux (André) : Mais, je veux dire, c'est ça, tu sais, 12 000 sur 8 millions, bien... Puis c'est un sondage en ligne, ça a ses limites, aussi, par rapport à un sondage traditionnel. Ça, on le sait aussi.

M. Ouellette : Mais le chiffre que vous allez voir dans les prochains mois, prochaines semaines, c'est 75 %.

M. Mondoux (André) : D'adoption?

M. Ouellette : C'est 75 % qui ont dit qu'ils étaient favorables à cette application-là. Le 12 000, vous ne le verrez jamais. On ne l'a pas vu, nous autres, là, il traîne...

M. Mondoux (André) : Ah! O.K. J'avais inversé les chiffres. O.K., je comprends.

M. Ouellette : Mais ça va être 75 %. C'est ça qui va être dans la bouche de ceux qui vont nous enligner puis qui va être répété, répété, mais le phénomène de banalisation ne m'a jamais paru aussi important que dans les 45 dernières minutes.

M. Mondoux (André) : Bien, l'idée, c'est ça, c'est parce que les 8 millions de citoyens, citoyennes ne sont pas nécessairement au courant. Ils n'ont pas à l'être non plus, c'est plus les spécialistes. Mais, encore une fois, c'est le politique. Je veux dire, nous, on arrive avec nos opinions, on vous dit ce qu'il en est et les laissés-pour-compte derrière tout ça, mais il faut faire attention.

Le Président (M. Bachand) : Pr Mondoux, merci beaucoup d'avoir été avec nous cet après-midi. Merci beaucoup, aussi, d'avoir utilisé un peu de latin. Ça me rappelait mon enfance... pas mon enfance, mon adolescence, disons. Je ne suis quand même pas si vieux que ça.

Merci. La commission suspend ses travaux quelques instants. Merci.

(Suspension de la séance à 15 h 37)

(Reprise à 15 h 43)

Le Président (M. Bachand) : À l'ordre, s'il vous plaît! Rebonjour. Je souhaite maintenant la bienvenue à M. Pierre-Luc Déziel, professeur de droit et spécialiste de la vie privée à l'Université Laval. Alors, bienvenue à la commission. Donc, comme vous savez, vous avez 10 minutes de présentation, après ça on échange avec les membres de la commission. Alors, la parole est à vous.

M. Pierre-Luc Déziel

M. Déziel (Pierre-Luc) : Oui, parfait, très bien. Merci beaucoup. Alors, bonjour à toutes et à tous. Je tiens d'abord à vous remercier de m'avoir invité à venir discuter et échanger avec vous sur cet enjeu particulièrement important.

Alors, mon nom est Pierre-Luc Déziel, je suis professeur à la Faculté de droit à l'Université Laval. Je m'intéresse au droit à la vie privée et à l'impact que les technologies peuvent avoir sur la protection des renseignements personnels, donc mon intervention, aujourd'hui, va surtout se concentrer sur cet élément-là, l'enjeu de la vie privée, qui est un des éléments dans le débat qui est un petit peu plus large, finalement.

Comme vous le savez sans doute, les juristes, on aime bien discuter à partir de faits, de contextes, d'affaires concrètes. Et donc, pour l'exercice du mémoire, mais aussi pour l'exercice de ma présentation aujourd'hui, j'ai décidé de m'attarder à l'application qui a été développée au niveau fédéral, l'application Alerte COVID. Ce choix-là s'explique pour un certain nombre de raisons. Dans un premier temps, les informations qui sont disponibles par rapport à l'application qui serait proposée ou qui serait envisagée au niveau provincial affichent plusieurs éléments, en fait énormément d'éléments, qui correspondent à ceux qui sont disponibles au niveau de l'application fédérale. Et donc mon intuition, c'est que les recommandations, les nuances, les conclusions auxquelles on pourrait arriver en analysant l'application fédérale pourraient être aussi pertinentes dans le contexte provincial.

Donc, il y a deux éléments centraux qui, je crois, traversent ma présentation et sur lesquels je vais insister. Le premier est celui que l'utilisation d'une application de notification au Québec, si on en venait à aller de l'avant avec ce projet-là, devrait absolument être soumise à l'application des lois sur la protection des renseignements personnels au Québec. Ça peut paraître évident, mais, comme je vais essayer de vous le montrer un petit peu plus tard, ce n'est peut-être pas aussi facile ou évident que ça, au final. Le deuxième point fondamental est celui de la confiance, celui

de l'importance de nourrir la confiance du public, surtout dans un contexte d'urgence sanitaire, dans un contexte de santé et dans un contexte où le droit à la vie privée est interpellé, donc l'importance des lois, l'importance de la confiance.

Il y a quatre points sur lesquels je veux revenir. Le premier, comme je viens de vous le mentionner, celui de l'application des lois sur la protection des renseignements personnels dans le contexte de l'utilisation de cette application-là. Alors, pourquoi est-ce que cette question-là est importante? Et cette question-là renvoie à la qualification des données qui vont être collectées par l'application. Qu'est-ce qu'on veut dire par là? C'est de déterminer est-ce que les renseignements qui vont être collectés par l'application peuvent être considérés comme des renseignements personnels. Pourquoi cette question-là est importante? Elle est importante parce que, si on ne considère pas que ce sont des renseignements personnels, par définition, la Loi sur la protection des renseignements personnels ne va pas s'appliquer. La loi, son champ de protection, c'est les renseignements personnels, donc, si on dit : Ce ne sont pas des renseignements personnels, bien, la loi ne va pas s'appliquer.

Donc, déterminer, déjà, les données qu'on a, est-ce que ce sont des renseignements personnels ou pas, ça a l'air d'une question banale, mais ce n'est pas une question qui est si banale que ça, surtout si on regarde l'application qui a été développée au niveau fédéral. L'application qui a été développée au niveau fédéral... Le point de vue du gouvernement du Canada, dans l'évaluation sur la protection des renseignements personnels ou les facteurs de vie privée qui a été transmise au Commissaire de la protection à la vie privée au niveau fédéral, son argument, c'est que l'application ne collecte pas de renseignements personnels. Un renseignement personnel, c'est un renseignement qui porte sur une personne qui est identifiable, au Québec, qu'on va être capables d'identifier la personne. Or, comme vous le savez sans doute, l'application va nous dire qu'il y a de très faibles possibilités d'identifier... très faibles possibilités d'identification des personnes.

Donc, le Commissaire de la protection à la vie privée au niveau fédéral a poussé un petit peu la question avec le gouvernement du Canada pour leur dire : Bien, dans ce cas-là, vous considérez qu'on ne collecte pas vraiment de renseignements personnels, et donc que la Loi sur la protection des renseignements personnels au niveau fédéral ne s'appliquerait pas à l'application? Et la réponse a été : Oui, exactement, c'est ce qu'on pense. On pense néanmoins qu'il y a plusieurs mesures qui ont été prises pour protéger la vie privée des personnes, mais la protection de la vie privée, ça serait... les lois sur la protection de la vie privée ne s'appliqueraient pas parce qu'on ne considère pas que ce sont des renseignements personnels.

Alors, pourquoi cette question-là est importante? Bien, la première... c'est de se dire... En fait, si on ne considère pas que c'est des renseignements personnels, bien, toute la suite de la protection va aussi tomber, hein? Tout ce qui va être... Là, on va parler de consentement, mais tout ce qui peut être, par exemple, le droit à l'accès, les communications non consenties, ce genre de chose là, toute cette protection-là va tomber.

La deuxième chose qui est importante, c'est de savoir que c'est une interprétation du gouvernement fédéral, que ce ne sont pas des renseignements personnels. Ce n'est pas une question qui a été encore tranchée, donc ce n'est pas un fait juridique. Donc, ça se peut qu'éventuellement, s'il y a une plainte, s'il y a une réidentification des personnes, si le Commissaire à la protection de la vie privée ou la cour fédérale détermine qu'il y a eu une collecte de renseignements personnels, bien, en fait, ça voudrait dire que, depuis le début, on dit qu'on ne collecte pas les renseignements personnels puis on se retrouve, un mois, deux mois, trois mois après, en disant : Bien, en fait, on a fait une collecte de renseignements personnels. À partir de ce moment-là, on pourrait dire qu'on a eu une approche qui était peu prudente, qui n'était pas nécessairement... qui peut être problématique, et puis, à partir de ce moment-là, commencer à miner la confiance de la population, en se disant : Bien, on nous avait dit qu'on ne collectait pas de renseignements personnels puis on se rend compte qu'on collecte des renseignements personnels.

Donc, à ce sens-là, moi, ma première recommandation, ça serait de dire : Le gouvernement du Québec, s'il en venait à utiliser une application de notification, devrait s'engager à dire que les lois de protection des renseignements personnels vont s'appliquer à l'utilisation de cette application-là, donc, que ça soit la Loi sur l'accès, pour le secteur public, ou la Loi sur la protection des renseignements personnels dans le secteur privé, pour le secteur privé. Donc, c'est une question qui dépasse un petit peu le fait juridique, mais c'est une question, à mon sens, d'acceptabilité sociale.

Le deuxième point sur lequel je voudrais revenir, c'est le caractère volontaire de l'application. Donc, le gouvernement du Canada et le gouvernement du Québec se sont engagés à dire : Bon, c'est une application qui va être volontaire. Vous en avez parlé beaucoup ici, c'est un fait qui est absolument important. C'est un fait qui va nourrir la confiance du public. Je pense que c'est un engagement qui devrait être maintenu, mais ça soulève quand même des questions qui sont assez importantes. Donc, dans un premier temps, quand on veut parler de consentement ou de volontaire, il va falloir avoir des informations pour transmettre, communiquer des informations qui sont exactes, qui sont vraies, qui sont complètes aux utilisateurs pour qu'ils puissent savoir, quand ils utilisent... ils prennent une décision qui est informée quand ils ont recours à cette application-là.

Or, un des problèmes qu'on a eus au niveau fédéral, et je pense qu'il faudrait l'éviter au niveau provincial, ça a été de dire : Bien, c'est une application qui est anonyme et confidentielle. Et le Commissaire à la protection de la vie privée leur a dit : Bien, est-ce que vous êtes certains de tout ça? Parce que la définition de l'anonymat, puis c'est même la définition qu'on trouve dans le projet de loi n° 64 sur la protection des renseignements personnels, c'est qu'il y a une impossibilité... que ça soit impossible, il n'y a aucune chance qu'on réidentifie les personnes. Or, de l'aveu même du gouvernement fédéral, dans son évaluation, il va dire : Bien, il y a de faibles possibilités, mais ces possibilités-là existent quand même. Donc, une des recommandations du Commissaire à la protection de la vie privée du Canada, qui a été entérinée aussi au niveau de l'Ontario, c'est de dire : Bien, vous ne devriez pas la présenter comme quelque chose d'anonyme, vous ne devriez pas la présenter comme quelque chose de confidentiel parce que

ce n'est pas vrai. Et c'est quelque chose sur lequel le gouvernement a reculé, puis, dans les conditions d'utilisation, on ne retrouve plus cette affirmation-là.

• (15 h 50) •

Donc, une des inquiétudes que j'ai, moi, par rapport à l'application qui est envisagée au Québec, c'est que, quand on va regarder les informations qui sont partagées, on la présente comme étant anonyme. Donc, encore dans cette question de transparence puis de vouloir nourrir cette confiance du public, là, je vous avouerai que, moi, de mon côté, une des recommandations que je ferais, ce ne serait peut-être pas de la présenter comme étant anonyme et confidentielle parce que c'est un seuil ou une promesse qui va peut-être être très difficile à rencontrer. On pourra y revenir un petit peu plus tard.

Troisième point que je voudrais souligner, c'est celui de l'efficacité, donc — évidemment, vous en avez beaucoup parlé depuis hier matin — est-ce que c'est efficace? Est-ce que ce n'est pas efficace? Bon, une des questions qui est assez intéressante, c'est que l'efficacité, c'est un principe fondamental. En tout cas, c'est un des critères qu'on doit absolument évaluer en matière de protection de la vie privée. Au niveau fédéral, ce qui s'est passé, au niveau provincial aussi, de l'Ontario, les deux commissaires à la protection de la vie privée nous ont dit : Évidemment, c'est difficile de tester, là, dans une situation exceptionnelle comme ça, cette nouvelle application là, tester empiriquement, c'est quelque chose de nouveau. Il y a des raisons de croire que ça peut être efficace, donc allons-y de ce côté-là. Mais ce qui est certain, c'est qu'on doit faire un suivi de cette efficacité-là et qu'on doit s'engager à retirer, à mettre hors service l'application si on se rend compte que c'est une application qui n'est pas efficace. Donc, une de mes recommandations, puis, si on va de l'avant, encore une fois, avec un projet d'application au Québec, ça va être de faire un suivi extrêmement serré de l'efficacité de cette application-là au Québec, mais peut-être même aussi à travers le Canada, de bien définir qu'est-ce qu'on entend par «efficacité», de publier cette information-là, et de s'engager à retirer l'application, de la mettre hors service et de supprimer tous les renseignements qui auront été collectés si jamais on se rend compte que l'efficacité n'est pas rencontrée. Donc, ça, c'est une nuance qui est à retenir au niveau fédéral puis au niveau de l'Ontario aussi, mais qui est excessivement importante, à mon sens.

Mon quatrième point, dernière recommandation, porte sur tout ce qui va être important de mettre en place au niveau provincial si on en venait à utiliser l'application fédérale. L'application fédérale, telle qu'elle est décrite par le gouvernement du Canada, telle qu'elle est décrite dans le rapport d'évaluation des impacts sur la vie privée et telle qu'elle a été analysée par le Commissaire à la protection de la vie privée, ne porte que sur une partie de l'application, c'est-à-dire tout ce qui serait géré par le fédéral. Il y aurait tout un mécanisme à mettre en place au niveau provincial aussi, qui tombe un peu dans l'angle mort, parce que le Canada ne va pas se prononcer sur le mécanisme qui serait mis en place au Québec puis lui donne la possibilité de le faire comme il veut.

Mais c'est là, et c'est très clair, dans l'évaluation du gouvernement fédéral, qu'il y aurait des enjeux de protection de la vie privée qui seraient plus importants. Pourquoi? Parce que c'est au niveau provincial que l'appariement entre les codes uniques des usagers et les diagnostics médicaux, qui sont, évidemment, des renseignements personnels, vont être appariés. C'est là qu'on va faire la combinaison entre les deux et c'est là qu'on va transmettre ce code-là qui va permettre aux usagers de téléverser leur code... pardon, leur clé d'exposition temporaire sur le serveur fédéral. Donc là, il y a un risque de... Comment est-ce qu'on va mettre en place ce mécanisme-là, finalement? Ça n'a pas été discuté au niveau fédéral. Et, quand on parle même de prendre l'application fédérale, si on en venait jusque-là, il y aurait tout ce mécanisme-là à mettre en place, qui serait beaucoup plus sensible. Donc, encore une fois, là, l'importance de nourrir la confiance, d'assujettir ces mécanismes-là à la protection des renseignements... aux lois... pardon, à la Loi sur la protection des renseignements personnels, donc, comment est-ce qu'on pourrait faire ça? Très rapidement...

Le Président (M. Bachand) : Je dois malheureusement vous arrêter, vous avez dépassé le temps, mais il y a la période des questions, faites-vous-en pas, M. Déziel. Alors donc, je me tourne vers le gouvernement. M. le député de Chapeau.

M. Lévesque (Chapeau) : Oui, merci beaucoup, M. le Président. Merci beaucoup, maître. C'est un plaisir de vous voir. Merci de votre témoignage.

J'irais peut-être directement avec la notion d'anonymat et de confidentialité. Donc, au fédéral, vous dites qu'ils ont retiré cet élément-là. Évidemment, l'objectif, c'est que ça soit anonyme et confidentiel, dans l'idée, justement, de la protection de la vie privée, protection des renseignements personnels. Y aurait-il un moyen, soit juridique ou même technique, ou que vous avez... qu'on pourrait s'assurer que ça le soit, que ça soit anonyme et confidentiel, ou c'est vraiment par la voie du retrait de cette affirmation-là que ça se passe? Parce que l'objectif, ça serait que ce le soit, là. On ne veut pas que ça soit... les gens soient identifiés ou nommés, on veut que ça reste confidentiel.

M. Déziel (Pierre-Luc) : Mais il y a deux choses que je dirais par rapport à ça. La première, c'est que l'anonymat, tel que défini au niveau de la loi puis même tel que défini dans la loi... dans le projet de loi n° 64, est un seuil extrêmement difficile à avoir, puis c'est donc de donner la garantie qu'on ne va jamais être en mesure d'identifier personne. Or, depuis hier matin, ce qu'on entend, ça, c'est avec les technologies Bluetooth, on l'a entendu à travers les différentes interventions, il y a un certain nombre de vulnérabilités. Il y a un certain nombre d'attaques qui sont possibles, même si elles sont minimes. De dire que ça serait anonyme, ça peut être très difficile à rencontrer comme seuil, vraiment, de garantir cette impossibilité d'identification ou de réidentification là. Donc, avec l'application fédérale, ça n'a pas été fait. Est-ce que j'ai entendu des solutions où qu'ils étaient 100 % anonymes? Non, je n'en ai pas entendu, je n'en ai pas vu. Je n'en ai pas entendu, encore une fois, mais c'est au niveau du terme technique, peut-être, qui est utilisé en droit.

Maintenant, ça peut être un terme... et puis c'est peut-être le deuxième point sur lequel je veux arriver, et c'est une question qui me tient beaucoup à coeur, c'est de dire : Pour rassurer les gens, pour en nourrir leur confiance, à mon sens, on n'est pas obligés de dire que c'est quelque chose d'anonyme, nécessairement, on peut leur dire : C'est une application qui respecte la vie privée, qui a des garanties très fortes de protection de la vie privée, ce qui est protégé par nos lois sur la protection de nos renseignements personnels. Pour moi, le fait de chercher absolument l'anonymat, ce n'est peut-être pas le bon chemin, de toute façon. À mon sens, c'est quelque chose qu'on doit... C'est un gros problème qu'on a, en droit à la vie privée, c'est de penser que le droit à la vie privée, c'est de taire les choses, que tout soit silencieux, tout soit caché tout le temps. Le droit à la vie privée, c'est d'être capable de choisir volontairement, sur une base éclairée, qu'est-ce que je vous communique comme renseignements personnels. Si je vous donne mon adresse, par exemple, ou mon adresse courriel, je vous donne un renseignement personnel, mais je le fais volontairement. Ce n'est pas anonyme, mais j'exerce quand même mon droit à la vie privée parce que je vous le donne. Je sais qu'est-ce que vous allez faire avec, pourquoi vous me le demandez, ce genre de chose là.

Donc, de dire qu'il y a une collecte de renseignements personnels ou qu'il y en aurait, à mon sens, ce n'est pas un problème. On le fait régulièrement. Quand vous allez faire un achat à l'épicerie, vous payez avec votre carte de crédit, il y a une collecte de renseignements personnels. Quand vous allez chez le médecin et vous passez un diagnostic de COVID-19, il y a une collecte de renseignements personnels. Il y a beaucoup de contextes dans lesquels il y a une collecte de renseignements personnels et où ce n'est pas un problème parce qu'il y a des mécanismes qui sont faits, qui sont mis en place par la suite et qui sont dans nos lois de protection des renseignements personnels pour les protéger. Donc, même la recherche de contacts manuelle implique une somme colossale de renseignements personnels.

M. Lévesque (Chapleau) : Donc, la divulgation, la transparence, l'explication est source de confiance pour la population. Donc, ça serait plus sous cet angle-là que vous l'aborderiez, à ce moment-là, plutôt que de dire l'anonymat ou quelque chose... alors qu'il y a peut-être un petit risque là?

M. Déziel (Pierre-Luc) : Exactement.

M. Lévesque (Chapleau) : J'aimerais peut-être vous amener sur l'efficacité. Effectivement, c'est un sujet qui a alimenté nos débats, là, hier et aujourd'hui, évidemment, la nécessité de la vie privée, la protection. Vous dites de définir et publier, dans le fond, ce que représente l'efficacité, et la retirer, retirer l'application, si on n'atteint pas cette efficacité-là. Il n'y a pas de consensus entre les experts. Je veux dire, il n'y a pas personne qui nous dit c'est quoi, l'efficacité, exactement, et tel point, tel million, tel ci, tel ça. Comment on fait ça? Comment on atteint cet objectif-là que vous nous présentez sur l'efficacité?

M. Déziel (Pierre-Luc) : Bien, c'est sûr que ça prendrait une réflexion, par la suite, pour définir cette efficacité-là, définir, par exemple, un seuil, par exemple, qui devrait être atteint ou pas. Je pense qu'il y aurait une délibération qui serait importante au niveau d'experts dans ce domaine-là, par exemple, au niveau des statistiques, au niveau de ce genre de chose là. Je vous dirais qu'en tant que juriste je n'ai pas vraiment cette définition-là et je suis pas mal convaincu que la définition de l'efficacité juridique ne vous conviendrait pas, c'est-à-dire que la... qui est la capacité d'atteindre la fin visée. Bon, c'est ça, on tourne en rond avec cette définition-là. Mais je pense qu'il y aurait cet aspect-là qui serait excessivement important, mais qui serait certainement fait par... qui serait défini par des experts. Cette recommandation-là, elle a été faite au niveau fédéral puis elle a été faite au niveau provincial par le commissaire à la protection de la vie privée de l'Ontario aussi.

M. Lévesque (Chapleau) : O.K. Au niveau de l'application fédérale, vous avez parlé de... il y a un risque de la mise en place, au Québec. Qu'est-ce que vous entrevoyez pour assurer la confiance, dans le fond, des Québécois pour s'assurer que, bon, lorsqu'il y aurait une... s'il y avait une mise en place d'une telle application, les Québécois soient en confiance, soient rassurés par rapport à ça, donc, dans l'application, la transition, l'espèce de...

• (16 heures) •

M. Déziel (Pierre-Luc) : Oui, bien, je vous remercie beaucoup pour cette question-là parce que c'était mon quatrième point, que je n'ai pas eu le temps d'exposer tout à l'heure, donc merci pour ça. Donc, comme je disais, bien, il y aurait toute cette collecte-là, potentiellement, de renseignements personnels qui se passerait au Québec, qui va être un peu plus sensible qu'au niveau fédéral. C'est quelque chose qui est clair dans les rapports au niveau fédéral aussi. Et une des choses qui ont été recommandées au niveau de l'Ontario, parce qu'eux ont à mettre en place cette structure-là, ça a été de faire... c'est des choses qui ont été discutées ce matin par la Commission d'accès à l'information aussi, c'est de dire : Faisons une... le gouvernement devrait faire une évaluation des facteurs relatifs à l'impact sur la vie privée des gens de ce mécanisme-là, devrait publier cette évaluation-là, devrait la transmettre à la Commission d'accès à l'information et s'engager, à mon avis, à respecter les recommandations qui vont être formulées par la Commission d'accès à l'information, qui est notre expert, au Québec, en termes de protection des renseignements personnels, et que cette évaluation-là soit publique, et que les recommandations, bien, qui sont par nature publiques, aussi, du Commissariat à la protection... de la Commission d'accès à l'information, soient faites.

Je souligne le fait que c'est important que ça soit public, parce qu'au niveau provincial, en Ontario, l'évaluation des facteurs relatifs à la vie privée qui a été effectuée par le gouvernement de l'Ontario a été examinée par le Commissaire à l'information et à la protection de la vie privée de l'Ontario, et il y a une recommandation pour

qu'elle soit publique, cette évaluation-là, elle ne l'est pas encore. J'aurais bien aimé. Ça fait deux semaines que je cours après, je n'ai pas encore réussi à trouver cette évaluation-là. Donc, dire comment ça a été fait en Ontario, exactement, c'est difficile parce qu'on n'a pas accès à cette information-là. J'ai bon espoir qu'elle le devienne, éventuellement, mais je pense qu'au Québec on devrait d'emblée la publier... la publier, comment est-ce qu'on a fait ça, s'engager à respecter les recommandations du Commissaire... de la Commission d'accès à l'information, pardon.

M. Lévesque (Chapleau) : O.K. Vous m'avez surpris, tout à l'heure, en disant que le fédéral avait, dans le fond, soustrait l'application... du moins, la notion de renseignements personnels dans l'application. Évidemment, tu sais, si on envisage ça au Québec, ça serait avec la plus grande protection possible pour les citoyens. Donc, je ne pourrais pas envisager nécessairement qu'on ne mettrait pas, tu sais, l'application sous ce couvert-là, sous cette protection-là.

Voyez-vous d'autres failles, d'autres vulnérabilités, dans les lois actuelles, qu'on pourrait, tu sais, s'assurer que ça s'applique pour qu'on puisse, dans le fond, tu sais, avoir la meilleure protection possible pour les citoyens?

M. Déziel (Pierre-Luc) : Bien, je vous dirais que moi aussi, j'ai été assez surpris quand j'ai lu ça, finalement, et leur argument tient la route, quand même, au niveau juridique. Mais au niveau, après, d'acceptabilité sociale, c'est peut-être un petit peu plus... c'est un peu plus compliqué, de ce côté-là. Leur argument, c'est de dire : Bien, il y a quand même des choses qui sont mises en place pour protéger la vie privée des gens, et c'est vrai, mais il y a des choses qui tombent en dehors de tout ça. Donc, c'est la raison pour laquelle je vous dis qu'au provincial on devrait faire cet engagement-là, au-delà d'un débat théorique sur est-ce que c'est un renseignement personnel ou pas, qui demeure une interprétation.

Une des choses, peut-être, qu'il est intéressant de noter de ce côté-là et qui est peut-être un angle mort, si on va dans le contexte de la Loi sur l'accès, c'est que le consentement n'est pas un fondement juridique pour obtenir des renseignements personnels au niveau provincial, hein? C'est une chose, même, qui a été discutée par l'Alberta avec son application ABTraceTogether. Très clairement, il y aurait une autorité légale pour aller chercher ce renseignement-là, mais le caractère volontaire, ça serait volontaire du gouvernement, dans une certaine mesure, même en suivant ces lois-là, il ne serait pas tenu d'aller le chercher. Donc, un engagement fort serait important. Peut-être que c'est même là, comme vous en discutiez ce matin, d'avoir une loi ou un décret, là, particulier sur cette application-là qui dit qu'il doit être volontaire pour tout le monde, ça viendrait combler, peut-être, ce vide-là qu'on aurait au niveau des lois sur l'accès au Québec.

M. Lévesque (Chapleau) : O.K., intéressant. Merci. Peut-être plus large, là, vu qu'on vous a ici, là, vous êtes un expert, sur les lois actuelles en matière de protection de vie privée puis de renseignements personnels puis le projet de loi n° 64, là. Vous en avez fait mention. J'imagine que, vu que c'est votre champ d'études, vous avez sûrement lu ce projet de loi là aussi. Il y a-tu des éléments qui manquent? Il y a-tu des choses qui seraient pertinentes à ajouter, si on va plus global, là?

M. Déziel (Pierre-Luc) : Moi, un de mes champs de bataille, en quelque part, dans le contexte du droit à la vie privée, puis ce n'est pas tous mes collègues qui sont d'accord avec ça non plus, je dois l'avouer, c'est — puis on revient à qu'est-ce que je vous disais tout à l'heure — la définition même d'un renseignement personnel, en fait.

Donc, une des grandes failles de notre loi actuelle, c'est de dire : Bien, un renseignement personnel, c'est un renseignement qui permet d'identifier les personnes; si on n'identifie pas les personnes ou il n'y a pas des bonnes chances d'identifier les personnes, ça tombe en dehors de la sphère de la protection à la vie privée. Mais aujourd'hui, vous le savez, on en a parlé, il y a tout le temps un risque, il y a tout le temps une possibilité de réidentifier les personnes. Et puis ce facteur-là ou ce critère-là qu'on a dans la jurisprudence pour dire : Il faut qu'il y ait une forte possibilité, par exemple, de réidentification, bien, ça fait tomber plein de renseignements en dehors de tout ça.

Donc, dans le projet de loi n° 64, il y a peut-être un meilleur encadrement des renseignements qui ont été dépersonnalisés, comme on va dire, ou qui ont... c'est-à-dire qu'on a retiré des identifiants directs, ou indirects, ou même anonymisés. Ma première lecture, c'est que c'est un bon pas de l'avant de ce côté-là, mais qu'il y avait encore... et là je ne veux pas rentrer dans les détails non plus parce que je ne l'ai pas sous les yeux puis je ne suis pas venu préparé pour cette question-là en tant que telle, mais...

M. Lévesque (Chapleau) : Non, c'est juste si vous avez des petites idées à brûler-pourpoint.

M. Déziel (Pierre-Luc) : ...que c'est un bon pas dans cette direction-là, mais, pour moi, il y a encore peut-être un petit peu de travail à faire de ce côté-là.

M. Lévesque (Chapleau) : Une lacune? O.K. Puis, en terminant, on a parlé beaucoup de confiance, auriez-vous un autre conseil, si jamais le gouvernement décidait d'aller de l'avant avec une application, pour ajouter à la confiance des Québécois?

M. Déziel (Pierre-Luc) : En termes de vie privée, vraiment, c'est ce que j'ai dit, c'est vraiment de nourrir puis chérir cette confiance-là, c'est-à-dire de comprendre ce lien synergique là. Peut-être que c'est plus un état d'esprit ou une attitude, je pense, qu'il faut adopter.

Au cours des auditions, jusqu'à présent, on a beaucoup parlé de l'équilibre à atteindre entre la vie privée, puis d'autres impératifs comme le droit à la santé, par exemple, ou la sécurité dans un contexte comme ça, puis que, pour donner à un, il faut un peu reprendre à l'autre, puis qu'il y ait cette équilibration-là comme ça. Moi, dans ma perspective, c'est un petit peu les recherches que je mène, c'est comment est-ce qu'on peut faire travailler ces deux choses-là ensemble, finalement, puis nourrir la confiance des gens en disant : On collecte des renseignements personnels, on peut protéger votre vie privée, puis en protégeant votre vie privée, bien, ça vous donne confiance, vous allez utiliser l'application, puis en utilisant l'application, bien, peut-être, si elle est efficace, là — faisons ce postulat-là pour les fins de la discussion — bien là... améliore encore plus la santé.

Donc, c'est peut-être de plus voir la relation entre le droit à la vie privée puis d'autres impératifs comme pas nécessairement conflictuelle, parce que ça nous amène nécessairement à faire des choix, peut-être, des fois, qui ne sont pas nécessaires, mais de le voir comme quelque chose qui peut être synergique. Puis, pour faire ça, bien, ça nous prend la confiance des personnes, ça nous prend une communication honnête, ça nous prend une explication qui est fiable, ça nous prend un suivi, ça nous prend des experts indépendants ou une surveillance indépendante, par exemple, comme la Commission d'accès à l'information. Puis, à partir de ce moment-là, moi, le fait que ça soit... on collecte des renseignements personnels, puis ce n'est pas anonyme, mais on a toute une batterie de choses qui viennent encadrer ça, on ne va pas réutiliser les données à d'autres escients. Une fois que la pandémie est faite, puis c'était une des recommandations que je faisais dans mon mémoire aussi, on enlève tout ça, on «delete» tout ça et puis on ne va jamais réutiliser ces données à d'autres fins, là. Ça, c'est des méthodes de reconnaître qu'on collecte des renseignements personnels, qu'on est honnêtes avec les gens et qu'on n'essaie pas d'aller au va-vite en disant : C'est quelque chose de fantastique, il n'y a jamais rien qui va se passer. Il faut nourrir cette confiance-là parce qu'après, quand il y a des incidents, on perd cette confiance-là puis on la perd pour longtemps.

M. Lévesque (Chapleau) : Merci beaucoup. Merci, M. le Président.

M. Déziel (Pierre-Luc) : Ça me fait plaisir. Merci à vous.

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

Mme Boutin : Je vais être relativement brève. J'aimerais revenir, parce que je n'ai pas super bien compris la réponse. Bon, on a parlé de l'expérience de l'Ontario, l'expérience du Canada puis le fait, bon, que ce soit un téléphone, bon, c'est la Santé publique qui émet un identifiant relié à un test, si on a un test positif, on le met sur notre téléphone. Puis là, bien, il n'y a pas de décision qui a été prise puis même sur le type, si c'est une application seulement au Québec ou si on décide, étant donné qu'il y a des touristes, puis on voyage en Ontario... Puis peut-être qu'il y a des gens qui voudraient, justement, savoir si, exemple, on est en contact avec des Ontariens... Quels mécanismes... parce que vous avez brièvement mentionné des mécanismes qui pourraient être mis en place pour, mettons, nous aider à encore mieux protéger les données, parce que, souvent, si on décidait d'aller, par exemple, utiliser l'application fédérale, comme l'Ontario, et tous ensemble, toutes les provinces, bien, c'est sûr qu'à un certain moment donné, même si on stocke... la Santé publique stocke, collecte les données de la santé, les stocke au Québec, bien, j'imagine que ça se promène, tu sais. Les données n'ont pas de frontières, elles sont stockées, mais... Quand tu es sur le téléphone, si moi, je m'en vais en Ontario, bien, j'ai traversé... Est-ce que des mécanismes peuvent être mis en place pour protéger les données personnelles?

M. Déziel (Pierre-Luc) : Je vais essayer de répondre en essayant de comprendre.

Mme Boutin : Ce n'est pas clair, peut-être, hein?

M. Déziel (Pierre-Luc) : C'est une question qui est importante puis qui est assez large. Comme je vous dis, quand on réfléchit à ces questions-là, c'est toujours dans un contexte particulier, donc moi, je l'ai regardé en fonction de l'application au niveau fédéral, parce qu'après, sinon, il y a mille et une façons, là, de protéger les...

Mme Boutin : Ou est-ce qu'ils ont mis les mécanismes, peut-être, en Ontario puis le fédéral, du fait que les données sont interopérables? C'est plus ça, peut-être?

• (16 h 10) •

M. Déziel (Pierre-Luc) : Oui, c'est ça. Bien, en fait, c'est que ça tient à la structure un petit peu décentralisée de l'application, qu'il y a des données qui sont générées... qui sont gérées par le serveur fédéral, par l'utilisateur et puis par le niveau provincial, puis que c'est en faisant cette séparation-là — c'est un peu comme si on prenait une photo puis on la déchirait, bien, chacun a une partie de la photo, mais n'a pas l'ensemble total — puis que les échanges se font entre ces différents acteurs-là, si vous voulez, avec des systèmes de cryptographie asymétrique, des fonctions de hachage, ce genre de choses là. C'est des choses qui sont détaillées dans le rapport.

Et puis, donc, à partir de ce moment-là, ces mesures-là, si on... Je ne suis pas un expert en informatique non plus, il faudrait peut-être leur demander à eux, exactement, techniquement, comment le faire, mais l'évaluation du Commissaire à la protection de la vie privée, c'est que ce sont des protections quand même qui sont assez solides. Les recommandations que... Les conclusions, au niveau fédéral puis au niveau de l'Ontario... Elles ont été recommandées, ces applications-là, par les commissaires, mais c'est en prenant en compte toutes ces autres mesures là par la suite.

Donc, comme je vous dis, un des problèmes qu'on a en ce moment, on pourrait se baser... ou je pourrais vous répondre en disant : Bien, en Ontario, c'est comme ça qu'ils ont fait, mais on n'a pas vraiment de détails sur comment ils ont fait. C'est la raison pour laquelle, même au niveau de cet échange-là entre les provinces, il va falloir que les choses soient transparentes puis que, même, la population ait accès à cette information-là.

Mais une chose qui est certaine, c'est que le danger derrière tout ça, c'est l'appariement des données, finalement. Donc, un des risques qui est évoqué dans le rapport du Commissaire à la protection de la vie privée, c'est qu'au niveau provincial c'est là qu'on va avoir accès au diagnostic, c'est là qu'on va communiquer avec les personnes, on va vouloir leur donner un code unique, c'est là qu'il y a certaines personnes qui vont avoir des diagnostics où le nom des personnes est le code unique, puis que, à la limite, ces personnes-là vont être capables de savoir... puis ça devient déjà un renseignement personnel, telle personne a utilisé telle... a déjà téléchargé l'application, puis ça, ça peut être déjà un enjeu, finalement. Dans la structure actuelle, ils n'auraient pas accès aux clés d'exposition temporaires, donc ils ne pourraient pas savoir qui était où, à qui ils ont parlé, comment ces choses-là se sont échangées entre les différentes personnes. Mais c'est une question qui est technique, sur laquelle on n'a pas beaucoup d'information. Donc, je pense que... bien, j'essaie de répondre au mieux de mes capacités, mais je pense que...

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

Mme Rizqy : Merci beaucoup. Bonjour. Bienvenue parmi nous. Je commencerais avec le même ordre de votre présentation, avec le point n° 1, c'est-à-dire, vous avez adressé la question suivante : Le fédéral, le gouvernement fédéral est d'opinion que ce n'est pas un renseignement personnel. Partagez-vous cette même opinion?

M. Déziel (Pierre-Luc) : C'est une opinion qui est très forte en droit, en tout cas. L'argument est très fort, en fait. Si on suit la définition du renseignement personnel, est-ce que c'est quelque chose qui permet, à sa face même, d'identifier directement les personnes? Ce n'est pas un renseignement personnel. Et la jurisprudence va nous dire : Il faut qu'il y ait une forte possibilité de réidentifier les personnes. Et l'analyse du Commissaire à la protection de la vie privée, qui a pu voir, là, sous le capot, comme il a été dit ce matin, et l'analyse du fédéral, c'est de dire : Bien, il y aurait de faibles probabilités. Donc, c'est un argument qui est très fort, en droit. Mais c'est... vous savez très certainement, ce n'est pas parce que le droit le dit que c'est une bonne chose, nécessairement. Donc, même les lois...

Mme Rizqy : Avez-vous peut-être une décision à nous citer ou à nous remettre plus tard? Bien, peut-être pas à brûle-pourpoint, là. Parce que je suis un peu étonnée de votre propos, parce que vous avez aussi commencé en nous disant : Comme tout bon avocat, je travaille avec des faits. Alors, je vais vous donner un exemple, peut-être, pour mieux illustrer les propos. Prenons un exemple réel : avril 2018, Facebook a l'application où est-ce qu'on peut identifier nos amis ou des gens potentiellement amis, amis avec nous, qui sont au même endroit, alors certains avocats se sont dit : Hum! J'ai un procès avec jury... Vous savez... Vous êtes avocat?

M. Déziel (Pierre-Luc) : Non, mais j'ai un doctorat en droit.

Mme Rizqy : Ah! O.K. Dans ce cas-là, juste... D'accord, d'accord, je pensais... j'ai tenu pour acquis que vous étiez avocat, vu que vous avez dit «comme tout bon avocat».

M. Déziel (Pierre-Luc) : Non.

Mme Rizqy : Alors, bien, vous n'êtes pas sans savoir qu'il est important de garder l'anonymat des membres du jury.

M. Déziel (Pierre-Luc) : Absolument.

Mme Rizqy : Alors, les avocats, côté défense, ont identifié, grâce à cette application, les membres du jury parce qu'ils étaient géolocalisés au même endroit. Alors, c'est pour ça que je suis un peu étonnée, lorsque... cette affirmation de jurisprudence, parce qu'il y a même le Barreau, là-dessus, qui était sorti pour dire : Bien, c'est allé trop loin. Même si on ne pouvait pas les identifier immédiatement, on a été capables de les identifier indirectement. Alors, c'est pour ça que je suis un peu étonnée, mais je...

M. Déziel (Pierre-Luc) : Bien, je dirais que, dans ce contexte-là, il y a une collecte de renseignements personnels, c'est-à-dire, bien, c'est une... si on peut identifier la personne, là ça serait un renseignement personnel. Donc là, si on a cherché à identifier des personnes, ça va être un renseignement personnel. Mais, juste pour revenir sur... parce que...

Mme Rizqy : Mais, si vous permettez, parce que le temps file... laisser terminer, parce que c'est...

Le Président (M. Bachand) : ...peut-être juste laisser terminer...

Mme Rizqy : Oui. Non, mais c'est... M. le Président, vu que c'est mon temps, je me permets de pouvoir...

Le Président (M. Bachand) : Parce que vous le coupez, c'est pour ça, là.

Mme Rizqy : Non, ce n'est pas que je le coupe, c'est qu'il a répondu à ma question, puis j'ai tout de suite une question, puis le temps file.

Le Président (M. Bachand) : Allez-y, allez-y.

Mme Rizqy : Ma deuxième question, c'est que le commissaire à la vie privée, dont vous faites mention, le 31 juillet, mentionne, et vous l'avez affirmé vous-même, qu'on peut identifier des gens. Est-ce que ça, ça ferait en sorte que, pour nous, on pourrait considérer que ça pourrait être un renseignement?

M. Déziel (Pierre-Luc) : Bien, c'est exactement... puis c'est exactement le point, puis c'est pour ça que c'est difficile, puis c'est des définitions techniques, en droit. Donc, la définition, à mon sens... Je pense que l'argument est fort, comme je vous dis, du gouvernement, mais ça ne veut pas dire qu'il n'y a pas quelque chose, en dessous du droit, qui cloche, en fait. Puis c'est un peu ce que je vous disais tout à l'heure, la définition même du renseignement personnel, elle est problématique. La définition, c'est la... quelque chose que... Le Commissaire à la protection de la vie privée l'a dit, la Commission d'accès à l'information, les lois doivent être modernisées, on doit améliorer la définition même du renseignement personnel. Donc, l'argument est fort, mais ça ne veut pas dire qu'on devrait le suivre dans un contexte purement juridique, mais le voir un petit peu plus large puis dire... On peut jouer sur les technicalités puis dire que ce n'est pas des renseignements personnels, mais est-ce que, vraiment, ça nous avance à quelque chose, finalement?

Tout à l'heure, vous m'avez demandé la référence. La référence, c'est Gordon contre Santé, qui est une décision de la Cour fédérale de 2008 qui va nous dire qu'il faut qu'il y ait des fortes probabilités de réidentifier les personnes. Donc, c'est pour ça qu'il y a un danger. C'est-à-dire que, là, pour le moment, on nous dit : Ce n'est pas des renseignements personnels parce qu'il y a des faibles possibilités de réidentifier les gens. Ce n'est pas des fortes probabilités, donc ce n'est pas un renseignement personnel, mais il y a quand même cette possibilité-là qui existe, c'est la raison pour laquelle ce n'est pas anonyme. Et, si jamais on venait à identifier des personnes, bien là, ce serait un renseignement personnel, puis là on collecterait des renseignements personnels en ayant dit qu'on ne le ferait pas, et puis là on est dans ce conflit-là, qui va venir miner la confiance des personnes, à mon sens.

Mme Rizqy : Mais il est encore toujours possible qu'un jour on puisse avoir un tribunal qui regarde la question avec les faits d'aujourd'hui. Parce que 2008, entre aujourd'hui et maintenant, ce qu'on ne connaissait pas avant, c'était... 2008, c'était juste avant l'arrivée d'Instagram et de d'autres applications et où est-ce que nous aussi, on a pris connaissance de tout ce croisement de données et des scandales comme Cambridge Analytica. Alors, on a encore, ici, beaucoup d'inconnues devant nous.

Et vous avez aussi parlé du caractère volontaire. Est-ce que vous avez entendu parler de certains employeurs... Je ne sais pas si vous avez eu la chance, parce que c'était ce matin, d'entendre la Commission des droits de la personne et des droits de la jeunesse, qui nous indiquait clairement... non, désolée, je vous ai induit en erreur, c'est la Commission d'accès à l'information, désolée, je vous ai induit en erreur, je vais me reprendre, la Commission d'accès à l'information, qui nous a indiqué qu'il y avait déjà, en ce moment, une enquête en cours parce qu'un employeur forçait, justement, l'utilisation. Est-ce que vous nous recommandez d'avoir, justement, tel qu'on l'a entendu ce matin, d'avoir une législation beaucoup plus robuste qui va permettre de mieux encadrer les employeurs?

M. Déziel (Pierre-Luc) : Absolument.

Mme Rizqy : Est-ce que vous allez aussi plus loin? Parce que, maintenant, on peut voir ailleurs dans le monde, dans des juridictions, disons, moins clémentes au respect des droits et libertés des individus... qui demandent de scanner un code UR, un code-barres, en fait, pour pouvoir entrer dans certains établissements. Est-ce que vous pensez que, ça, on devrait aussi ne pas permettre à ces établissements de pouvoir scanner... de demander, au fond, aux gens de scanner un code-barres afin de rentrer au restaurant, rentrer à tel endroit, de rentrer dans l'autobus?

M. Déziel (Pierre-Luc) : C'est la première fois que j'entends ce type d'exemple là. Donc, scanner un code-barres pour rentrer à quelque part?

Mme Rizqy : Oui.

M. Déziel (Pierre-Luc) : O.K. Bien, c'est dans certains contextes. Ça dépend si c'est un endroit qui est sécurisé... Peut-être pas n'importe qui peut rentrer dans un laboratoire, par exemple.

Mme Rizqy : Non, par exemple, l'autobus, services publics, là.

M. Déziel (Pierre-Luc) : Ah! O.K. Bien, rentrer ça, code-barres, j'imagine que l'idée, derrière tout ça, c'est de savoir... d'identifier la personne, là, puis de savoir que ce n'est pas juste quelqu'un qui est rentré, mais que c'est...

Mme Rizqy : Non, c'est parce qu'on veut savoir si la personne était testée avec la COVID-19, là.

M. Déziel (Pierre-Luc) : C'est ça, c'est ça. Bien, c'est très risqué, en tout cas, à mon sens.

Mme Rizqy : Parfait. Je vais continuer, je sais que le temps file, efficacité. J'entends que vous avez bien écouté, hier, nos invités.

M. Déziel (Pierre-Luc) : Absolument. J'ai regardé toutes les présentations jusqu'à tant que je doive partir d'ici.

Mme Rizqy : Ah! merci, c'est vraiment apprécié.

M. Déziel (Pierre-Luc) : C'était passionnant.

Mme Rizqy : La très grande majorité, à part peut-être un d'entre eux, la très, très grande majorité nous ont dit que c'était très peu efficace, voire anecdotique. Alors là, aujourd'hui, quand on balance les droits, les libertés, là, quand on tombe dans l'anecdotique, qu'est-ce que vous en pensez?

M. Déziel (Pierre-Luc) : Si l'efficacité est anecdotique? Bien, je ne serais pas compétent pour vous dire est-ce que c'est quelque chose qui est efficace très fortement ou anecdotiquement parlant. Comme je vous dis...

Mme Rizqy : Bien, en plus, en matière de droit, la proportionnalité des inconvénients, la balance, en fait, parce que, si on nous dit qu'une application est anecdotique dans son efficacité et le risque... C'est plus là-dedans que j'aimerais vous entendre.

M. Déziel (Pierre-Luc) : Bien, en termes de protection de la vie privée, c'est assez clair, et ça, c'est l'analyse même du Commissaire à la protection de la vie privée. Puis c'est pour ça qu'il y a des mesures qui sont mises en place, un petit peu comme on discutait tout à l'heure.

En fait, quand on veut chercher des renseignements personnels pour les personnes, il faut qu'on les informe de la finalité, il faut qu'on dise : Moi, c'est pour faire ça, que je veux aller chercher les renseignements personnels. Si je vais chercher ces renseignements personnels là, après on va regarder est-ce que la mesure que vous faites, que vous mettez en place va être efficace pour atteindre la fin qui est visée. Si ce n'est pas efficace pour atteindre la fin visée, bien, on fait une collecte qui est superflue ou qui est arbitraire de renseignements personnels, et donc, à partir de ce moment-là, on ne devrait pas la faire parce que ce qu'on n'a pas à collecter, on ne le collecte pas. Donc, l'efficacité est déterminante. Là, même si je ne suis pas placé pour l'évaluer, elle est déterminante parce qu'elle vient assurer le respect du principe de finalité de l'application et prévenir des collectes qui seraient superflues, excessives ou inutiles de renseignements personnels.

Mme Rizqy : O.K., merci. Et je continue exactement dans la même veine, parlons du stockage, deux affaires. Premièrement, à qui appartient la donnée? À l'utilisateur? À l'État? Aux développeurs de l'application? Première question. Deuxième sous-question : Le stockage, voulez-vous nous en glisser un mot, de ce que vous en pensez?

M. Déziel (Pierre-Luc) : Oui, absolument. Bien, c'est une question avec laquelle on est souvent confrontés : À qui appartient la donnée? En fait, il n'y a pas de droit de propriété sur un renseignement personnel, ce n'est pas quelque chose... on ne peut pas être propriétaire de ça. C'est quelque chose qui fait partie de nous, de notre liberté individuelle, donc on n'est pas propriétaire, ce n'est pas un bien qu'on peut commercialiser ou vendre.

On parle, en termes de lois sur la protection des renseignements personnels, de contrôle sur les renseignements. Donc, moi, j'ai un contrôle sur mes renseignements personnels, là, puis ce contrôle-là, c'est ce qui garantit ma liberté. Il s'opérationnalise entre autres avec le consentement, et, quand je le transmets à quelqu'un, il va être sous son contrôle. Donc, s'il est dans un serveur, bien, les personnes qui ont ce serveur-là, c'est un renseignement qui est sous leur contrôle, et donc ils ont des obligations qui vont découler des lois sur la protection des renseignements personnels par rapport à ce contrôle-là. Donc, on ne parle pas de propriété, mais on parle de contrôle.

Sur les serveurs, bien, c'est sûr que l'idéal, c'est que ça soit stocké dans des serveurs qui sont en sol québécois, canadien, sur lesquels on a un contrôle qui est aussi physique, finalement...

• (16 h 20) •

Mme Rizqy : Puis qui appartient au gouvernement du Québec?

M. Déziel (Pierre-Luc) : Qui appartient au gouvernement du Québec, oui.

Mme Rizqy : Parfait. Je vais aller rapidement parce qu'il me reste 30 secondes.

M. Déziel (Pierre-Luc) : Oui, je comprends.

Mme Rizqy : Désolée.

M. Déziel (Pierre-Luc) : C'est des questions qui sont complexes, quand même, c'est pour ça que...

Mme Rizqy : Là, j'ai failli oublier ma question. J'ai un trou de mémoire... Ah!

M. Déziel (Pierre-Luc) : Bien, je peux continuer, si vous voulez, sinon.

Mme Rizqy : Non, non, j'allais poser la question... Ah oui! Les pénalités. Lorsqu'il y a des fuites, trouvez-vous que nos lois ont assez de mordant, ou on devrait aller plus loin au niveau des pénalités?

M. Déziel (Pierre-Luc) : Bien, c'est...

Le Président (M. Bachand) : Rapidement, s'il vous plaît.

M. Déziel (Pierre-Luc) : Les lois actuelles n'ont pas du tout assez de mordant. Le projet de loi n° 64 est intéressant, mais, vous en discutiez ce matin, est-ce que... pour moi, c'est des gros chiffres, mais vous êtes plus experte que moi sur ce sujet-là. Est-ce que c'est assez gros quand même? On en reparlera éventuellement, c'est ça, mais c'est une amélioration, mais, pour le moment, c'est complètement insatisfaisant, ça, c'est clair, absolument. Merci à vous.

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

M. Nadeau-Dubois : Bonjour. J'ai très peu de temps.

M. Déziel (Pierre-Luc) : Je vais aller vite.

M. Nadeau-Dubois : Je vais vous bousculer un peu.

M. Déziel (Pierre-Luc) : Parfait. Je suis prêt.

M. Nadeau-Dubois : Dans l'état actuel du cadre juridique au Québec, si rien ne change — le projet de loi n° 64 n'est encore, pour le moment, qu'un projet de loi — jugez-vous que le tout est en place pour protéger la vie privée des Québécois, Québécoises, si une application calquée sur celle du fédéral était mise en place au Québec?

M. Déziel (Pierre-Luc) : Non, pas nécessairement. Voulez-vous que je développe?

M. Nadeau-Dubois : Est-ce que vous diriez qu'il y a des risques significatifs pour la vie privée des Québécois, si on allait dans ce sens-là?

M. Déziel (Pierre-Luc) : Ça dépend comment... Évidemment, ça dépend comment on défendrait... on définirait «significatifs», mais il pourrait y avoir des risques, oui.

M. Nadeau-Dubois : O.K. À la quatrième recommandation, vous dites... vous recommandez que l'application soit désactivée si son efficacité ne peut être scientifiquement démontrée. Je comprends que ce n'est pas votre compétence que de déterminer si l'application... si l'efficacité est scientifiquement démontrée. La grande majorité des experts nous ont fait... vous avez entendu les témoignages comme moi, nous ont donné comme témoignage que l'efficacité n'était pas démontrée. Dans ce contexte-là, qu'est-ce que vous recommandez, qu'on active ou qu'on n'active pas une telle application au Québec?

M. Déziel (Pierre-Luc) : Bien, je pense que la solution fédérale offre quand même une solution qui est assez intéressante. C'est-à-dire qu'il y a une configuration qui est différente, hein, il y a des... peut-être que ça va fonctionner, peut-être que ça ne va pas fonctionner, mais qu'il faut la surveiller très rapidement et désactiver si ce n'est pas nécessaire... bien, si ce n'est pas efficace.

La protection de la vie privée, une des facettes à prendre en considération pour savoir si on va de l'avant ou pas... Donc, ça serait un peu problématique pour moi de répondre en vous disant est-ce qu'on va de l'avant ou pas, en ne regardant que la vie privée, finalement.

M. Nadeau-Dubois : Et, si on... Parce que vous comprenez qu'il peut y avoir aussi un problème de dire : On l'essaie puis, si on voit qu'il y a des problèmes, on la désactive. Est-ce qu'une manière de contourner ce problème-là ne serait pas de procéder à des tests, par exemple, pour s'assurer de l'efficacité puis ensuite généraliser l'application? Est-ce que, du point de vue de la vie privée, ce ne serait pas plus prudent, comme manière de procéder, de commencer par des tests avant de généraliser?

M. Déziel (Pierre-Luc) : Je serais d'accord avec cette affirmation-là, oui.

M. Nadeau-Dubois : Parfait. Merci beaucoup.

M. Déziel (Pierre-Luc) : Ça me fait plaisir. Merci à vous.

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

M. Ouellet : Merci beaucoup. Donc, à mon tour de vous accueillir. Je voudrais aller rapidement sur la recommandation 8. Vous dites que «le gouvernement du Québec devrait veiller à mettre en place une stratégie efficace de distribution et d'analyse [de] tests à la COVID-19 afin de s'assurer que l'application ne s'avère pas contre-productive». J'aimerais vous entendre sur cette affirmation. Ce n'est pas votre champ d'expertise, mais vous dites : Faites attention, si vous allez de l'avant avec ça, il va falloir qu'on ait des tests, il va falloir qu'ils soient disponibles parce que ça pourrait être contre-productif. J'aimerais avoir votre regard.

M. Déziel (Pierre-Luc) : Bien, effectivement, je m'avance toujours un petit peu en dehors de mon champ d'expertise, mais qui continue sur cette idée de l'application mobile puis de son efficacité, finalement. C'est-à-dire que c'est des choses que vous avez discutées depuis hier, l'application, ce quelle va faire, c'est d'essayer de demander aux gens de les notifier d'une exposition potentielle puis leur demander d'aller se faire tester, leur demander d'aller passer des tests puis d'avoir une réponse rapide aux tests. Et puis donc l'application va être efficace si ce mécanisme-là est mis en place de manière productive, de manière efficace.

Ma crainte, pour en avoir parlé avec d'autres collègues, parce qu'on a travaillé un peu sur les applications de traçage aussi... bien, en fait, beaucoup plus sur les applications de traçage et sur les applications de notification, c'est les dangers relatifs à l'anxiété et à l'inquiétude. Puis, encore une fois, le point sur lequel j'appuie, celui de la confiance. Donc, si moi, je reçois une notification qui dit : Tu es à risque, vas te faire tester, puis j'arrive, je ne suis pas capable de trouver... je ne suis pas capable de me faire tester, les résultats arrivent très rapidement, bien là, peut-être que je commence à perdre un petit peu confiance puis à dire : À quoi elle me servait, l'application, finalement? Donc, c'est un des éléments dans une solution beaucoup plus large, beaucoup plus systémique.

Et puis il y a une interdépendance, à mon sens, entre les différentes efficacités. Donc, l'efficacité de l'application va être... va aller aussi loin qu'il va y avoir une efficacité, finalement, au niveau des tests. Donc, c'est... Et sinon on va commencer à nourrir, peut-être, cette méfiance-là, peut-être nourrir cet inconfort-là, cette anxiété-là puis là on va... ça risque d'être contre-productif, dans une certaine mesure.

M. Ouellet : Donc, si je comprends bien, pour améliorer la confiance des individus dans l'application... ou le désir du gouvernement que les individus téléchargent l'application, le gouvernement devrait affirmer très fermement : Ayez confiance en cette application parce que, si vous êtes notifié, vous aurez accès à un test rapidement qui va vous permettre d'être testé, et donc il n'y aura pas augmentation d'anxiété. Est-ce que vous voulez aller aussi loin que ça? Parce que vous dites «devrait veiller à mettre en place», mais on va un peu plus loin, là. Est-ce que le gouvernement devrait lui-même annoncer que, des tests, il y en aura, la rapidité sera au rendez-vous?

M. Déziel (Pierre-Luc) : Je pense que c'est important, mais je pense qu'il faudrait dire : Puis on est prêts pour les tests aussi. Je ne pense pas, par contre, là — puis je n'ai pas réfléchi à ça avant, on en parle maintenant — qu'il faille dire : Si vous avez l'application, vous allez avoir un accès plus rapide aux tests. Là, on tombe dans des questions que vous avez évoquées jusqu'à hier. Ce n'est pas tout le monde qui va avoir l'application. Est-ce que c'est une voie rapide pour les tests, avec l'application? C'est peut-être jouer un petit peu sur des enjeux qui sont très dangereux. Puis de commencer à mettre des conditions pour... ou en tout cas de «nudger», comme on dit, les personnes de manière peut-être un peu trompeuse vers l'application... Donc, je ne pense pas... je pense qu'il faut être prêts pour la stratégie, mais qu'il ne faut pas dire : Il y a une voie rapide pour les tests quand vous avez l'application. C'est très dangereux, à mon sens.

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

M. Ouellette : Effectivement, je vais faire un peu de pousse là-dessus, parce qu'effectivement, dans les milieux urbains, si vous donnez l'impression que, si vous avez l'application vous allez avoir accès à des tests, bon, tous les gens en milieu rural ou en région peuvent se sentir désavantagés.

Vous évalueriez la confiance de la population, au moment où on se parle, là, prête à recevoir une application complémentaire, comme le gouvernement s'apprête à l'appeler, ou il y a encore beaucoup de travail à faire? Parce que, tout le long de votre présentation, la confiance de la population, pour vous, à part de la définition des renseignements personnels, là, c'est le critère numéro un, la confiance de la population. Est-ce que vous évalueriez que la confiance de la population, présentement... la population est prête à ça?

M. Déziel (Pierre-Luc) : Bien, moi, au lieu de m'en remettre à mon intuition, je vais m'en remettre à... Il y a des sondages que je cite dans mon mémoire, un sondage Léger qui est sorti le 11 août, donc avant-hier, finalement, qui montrerait, si je me rappelle bien, là, il y a les chiffres dans le mémoire, que c'est... 54 % des Canadiens qui ont été interrogés ne font pas confiance que l'application Alerte COVID ne collecte pas de renseignements personnels. Donc, 54 %, même si on leur dit : On ne collecte pas des renseignements personnels, n'ont pas confiance qu'effectivement l'application ne collecte pas de renseignements personnels.

Donc, je pense qu'il y a un travail à faire. Des gens ont peur, peut-être... c'est des métriques qu'on trouve à travers la littérature sur la protection des renseignements personnels, les gens n'ont ni confiance au gouvernement, ni confiance, de manière générale, aux entreprises, ni aux universitaires ou aux chercheurs aussi. Dans le contexte de la confiance, c'est vrai, il y a tout le temps un travail à faire. Donc, ce 54 % là, pour moi, il est assez significatif, et ça rejoint les enjeux que je discutais un petit peu plus tard de ne pas essayer de cacher qu'on collecte des renseignements

personnels, de ne pas leur dire : On ne collecte pas de renseignements personnels, parce que, de toute façon, il y a une majorité de la population qui ne le croit pas. C'est un sondage qui est sorti, Léger, hier. Il faudrait voir la méthodologie aussi, mais ils n'ont pas l'habitude de faire n'importe quoi.

M. Ouellette : Effectivement, il faudrait voir la méthodologie. À plusieurs reprises, j'ai eu l'impression que vous aviez des doutes. Vous nous dites «si on va de l'avant», «si on va de l'avant». Ça pourrait-u arriver qu'on n'en ait pas besoin?

M. Déziel (Pierre-Luc) : Est-ce qu'on n'en a pas...

Une voix : ...

M. Déziel (Pierre-Luc) : Bien, c'est ça, mais ça pourrait tout à fait arriver. Je pense qu'il faut garder... Dans n'importe lequel processus délibératif ou décisionnel, il faut éviter les oeillères puis garder toutes les opinions ouvertes. Je pense que c'est le but de la discussion, aujourd'hui, puis des audiences que vous tenez depuis hier, et de la consultation publique qui a été ouverte. C'est sûr que, si on se dit : C'est sûr qu'il faut aller de l'avant, bien, ce n'est pas peut-être pas l'attitude, en tout cas, qu'il faut adopter quand on réfléchit à ces choses-là. Je pense qu'il faut tout le temps garder un esprit ouvert puis dire : Ça se peut qu'on arrive à la conclusion qu'on n'en a pas besoin, de l'application.

Encore une fois, moi, je pense que ce qui va être important à la fin de tout ça, c'est encore cette question de confiance qui va être importante à travers le processus de la gestion de la crise, au-delà de la question des renseignements personnels, c'est d'expliquer les décisions. Je pense qu'il va falloir que ça soit clair, puis je pense que ça a été précisé ce matin, je pense que c'était peut-être... je ne m'en rappelle plus, qui l'a précisé, mais peu importe ce qu'on va... en tout cas, je parle un petit peu comme ça, je ne veux pas avoir l'air... mais quelle décision on va arriver... il va falloir qu'elle soit justifiée puis qu'on l'explique. Si on prend une application, il faut l'expliquer, expliquer comment elle fonctionne, pourquoi est-ce qu'on l'a choisie, celle-là, pourquoi est-ce qu'on l'a choisie parmi d'autres. Si on arrive à se dire : On n'utilise pas d'application, il va falloir l'expliquer aussi. C'est toute une question de transparence puis de dire : On s'est basés sur tels critères, là on est arrivés à cette décision-là. Puis, à partir de ce moment-là, c'est là qu'on nourrit cette confiance-là aussi.

Le Président (M. Bachand) : Merci beaucoup, M. Déziel, de votre participation, ça a été très intéressant. Sur ce, je suspends les travaux quelques instants. Merci infiniment.

(Suspension de la séance à 16 h 31)

(Reprise à 16 h 36)

Le Président (M. Bachand) : À l'ordre, s'il vous plaît! Bonjour. La commission reprend ses travaux.

Nous avons le plaisir d'accueillir, maintenant, les représentants de l'Association québécoise des technologies, soit Mme Nicole Martel et M. Alain Lavoie. Comme vous savez, vous avez 10 minutes de présentation, et par après nous aurons un échange avec les membres de la commission. Encore une fois, bienvenue, et la parole est à vous. Merci.

Association québécoise des technologies (AQT)

Mme Martel (Nicole) : Merci. Alors, merci, merci de nous accueillir aujourd'hui. Je suis Nicole Martel, présidente-directrice générale de l'Association québécoise des technologies. Je suis accompagnée de M. Alain Lavoie, qui est président d'une entreprise technologique, Irosoft, également membre de notre conseil d'administration à l'AQT, pour diminuer un peu la longueur du nom.

Alors, ça nous fait plaisir de venir partager nos réflexions par rapport au projet en question, donc le déploiement d'une application mobile pour lutter contre la COVID-19. On espère que nos recommandations, nos positions sont en mesure d'apporter un éclairage à vos réflexions et qu'elles aideront le gouvernement à mener à bien ce projet tout en considérant les préoccupations qui sont perçues par l'industrie.

Sans détour, je dirais que, dans mon quotidien à la tête de l'Association québécoise des technologies depuis plusieurs années, je suis constamment à la découverte de nouvelles solutions qui aident des entreprises qui aident les humains, donc j'ai un a priori favorable face aux technologies et le potentiel qu'elles ont pour aider les individus, bien sûr, si elles sont bien développées et bien encadrées, naturellement.

Donc, jusqu'à maintenant, vous avez reçu plusieurs experts en matière de protection de vie privée, d'éthique, de cybersécurité. On a eu la chance d'entendre quelques-uns de ces témoignages, qui étaient fort éclairants. Nous allons donc concentrer nos recommandations autour de deux grands thèmes, soit la gouvernance et les communications, les communications pour bien expliquer l'outil. Donc, pour nous, il s'agit de mettre en place des conditions qui sont gagnantes pour le déploiement de l'application et faire en sorte que la technologie soit au service de l'humain.

En débutant, peut-être préciser le rôle de l'AQT et la composition du secteur des technologies de l'information. Donc, l'écosystème des TIC, là, est composé d'entreprises de toutes sortes d'expertises. Ça peut être des entreprises

en télécommunication, les équipements, les services informatiques, bien sûr, les logiciels. L'expertise québécoise est reconnue, ce n'est pas en reste, elle est reconnue sur la scène mondiale. D'ailleurs, deux tiers des entreprises membres de l'AQT ont des ventes hors Québec. C'est des entreprises qui... une empreinte chez des clients aussi prestigieux que la Maison-Blanche, n'en déplaise à nos voisins, mais, bon, des clients tous plus prestigieux les uns que les autres, signe, dans le fond, de la pertinence de nos produits.

Nos solutions québécoises visent tous les secteurs d'activité économique, que ce soit le secteur financier, la santé, les grandes entreprises manufacturières, la gestion des données, pour n'en nommer que quelques-uns. On utilise ces technologies-là à tous les jours, dans notre quotidien. C'est transparent à nous, et c'est tant mieux, c'est ce qu'on veut. Au Québec, on dénombre près de 2 000 entreprises qui, à leur tour, représentent 150 000 emplois, 150 000 professionnels qui sont dans un secteur qui est toujours en croissance et qui, quand même, se porte bien, malgré toutes les circonstances qu'on connaît actuellement.

Notre mission, à l'AQT, c'est de faire en sorte que l'environnement d'affaires soit favorable à leur croissance, et ça passe notamment par l'accès à des meilleures pratiques et par, aussi, des occasions de partenariats qu'on provoque entre les membres, soit des partenariats technologiques ou des partenariats commerciaux.

• (16 h 40) •

Donc, tel que mentionné au début, si elles sont utilisées de façon éclairée, les technologies représentent un outil de plus dans l'arsenal des moyens à notre disposition pour combattre les fléaux, dont la propagation de la COVID-19. En ce qui a trait à l'actuelle pandémie, l'ère dans laquelle nous vivons permet un avantage lorsque comparée aux époques antérieures où les moyens dont on disposait étaient plus limités. C'est notre opinion. De la façon dont nous sommes... De la même façon, on est convaincus que l'innovation peut très bien cohabiter avec la protection de la vie privée et que l'un ne doit pas se faire au détriment de l'autre. Bien au contraire, les technologies peuvent et, surtout, doivent intégrer les concepts de vie privée dès la conception. Vous avez entendu parler de ce concept-là aussi jusqu'à maintenant. Il faut veiller à ce que les technologies s'arriment aux exigences de nos sociétés. En ce sens, les paramètres technologiques devront correspondre aux plus hauts standards de protection de vie privée. On pense que le gouvernement devra veiller à ce que les conditions dans lesquelles la solution sera offerte n'outrepassent jamais les conditions d'utilisation qui auront été préalablement communiquées, question de conserver la confiance.

D'ailleurs, on profite de l'occasion pour saluer le travail de fond qui a été effectué par les équipes. Le document de consultation démontre qu'il y avait un bon travail de vigie qui avait été réalisé. Les options retenues, Bluetooth, excluant le GPS, et les données décentralisées nous apparaissent comme des choix judicieux également.

Donc, tel que mentionné plus tôt, nos deux recommandations se regroupent en deux thèmes : une gouvernance qui sera irréprochable et multi-expertises et des communications adoptant les plus hauts standards de transparence. Prenant pour acquis que l'utilisation d'une application mobile puisse véritablement aider la Santé publique et, par ricochet, la population, le gouvernement doit prendre tous les moyens pour que l'initiative soit un véritable succès. Pour ce faire, les citoyens doivent avoir une confiance inébranlable face à l'État quant à l'utilisation qui sera faite des données. Le champ d'action de l'application mobile qui sera sélectionnée doit être délimité et clairement communiqué. Le gouvernement ne doit en aucun cas se soustraire à son engagement ou encore étendre l'utilisation de l'outil à d'autres fins.

Parmi les bonnes pratiques pour un succès de projet techno, on parle souvent de bureaux de projets multidisciplinaires. Dans ce cas-ci, on recommande de créer un comité de gouvernance réunissant des membres aux expertises et provenances complémentaires, comité qui comprendrait, bien, des employés de l'État, des professionnels de l'État, des chercheurs, des juristes, des experts en protection de vie privée, des spécialistes en technologie, bien sûr, des professionnels de la santé publique pour qui on développe cet outil. L'AQT pourrait certainement y désigner des représentants. Ce comité devra établir et valider les critères de succès en amont et devra recevoir une rétroaction en continu et fournir des avis tout au long du processus. Parmi son rôle et ses responsabilités, nous recommandons que le comité s'assure, avant le déploiement de l'application, des règles claires d'utilisation, devra aussi veiller à ce que soit envisagées, voire identifiées, les situations qui justifieraient le retrait de l'application, le cas échéant. Le comité devrait aussi faire en sorte que soit précisée la durée projetée de l'application et définir le protocole de mise hors service. Le comité devrait voir au respect des accréditations pour les ressources humaines qui sont autorisées à consulter et traiter les données. Les standards canadiens nous apparaissent des standards mondialement reconnus pour ce faire. Il devrait aussi poursuivre la vigie internationale quant à l'utilisation d'outils comparables pour analyser les écueils et apporter les ajustements nécessaires au besoin.

Sur le plan de l'adhésion, bien, il va sans dire que la situation actuelle, couplée à l'utilisation d'un outil technologique, peut être propice à une augmentation de stress et d'anxiété au sein de la population, on en est bien conscients. Cet enjeu doit être sérieusement pris en compte. C'est pourquoi on recommande qu'il y ait un plan de communication et de mobilisation qui soit mis en place. Le plan devrait voir à vulgariser l'information dans une perspective d'éducation face à la population. Il faudra expliquer les caractéristiques technologiques liées aux préoccupations, qui sont fort légitimes, de la part des citoyens, par exemple que les données sont anonymisées — on l'aime, ce mot-là, «anonymisées» — qu'il y a absence de localisation GPS, que les données résident sur les appareils des utilisateurs, et ainsi de suite. Ce plan de communication pourrait avoir un double objectif et informer la population de leur exposition face à leur utilisation d'outils, je dirais, grand public, qui sont déjà sur leurs appareils, les appareils auxquels ils ont possiblement accordé des autorisations soit de localisation ou autres, bien souvent à leur insu, par méconnaissance ou manque de littératie numérique. L'angle éducatif ne devrait certainement pas être négligé, puisque les projets technologiques seront omniprésents dans le futur, et il est important pour le Québec d'encourager la population à devenir des citoyens numériques plus avisés.

Pour illustrer sa transparence, le gouvernement devrait communiquer les progrès au niveau de la mise en place de l'outil, son adoption, ses retombées, notamment au niveau de la prise en charge rapide des personnes à risque, et des invitations à se faire tester rapidement pour limiter la propagation. Depuis le début de la pandémie, on a pu observer que la population était très intéressée à être informée, puis la population collabore aussi, puis elle ajuste ses comportements en conséquence puis face aux diverses éventualités, donc on pense qu'elle serait réceptive à des messages comme ceux-là. L'objectif ultime sera de mobiliser le plus grand nombre de citoyens, d'organisations qui sont susceptibles d'encourager l'adoption de l'outil par la population.

Donc, en résumé, nous sommes convaincus que l'utilisation des technologies est un outil de plus dans l'arsenal déjà existant des moyens dont on dispose pour lutter contre la pandémie. Ça ne remplace aucun des moyens existants. L'innovation n'exclut pas la protection de la vie privée si les conditions et les paramètres sont bien définis et bien encadrés.

Puis je terminerais en disant que la médiatisation d'écueils survenus dans les grands projets technologiques par le passé... il peut être vrai de penser que la population nourrit un certain cynisme à l'égard d'un tel projet, de projets technologiques en général. Donc, qu'on se le tienne pour dit, le succès de ce projet fera foi des projets à venir. Si le gouvernement va de l'avant, on n'a pas le droit à l'erreur. Advenant qu'on accuse des ratés par rapport à l'application et à l'utilisation des données, ça pourrait avoir des retombées extrêmement négatives sur la confiance de la population et sur la perception de notre industrie et des entreprises qui la composent. Un échec pourrait également compromettre la viabilité d'autres projets numériques d'envergure, qu'ils soient privés ou publics. Bref, nous sommes condamnés à réussir. Nous avons le devoir de tout mettre en place ensemble pour favoriser cette réussite et ainsi permettre d'aider la Santé publique à circonscrire cette crise sanitaire. L'industrie québécoise des technos tend la main, et on espère pouvoir poursuivre les échanges avec vous. C'est le fruit de nos réflexions aujourd'hui.

Le Président (M. Bachand) : Merci infiniment pour votre présentation. Je me tourne vers la députée de... non, de Beauce-Nord, M. le député, pas «la députée». M. le député de Beauce-Nord, pardon.

M. Provençal : Merci, M. le Président. C'est parce que je ne suis pas habitué d'occuper cette place-là, c'est pour ça. Alors, merci beaucoup. Comme l'ensemble des gens qui viennent nous déposer de l'information, c'est très intéressant de regarder la paire de lunettes que vous avez face à ce dossier-là. Il y a différents éléments, et, d'entrée de jeu, vous parlez d'arrimage, dans votre document, en arrimage, technologie, concept de vie privée puis... versus les bénéfices attendus, mais est-ce que vous avez une idée des ficelles qu'on pourrait utiliser pour bien réussir cet arrimage-là? Ça serait ma première question.

M. Lavoie (Alain) : Écoutez, on fait des recommandations, dans le mémoire, par rapport à mettre un comité qui pourrait être en place, qui pourrait faire un suivi en continu par rapport à ça, faire de la vigie au niveau international parce que c'est un «working in progress», excusez l'expression, mais c'est une cible mouvante qui... en continu. Il faut être alertes, il faut qu'autant du point de vue du gouvernement que du point de vue des comités externes on puisse avoir cette transparence-là puis qu'on puisse agir en fonction de ça. Comme on le dit dans notre mémoire, il faut avoir des règles d'engagement, hein, comment on s'y prend pour le mettre, mais comment on s'y prend pour sortir de là en cas de risque, c'est quoi, les règles de désengagement par rapport à ça. C'est toutes des choses qu'on a mises en place dans les recommandations.

Donc, plusieurs types de comités, là, qu'il pourrait y avoir, des comités interministériels, des comités avec l'externe aussi, avec des spécialistes, comme on le recommande, des comités citoyens qui pourraient être à l'intérieur de ça, mais qu'on ait une grande transparence. Parce que tout le monde est de bonne foi, je pense, à l'intérieur de ça, et ce qu'on veut, le but du jeu, c'est qu'à partir du moment où il y a quelqu'un qui est détecté avec la COVID on puisse retracer le plus rapidement possible les gens qui ont été en contact avec cette personne-là et être en mesure, donc... Mais ça prend des encadrements, ça prend des balises, et on... sans rentrer dans les détails de ça, parce qu'on n'est pas dans tous les détails, mais on pense que le gouvernement et les fonctionnaires ont fait leur job, autant au point de vue canadien que québécois, par rapport à ça et encadrer ça.

• (16 h 50) •

M. Provençal : J'aurais un deuxième élément, parce que, tout à l'heure, dans votre présentation, vous avez dit : On n'a pas le droit à l'erreur. Et d'ailleurs, dans votre mémoire, à un moment donné, vous mentionnez qu'on n'a pas le droit d'avoir un dérapage de ça parce que ça pourrait... on pourrait avoir une perte de confiance énorme envers tout ce qui est de la technologie numérique puis les organisations qui... Et, quand je regarde les recommandations que vous avez mises, entre autres les recommandations n° 5 à 8, est-ce qu'on ne peut pas dire... est-ce qu'on peut dire, excusez-moi, que ces recommandations-là ne pourraient pas être la base pour éviter, justement, un dérapage? Parce que vous parlez de «vulgariser l'information», d'«expliquer les caractéristiques technologiques» — je lis juste le début, là — «communiquer les progrès» au niveau de la technologie puis «mobiliser le plus grand nombre d'organisations», alors, personnellement, quand je lisais l'ensemble de votre document, j'avais l'impression que vous faisiez un lien entre ces recommandations-là, 5 à 8, et la notion des outils qui pourraient nous éviter un dérapage, pour employer le terme que vous aviez dans votre document.

Mme Martel (Nicole) : Bien, je peux répondre. Dans le fond, les recommandations 5, 6 à 8 sont vraiment pour faciliter ou comment engager une meilleure adhésion de la population. Les dérapages, il y a toutes sortes de moyens de se prémunir de dérapages, puis vous avez des spécialistes, aussi, qui sont venus vous le mentionner, donc

c'est de faire des tests constamment sur des intrusions, des tentatives d'intrusion, de faire... de tester l'application constamment. C'est ce que toutes les grandes organisations, petites organisations font aussi avec leurs systèmes parce qu'il y a toujours des gens qui seront malveillants puis qui vont essayer de trouver des failles dans le système. C'est d'être très, très, très à l'écoute, très alerte puis de constamment bonifier la solution puis s'assurer qu'elle soit extrêmement robuste. C'est, malheureusement, toujours du «work in progress» aussi... pas malheureusement, mais c'est le propre de l'industrie des technologies, il faut constamment être alertes puis avisés puis surveiller qu'il n'y ait pas de fuite ou de...

M. Lavoie (Alain) : Si je peux compléter, c'est une préoccupation qu'on a, parce qu'il faut se rappeler, là, pour... on est là-dedans depuis longtemps, il faut se rappeler que les technologies de l'information n'ont pas toujours eu bonne presse, on a eu de la misère à aller recruter des gens, à une période. Avec l'avènement de l'intelligence artificielle, ça nous a donné un «boost» dans notre domaine. On a un beau momentum pour les gens pour aller en technologies de l'information et on veut... Puis aujourd'hui on parle de ça, mais, dans trois, quatre, cinq ans, on va parler des voitures autonomes qui s'échange des données qui... plein d'autres choses. Donc, ce qu'on veut, c'est qu'on prenne les... aujourd'hui, c'est la première étape d'une multitude d'étapes qu'on va travailler avec les données, puis il faut prendre des bonnes décisions à ce moment-là. Puis le dérapage, pour nous, serait désastreux, on reviendrait comme cinq ans ou 10 ans à l'arrière, et ça, ça ne serait pas une bonne nouvelle pour notre industrie.

M. Provençal : Dernière question, parce que je veux laisser du temps à mes collègues. Vous mentionnez, dans votre document : «Pour alimenter nos réflexions, il est nécessaire d'établir certaines hypothèses qui nous permettront de bien circonscrire les enjeux», et là vous émettez cinq hypothèses. Quand je lis chacune de vos hypothèses, est-ce que ces hypothèses-là ne définissent pas, en même temps, le profil de l'outil qu'on devrait mettre en place?

Mme Martel (Nicole) : Dans le fond, on est partis aussi de vos... des hypothèses du document de base, c'est-à-dire qu'on prendrait le choix d'une technologie Bluetooth plutôt que d'une technologie qui utiliserait les localisations GPS. Donc, c'est les hypothèses qu'on a reprises aussi. Mais la première hypothèse, pour nous, c'est la plus importante, c'est la définition du besoin par la Santé publique. Donc, il faut que ça serve la Santé publique, donc, pour nous, c'est la base, c'est la base de tout. On souhaite que ces gens-là soient sur le comité de gouvernance également, qu'ils soient aux premières loges pour nous dire est-ce que ça facilite le travail ou pas. Parce qu'en ce moment on travaille peut-être avec des blocs-notes, des listes de numéros de téléphone, mais est-ce que cette application facilite ou non le travail? Donc, c'est les hypothèses avec lesquelles on a bâti les recommandations.

M. Provençal : ...que vous avez défini le tout, au tout départ, comme étant un outil.

Mme Martel (Nicole) : Parmi les autres outils. Donc, on va écouter le Dr Arruda, on va continuer de garder la distanciation, se laver les mains, tousser dans notre coude, mais on va avoir un outil de plus, peut-être, qui va combler... bien, compléter l'arsenal ou, en fait, l'enrichir.

M. Provençal : Merci.

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

Mme Boutin : Bonjour, Mme Martel, M. Lavoie. Je suis très contente que vous soyez ici. J'ai trouvé votre rapport très intéressant, parce qu'on entend toutes sortes de groupes, puis ils nous amènent dans toutes sortes de directions, vous, vous êtes très dans le pratico-pratique, très, très concret, surtout au niveau de tous les dispositifs à mettre en place, la gouvernance.

Moi, j'ai souvent des questions par rapport à ça, puis, tu sais, il y a une réflexion, puis comment est-ce qu'on réalise ça, puis ça s'applique à cette application-ci, si... advenant un cas qu'on va de l'avant, ou à d'autres applications futures. Tu sais, c'est des réflexions qu'il faut avoir. Puis, dans les dispositifs à mettre en place, vous avez mentionné un processus de gouvernance de données. Bon, vous avez aussi parlé du protocole de mise hors service, c'est hyperintéressant, mais, le processus de gouvernance de données, est-ce que vous pourriez m'en parler un peu plus? C'est des questions qu'on a.

M. Lavoie (Alain) : Bien, écoutez, c'est un processus qu'on retrouve généralement en architecture d'information — qu'est-ce qu'on va faire de ces données-là? Où ils circulent dans l'appareil? Qui va y toucher? À quel moment il va y toucher? — avoir la chaîne de possession, essentiellement, de savoir qui a fait quoi avec quoi dans ces choses-là. Donc, c'est dans ce contexte-là qu'on parle de gouvernance de données, donc s'assurer qu'on sait qui travaille avec quoi et qui est habilité à faire les choses avec les données, essentiellement, et que ce ne soit pas juste : On capte la donnée puis n'importe qui peut embarquer. Donc, c'est ça, quand on parle de gouvernance de données.

Mme Boutin : Donc, c'est déterminer qui est en charge de la donnée, qui la stocke.

M. Lavoie (Alain) : C'est ça.

Mme Boutin : Puis vous pensez que le gouvernement du Québec devrait faire quoi? Comment on devrait procéder?

M. Lavoie (Alain) : Oh! comment? Bien, comme d'habitude. Le gouvernement a des processus, il y a même une loi qui l'oblige à faire... à s'assurer d'avoir... par exemple, si on regarde au niveau archivistique, savoir quand est-ce qu'on détruit, quand est-ce qu'on garde, comment on le met. Si on regarde au niveau de la Sûreté du Québec, où des choses... ils ont des processus pour savoir comment chemine la donnée. Il y a des normes aussi, essentiellement, pour s'assurer par rapport à ça. Donc, c'est... je pense que le gouvernement est habitué à faire ces choses-là.

Ce qu'on dit, c'est que ça prend un plan de match, là-dessus, et des habilitations. Ce n'est pas juste de la technologie, là, qu'on parle, c'est des humains aussi, c'est qui va toucher à ces données-là, puis s'assurer que les personnes qui y touchent, parce que... vont être habilitées, puis on va savoir qu'ils y ont touché. Donc...

Mme Boutin : ...la gestion des accès aussi.

M. Lavoie (Alain) : Pardon?

Mme Boutin : Donc, on parle aussi de la gestion des accès.

M. Lavoie (Alain) : Oui, gestion des accès, mais aussi ça va en amont, à savoir... par exemple, moi, je suis classifié secret, par exemple, au niveau du gouvernement, j'ai le droit de voir de la donnée secrète, donc c'est des types de classifications qui doivent... des habilitations qu'on parle pour avoir accès à cette information-là pour ne pas que ça soit, excusez-moi, un zoo, là, où tout le monde prend la donnée comme il veut, il faut que ça soit encadré. Puis c'est quand on dit : Il faut bien le faire, il faut le faire... oui, le faire mais le faire correctement. Donc, il faut prendre ces dispositions-là, et je suis convaincu, et on est convaincus que le gouvernement a toutes ces habilités-là pour le faire et s'assurer que la donnée va être bien protégée à ce niveau-là.

Mme Boutin : J'ai une autre question par rapport à l'efficacité, puis c'est une question que... tu sais, on peut la réfléchir de manière pragmatique. Est-ce qu'on l'a étudiée au niveau des indicateurs? Puis, dans votre rapport, vous aviez mis... vous avez parlé du Dr Amesh — c'est sûr que je massacre son nom, là, excusez-moi — un chercheur de l'Université Johns Hopkins, qui dit : Il n'y a pas vraiment de chiffre magique qui dit un niveau. Tu sais, à quel moment est-ce qu'une application est jugée efficace? Moi, je me pose la question. Puis là il dit : Quels sont les indicateurs? Est-ce que c'est le nombre de vies humaines? Est-ce que c'est le nombre de personnes qui vont adhérer à l'application? Puis on se pose ces questions-là.

Moi, ma question sur l'efficacité : Est-ce qu'on devrait la tester en amont pour être certains que ça fonctionne puis peut-être perdre du temps avant qu'il y ait des gens qui pourraient l'utiliser... si c'était efficace, ou la tester en temps réel? Tu sais, c'est toutes des questions qu'on doit se poser.

• (17 heures) •

M. Lavoie (Alain) : On va revenir sur l'histoire de... le but du jeu. Le but du jeu, c'est de permettre, à partir d'un moment que quelqu'un a été détecté COVID, de trouver l'entourage et de circonscrire ça. Donc, c'est une fonction multi-objectifs. Donc, par exemple, si je pogne la COVID, je vais... il y a quelqu'un qui va me tester, je vais aller voir la Santé publique, puis la Santé publique va dire : Qui tu as vu? À quel moment tu l'as vu?, ainsi de suite. Donc, il y a une enquête qui est faite, essentiellement, par rapport à ça.

Bon, en ce moment, c'est la Santé publique qui le fait. Il y a un outil, qui peut être un cellulaire, mais on pourrait prendre aussi bien... imaginez, là, que Dr Arruda demande à tout le monde de prendre un calepin puis, quand il se déplace, il prend des notes où il se déplace, qui il a vu, à quel moment, puis, quand la Santé publique va m'appeler, bien, on lui dit : Regarde, on prend ça, puis on va essayer de s'en souvenir... parce que moi, je n'ai pas de mémoire, puis je ne me souviens pas, puis je prends mon petit calepin, parce que j'ai été correct puis je l'ai pris. Bien là, on a peut-être une application qui n'est peut-être pas aussi efficace qu'on le voudrait, mais qui est capable de garder... puis, moi, si je suis détecté COVID, bien, on peut l'utiliser comme un outil de plus. Donc, la fonction objective, c'est de trouver à 100 %, avec plusieurs moyens, dont un de ces moyens-là est une application... un autre moyen, c'est peut-être le petit calepin, puis un autre moyen, c'est peut-être une enquête qui est faite autrement, mais l'idée, c'est d'aller vers le 100 % le plus possible.

Bon, ceci dit, il faut s'assurer que, si on y va avec la technologie, ça va beaucoup plus vite qu'avec le calepin, mais ça va beaucoup plus vite s'il y a une fuite de données, ça peut partir très vite. Donc, c'est pour ça qu'on dit, il faut le faire comme il faut, parce que, s'il y a un risque, il y a un balancement à faire entre l'outil qui amène un poids dans la fonction objective qui est de 100 %, qu'on veut amener... qu'on veut maximiser, puis le risque que la donnée soit en fuite, mais il faut prendre les moyens pour s'assurer que les données sont encryptées, que c'est fait selon les règles de l'art, que les spécialistes ont pu voir le code, essentiellement, pour le faire. Donc, il faut aller dans ce sens-là pour être en mesure... puis, en termes d'efficacité, si c'est un pourcentage aussi minime, comme le docteur disait dans sa recherche, bien, c'est déjà du bonus, si ça amène un petit peu plus.

C'est dans ce contexte-là et selon cette hypothèse-là qu'on dit : Si on y va, c'est parce que la Santé publique pense que ça peut l'aider véritablement. Si la Santé publique ne sait pas quoi faire des données que ça va collecter, bien là, on a un problème. Donc, c'est dans ce sens-là que nous, on voit la perspective de ce projet-là en version...

Puis en même temps, bien, il y a toute la question... en informatique, tout le monde sait, il y a la gestion du changement. La gestion du changement, bien, il faut s'occuper de la population pour bien les éduquer pour s'assurer qu'ils comprennent ce qu'on est en train de faire. Ça va?

Le Président (M. Bachand) : Mme la députée de Les Plaines, 1 min 20 s.

Mme Lecours (Les Plaines) : Bon, très rapidement, écoutez, bien, justement, quand on parle de gestion du changement, je voulais vous demander par rapport... justement, est-ce que ça pourrait être un frein, le fait qu'il y a des gens... on parle de 77 % de la population qui est munie d'un cellulaire, d'un téléphone quelconque, qui soit... Bon, dans ce 77 %, là, il y en a qui n'utilisent pas beaucoup d'applications, etc. On sait aussi que les gens âgés, qui ont été affectés, n'ont pas de cellulaire. Par contre, les jeunes, beaucoup l'ont et, effectivement, l'utilisent à toutes sortes de... Est-ce que ça pourrait être un frein ou... Le fait qu'il y a des gens qui n'ont pas de cellulaire, donc qui n'utilisent pas nécessairement ces applications-là, est-ce que ça pourrait être un frein ou, au contraire, le fait que ça va se répandre, si la population est bien informée, ça va se répandre sur le type d'utilisation?

Mme Martel (Nicole) : ...vous voulez savoir?

Mme Lecours (Les Plaines) : Oui, oui. On est condamné au succès, vous l'avez dit.

Mme Martel (Nicole) : Oui, c'est ça. Pour nous, il faut toujours le voir comme un des outils dans notre coffre à outils. Donc, on a plusieurs moyens, ça, c'en est un de plus. Je sais, on s'est beaucoup penché sur cette question-là aussi, à savoir les personnes les plus démunies, les personnes âgées, les personnes peut-être un peu plus vulnérables qui n'ont pas d'accès au cellulaire. On pense quand même que, si on arrive à stopper la... freiner la propagation ou, enfin, limiter la propagation, bien, ça va moins affecter, par exemple, les personnes âgées. Parce qu'on le sait, les travailleurs qui rentraient dans les CHSLD sont ceux qui, souvent, ont contaminé les personnes âgées. Donc, si ces personnes-là ont un appareil, qu'ils l'ont téléchargée, qu'ils l'ont mis en application, bien, peut-être que ça va éviter de propager le virus. Donc, pour nous, c'est un moyen qu'on doit conserver.

Il faut quand même trouver d'autres outils. Il faut continuer à chercher. Ce n'est pas une fin en soi, l'outil technologique, parce que, oui, il faut s'occuper de nos personnes les plus vulnérables, puis, en effet, ce n'est pas les personnes qui vont être couvertes par cette technologie-là, mais il faut faire aussi autre chose pour eux.

Le Président (M. Bachand) : Merci beaucoup. Je cède maintenant la parole à la députée de... Saint-Laurent, pardon.

Mme Rizqy : Merci beaucoup. Bonjour et bienvenue. Ça fait quand même plusieurs années que vous existez, n'est-ce pas?

Mme Martel (Nicole) : ...30 ans cette année.

Mme Rizqy : Félicitations! Dites-moi, est-ce que qui que ce soit du fédéral vous a contactés pour, justement, susciter votre expertise ou celle de vos membres? Parce que vous regroupez énormément de personnes. Est-ce qu'il y a eu un réflexe Québec?

Mme Martel (Nicole) : Non. D'ailleurs, je tiens à saluer le fait qu'il y a une consultation qui est faite au Québec, parce que je pense qu'il n'y a pas beaucoup de juridictions qui ont fait des consultations en amont, donc, non, absolument pas.

Mme Rizqy : Dans le fond, c'est que je me demande... c'est que j'ai l'impression que, lorsqu'on parle de technologie, on regarde souvent ce qui est fait ailleurs, mais on ne regarde pas ce qui est fait dans notre cour. Et moi, je suis à Saint-Laurent, comme vous le savez, tout comme vous, et, au niveau des technologies, je comprends que le fédéral est allé, on dirait, de façon très naturelle vers Toronto et que, même — hier, on recevait M. Yoshua Bengio — ça a été écarté. Mais je veux revenir... Au fond, si je comprends bien, on n'a pas eu le réflexe Québec.

Et j'aimerais, une autre affaire, vous demander... Avant de rentrer dans l'application, vous avez parlé d'arsenal. J'ai fait la visite de chez CAE, puis il existe quand même plusieurs autres outils. Notamment, CAE, oui, c'est une grosse multinationale, mais qui fait affaire avec plusieurs fournisseurs québécois. Et, par exemple, au niveau de la gestion de l'équipement, on peut voir très bien que, lorsqu'un employé prend un appareil sanitaire, bien, immédiatement, il y a un compteur, puis on sait d'avance que, O.K., il faut remplir la commande, et ça se fait.

Est-ce que ça serait quelque chose qui aurait pu être utile autant au niveau fédéral, pour la réserve sanitaire fédérale, que même pour chez nous, au Québec, pour un jour savoir, en temps pratiquement réel, ce qu'il nous manque pour préparer en amont une pandémie?

M. Lavoie (Alain) : Vous nous envoyez des... Premièrement, nul n'est prophète dans son pays. Ça, c'est la première chose que je vous dirais. Puis la deuxième chose, je vous dirais, vous nous envoyez une pelure de banane, mais c'est correct, mais, essentiellement, les technologies de l'information, on a beaucoup... moi puis l'AQT, on

préconise beaucoup le savoir-faire québécois, tu sais, puis on s'en rend compte, on est à l'international. Moi, personnellement, notre compagnie, on s'en rend compte, on est à l'international et on se rend compte que les gens nous aiment, là. Les gens au Québec, là, on a une bonne expertise.

Puis essentiellement, écoutez, c'est sûr qu'il y a du monde qui peuvent aider, c'est... On n'a pas été impliqués dans le choix, on ne veut pas prendre de position sur qui pourrait le faire ou qui ne pourrait pas le faire, mais, essentiellement, je peux vous dire qu'on a du bon savoir-faire québécois.

Mme Rizqy : On a l'expertise, là.

M. Lavoie (Alain) : Au Québec? Oui.

Mme Rizqy : Parfait. Je vais reprendre la pelure de banane, si vous permettez. Alors, je continue, là, je ne veux pas perdre mon fil conducteur, puis moi, il ne me faut pas grand-chose pour perdre mon fil conducteur. Dites-moi... Je l'ai perdu.

M. Lavoie (Alain) : ...

Mme Rizqy : Quelle morale! Non, le pire, c'est que j'avais vraiment une question spécifique. Ah! ça va me revenir. Bon, alors, je vais aller à ma prochaine question.

Vous avez aussi parlé de bien encadrer pour avoir le lien de confiance et tout ça. Nous, on a eu la Commission d'accès à l'information, la Commission des droits de la personne et des droits de la jeunesse, la Ligue des droits, bref, plusieurs experts nous disent clairement que le cadre législatif actuel, il n'a pas de mordant, là, il nous en manque. On a un projet de loi n° 64 qui s'en vient, qu'on n'a pas encore débattu, qu'on a... mais, clairement, là, c'est clair et unanime de ceux qu'on a entendus, les experts en droit de la protection des renseignements personnels, que ça nous prend un meilleur processus, un meilleur cadre juridique.

Pensez-vous qu'on peut regarder l'Ontario, faire ce qu'ils font, en ce moment, avec l'application, et, nous, peut-être travailler activement, et on peut même... bien, on nous a même dit, ce matin, de procéder par décret pour avoir un cadre juridique avant de lancer une telle application pour, justement, avoir cette confiance tant recherchée? Pas une autre pelure de banane, j'espère?

M. Lavoie (Alain) : Bien, c'est parce qu'on n'est pas juristes, là, non plus, on ne peut pas se prononcer sur la loi, là. Puis on va se revoir en commission parlementaire sur le projet n° 64.

Mme Rizqy : Mais là vous allez devoir aussi vous prononcer. Tôt ou tard, vous allez devoir vous prononcer. O.K. D'accord.

Bien, ma question de tantôt, j'ai oublié. Donc, il n'y a pas eu de réflexe Québec. Là, présentement, on comprend que le fédéral lance une application Alerte COVID qui est développée par des employés de Shopify. Nous, Shopify, évidemment, on a tenté tant bien que mal de les avoir, ils ne sont pas là. Trouvez-vous que, si jamais on va de l'avant, il ne serait pas impératif d'avoir, justement, des entreprises qui, lorsqu'elles lancent des applications, elles viennent nous jaser et nous expliquer leurs applications? Et, par conséquent, est-ce qu'on devrait exclure ce type d'entreprises étrangères qui ne sont pas devant nous aujourd'hui pour s'expliquer?

Mme Martel (Nicole) : Bien, c'est absolument impératif, c'est une relation de confiance qu'on doit avoir avec le fournisseur. Est-ce que c'est dans le cadre d'une commission? Ça aurait été bien parce que ça aurait permis d'éduquer les parlementaires puis la population aussi, c'est de l'information publique. Donc, oui, absolument, puis il faut avoir des échanges comme on aurait avec tout autre fournisseur.

M. Lavoie (Alain) : ...des recommandations de communication.

• (17 h 10) •

Mme Rizqy : Vous avez parlé d'éducation, j'adore ça, de littératie numérique. Présentement, moi, je cherche et je fouille, et il n'y en a pas beaucoup, de littératie numérique et aussi accessible pour le grand public. Est-ce que c'est quelque chose que vous êtes capables de développer? Je connais déjà la réponse, là, mais je vous laisse quand même répondre.

Mme Martel (Nicole) : Bien, oui, on pourrait certainement collaborer. Il y a d'autres organismes, aussi, qui peuvent le faire puis avec... J'ai vu que les campagnes qu'on a lancées récemment avec la COVID étaient de nature beaucoup à se rapprocher des citoyens. C'est beaucoup d'illustrations, et tout ça, puis les citoyens sont réceptifs.

La période dans laquelle on vient de passer, le dernier trois mois, on a fait un bond de géant de presque deux ans d'avancées en matière d'utilisation des technologies de l'information. Donc là, il y a une certaine avidité à mieux comprendre les technologies puis il y a beaucoup de choses qui se font à l'insu des usagers. C'est allé vite, là. On a des appareils mobiles, on télécharge une application de restauration rapide, là, woups! on passe devant un restaurant, on a un rabais, on dit : Ah! c'est le fun. Mais il y a des impacts à ça, puis je pense qu'il faut que les gens comprennent les impacts de leur utilisation de leur téléphone puis des réseaux mobiles, et tout ça.

Donc, oui, il faut créer des citoyens numériques responsables. Les jeunes à l'école, au secondaire, qui disposent d'appareils électroniques, c'est aussi la vocation des professeurs, donc, absolument.

M. Lavoie (Alain) : Puis notre industrie est déjà impliquée dans ça puis qui essaie de faire des choses. Je nommerais pour ça CyberCap, qui est une autre organisation pour laquelle je me suis impliqué pendant de nombreuses années, qui va chercher des jeunes au secondaire puis qui essaie... et au primaire puis qui fait des séances pour les amener à s'éduquer là-dessus, Academos, que peut-être que des gens connaissent aussi.

Donc, notre industrie s'implique, et l'industrie est très, très, très préoccupée aussi par les talents. Donc, on veut les... on veut, dès le jeune âge, les préparer, pas juste pour notre industrie, mais pour que ça puisse s'imprégner, parce que plus il va y avoir de monde qui va utiliser le numérique, plus ça va être bien pour l'industrie des technologies.

Mme Rizqy : Je me demande... Il ne me reste pas beaucoup de temps, donc je vais poser mes deux questions rapidement. Est-ce que vous avez pu observer l'Australie, l'Islande, le Singapour et la France, qui ont utilisé la technologie Bluetooth et que, finalement, ont arrêté, notamment en Australie, parce que, même, ça interférerait avec le travail déjà fait par la Santé publique? Est-ce que vous avez pu observer, là-bas, pourquoi ils se sont arrêtés et voir quelles lacunes qu'on doit vraiment avoir devant nous pour s'assurer de ne pas reproduire les mêmes erreurs? Premièrement.

Et, deuxièmement, vous avez parlé d'un protocole de mise hors service. Qu'est-ce qu'il devrait absolument contenir?

Mme Martel (Nicole) : Bien, d'abord, c'est la Santé publique, je pense, qui doit être celui qui... comme, quand ils annoncent les confinements, les déconfinements, c'est la Santé publique qui doit déterminer c'est quoi, le protocole de mise hors service. Ce qu'il devrait contenir, c'est des critères... Est-ce qu'on est à la fin de la pandémie? Est-ce qu'on rencontre ou non les objectifs attendus?

M. Lavoie (Alain) : Est-ce que ça génère trop de faux positifs? Ça peut être un paquet de facteurs, mais je pense que c'est aux experts de déterminer c'est quoi qui... à quel moment, puis on est... Nous, on est au niveau de la technologie, mais on n'est pas au niveau de la Santé publique. C'est eux, les experts qui vont nous dire...

C'est un outil, là, hein, c'est un outil d'aide à la décision. Peu importe ce que vont faire les outils alentour de ça, ça va être un humain qui va prendre les décisions, à la fin. Et donc c'est... il faut que la Santé publique s'assoie avec des experts, avec des gens pour leur dire : Bien, voici les critères de désengagement qu'aussitôt on va prendre. Le gouvernement pourrait en décider un autre aussi, la population pourrait en suggérer, mais essentiellement il faut qu'il y ait des critères de désengagement, parce que, nous, ce qui nous préoccupe, c'est le dérapage, et ça... Et, à partir du moment où on sent qu'il y a un dérapage potentiel, bien, il faut regarder comment on s'y prend puis mettre ça dans la balance avec la Santé publique, avec les gens qui peuvent mourir. Essentiellement, c'est ça, et aussi la protection des renseignements personnels, les développements économiques, tout ça est ensemble, mais c'est des experts du gouvernement et de la Santé publique qui prendront les décisions.

Mme Martel (Nicole) : Juste pour revenir un petit peu sur votre question sur l'international, on a vu, je pense, un... je ne me souviens plus dans quel pays à l'international, on avait une application de base qui avait certaines fonctionnalités, puis le pays a décidé que, ah! ça serait le fun si elle faisait ça aussi, là, la reconnaissance visuelle, et tout ça. Donc, c'est pour ça que nous, on dit : Il ne faudrait jamais, au grand jamais, qu'une application qui soit proposée à la population outrepassse le champ... le carré de sable, le champ d'expertise ou le champ d'application qui était préalablement mentionné. Donc, cette application x là va faire ça, puis, si on veut faire autre chose plus tard, on fera autre chose.

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

M. Nadeau-Dubois : Merci, M. le Président. Bonjour, monsieur. Bonjour, madame. Merci d'être avec nous cet après-midi.

J'ai peu de temps. J'ai, essentiellement, une question pour vous. Vous vous êtes dit, puis je le comprends bien, préoccupés par la confiance des gens envers votre industrie. Puis j'ai lu dans votre mémoire... puis, Mme Martel, vous l'avez mentionné, vous avez dit que vous redoutez que, si ça se passe mal, il y ait des contrecoups, en anglais on dirait un «backlash», puis que votre industrie en soit la victime. Et un des critères que vous établissez, dans votre mémoire, pour que ça se passe bien, puis c'est à la page 8 de votre mémoire, c'est repris à la recommandation, également, numéro 8, vous dites : «[L'importance de] mobiliser le plus d'acteurs de la société possible [...] de façon à appuyer l'initiative[...], obtenir le plus grand consensus.»

Ça fait l'objet d'un vif débat, une potentielle application, là, depuis plusieurs mois. La Ligue des droits et libertés a fait signer une déclaration par une centaine d'organisations syndicales, communautaires, sociales, citoyennes. Il y a la... Je vous dirais que, du côté de la deuxième opposition, on a beaucoup de questions. Si ces oppositions-là se maintiennent et si... et j'ajoute une hypothèse, si un ou plusieurs partis d'opposition s'opposent clairement à la recommandation d'une telle application, est-ce que vous jugez qu'il y a... ce serait trop controversé et que, donc, on devrait peut-être se garder de mettre en place une telle application ou est-ce qu'au contraire le gouvernement pourrait, malgré cette opposition, aller de l'avant? Qu'est-ce qui serait le mieux pour votre industrie, une application fortement controversée et on se retient ou une application controversée et on va de l'avant?

M. Lavoie (Alain) : En fait, la première chose qu'il faut dire, c'est que ce n'est pas qu'est-ce qui est le mieux pour notre industrie, ce qui est mieux pour la Santé publique. Ça, c'est la première réponse qu'on donnerait. Et que... Et ensuite ce qu'on veut, c'est que les décisions qui seront prises feront que notre industrie va pouvoir évoluer dans le futur. Mais la première chose, le premier objectif : Est-ce qu'on va sauver des vies? Est-ce qu'on va aider la Santé publique à ça? C'est ça qui est plus préoccupant pour nous dans le contexte actuel.

M. Nadeau-Dubois : ...qui mettez dans votre mémoire ce critère d'un plus large consensus possible. Je vous dis, on peut douter que ce critère-là, aujourd'hui, soit rempli. Si je vous dis : Il y a des bonnes chances qu'on ne le remplisse pas, ce critère du consensus large, comment vous réagissez à ça?

Mme Martel (Nicole) : Bien, je vais vous dire, on a des technologies québécoises qui sont utilisées sur la planète Mars, en orbite un peu partout, donc on est capables de respecter les plus hauts standards de confidentialité, tous les outils le permettent. Donc, je pense qu'il faut s'assurer de bien communiquer cette information-là. Il faut rassurer la population que ça peut être fait, avoir toujours les garde-fous pour dire : Bien, s'il y a méprise ou quoi que ce soit...

M. Nadeau-Dubois : ...malgré tout ça, on n'y arrive pas puis que les oppositions se maintiennent?

M. Lavoie (Alain) : Écoutez, c'est très hypothétique, d'une part. Puis, d'autre part, je vous dirais que — mon petit hamster va très, très vite dans ma tête — ça va dépendre de la deuxième vague. Je vous dirais que, écoutez, sincèrement, là, c'est un outil dans le coffre à outils qui peut aider, puis même si les gens se mettent... mais qui peut aider, mais qui peut éviter... qui peut aider à éviter une autre catastrophe, si on repart sur une deuxième vague, puis que le développement économique tombe, puis que... Ce n'est pas juste notre industrie. C'est la Santé publique, c'est l'industrie, c'est un balancement qu'il faut trouver et il faut le trouver, cet équilibre-là, puis on trouve que...

Moi, là, je prends... on prenait l'exemple de l'égoïne, là, pour construire sa maison, bien, si tu prends l'égoïne, ça va aller plus lent pour la construire que si tu prends une scie électrique, mais tu peux te blesser avec la scie électrique. Ça peut arriver que tu te blesses aussi, mais l'idée, là-dedans, c'est que la technologie peut aider à sauver des vies.

M. Nadeau-Dubois : Merci beaucoup. Vous mettez, dans votre mémoire, le critère du...

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

M. Ouellet : Merci beaucoup. À mon tour de vous saluer. Je veux vous remercier pour la qualité de votre mémoire. Vous prenez... Vous avez pris le temps de mettre une annexe qui résume les faits saillants et le fonctionnement de plusieurs applications à travers le monde, et surtout vous avez produit... en tout cas, vous nous présentez un tableau, je ne sais pas si c'est vous qui l'avez produit, SensorTower, sur l'adoption des contacts de traçage par les pourcentages de population, puis on a, en un coup d'oeil, qu'est-ce qui a été fait ailleurs au pays, puis on voit qu'on est en bas de 21 %; notamment, en Australie, c'est plus élevé, à 21,6 %.

Donc, est-ce que, pour vous, ça serait important que le gouvernement du Québec... parce que vous faites référence... puis le collègue de Gouin en faisait référence, tout à l'heure, l'importance de votre industrie, d'avoir un... pas nécessairement une bonne image, mais il ne faut pas se tromper, si on lance quelque chose, pour que ça fonctionne parce que ça pourrait effectivement faire reculer votre industrie.

Donc, ma question : Est-ce qu'il serait pertinent que le gouvernement annonce déjà ses couleurs en disant : Pour aller de l'avant, pour que ça fonctionne puis pour que les gens aient confiance, voici le chiffre qu'on aurait besoin d'avoir, c'est-à-dire il faudrait un taux d'approbation, ou de téléchargement, ou de mise en application à l'application de 50 %, 60 %, 70 %? Est-ce que vous voudriez que le gouvernement annonce ses couleurs pour ce qui est de son indication à aller de l'avant ou pas avec une application?

• (17 h 20) •

Mme Martel (Nicole) : Juste avant de répondre précisément à cette question-là, je veux juste ouvrir une parenthèse. C'est vrai qu'on a peur que ce soit dommageable pour notre industrie s'il y avait un écueil, mais on a peur pour les avancées, aussi, pour la profession, pour les avancées, parce que, bon... tu sais, on n'a qu'à penser au système de paye Phénix. Tu sais, on nourrit un cynisme par rapport aux technologies puis on a les technologies constamment avec nous. Donc, je pense qu'il faut avoir des gains, des succès pour éviter de continuer à nourrir le cynisme. Je voulais juste faire cette parenthèse-là. Puis nos entreprises ne sont pas concentrées exclusivement sur leur image, là, ce n'est pas ça du tout, du tout que je voulais qui transparaît par mes propos.

Par rapport à l'indicateur, que le chiffre devrait être annoncé, et tout ça, ça revient un petit peu à la question de la députée de Jean-Talon, je crois, au début, il doit y avoir un certain nombre d'indicateurs. Nous, on aime beaucoup les tableaux de bord. Donc, est-ce que la mesure devrait être le nombre d'alertes qu'on a réussi à intercepter ou le nombre de propagations qu'on a réussi à intercepter? C'est peut-être ça, l'indicateur, ce n'est peut-être pas le taux d'adoption, parce que ça dépend dans quelle région c'est fait. Si l'adoption se fait en Gaspésie, bon, puis on a un 80 % d'adoption en Gaspésie, on n'aura pas les mêmes résultats que si on a 20 % d'adoption à Montréal. Donc, je pense... et c'est peut-être un mélange de quelques chiffres, mais, dans le fond, ce qu'on veut, ultimement, c'est bloquer des propagations.

M. Ouellet : ...ce qui est important, c'est que, au-delà de la gouvernance qui devrait être mise en place, ces indicateurs-là, ce fameux tableau de bord du succès ou de ce que l'application peut nous dire soit divulgué pour dire : Voici ce que ça donne, voici les informations qu'on a réussi à obtenir, voici la complémentarité de cet outil à travers tout ce qu'on fait, et ça, ça pourrait travailler sur la confiance et peut-être amener d'autres utilisateurs à télécharger l'application pour dire : Bien, écoutez, quand je vois ce que ça donne, ce que ça fait, j'ai confiance, donc j'embarque dans ce grand consensus.

Mme Martel (Nicole) : Oui, c'est ce qu'on pense.

Le Président (M. Bachand) : M. le député de Chomedey.

M. Ouellette : Merci. Bien, bonjour à vous deux. Effectivement, si on parle du tableau de bord, il faudra que ça soit basé sur la science. Vous avez une confiance très grande — je ne dirais pas «illimitée», mais je dirais «très grande» — à la Santé publique, puis la Santé publique, c'est basé sur la science. Normalement, plusieurs décisions gouvernementales sont, malheureusement, basées sur des sondages. Le tableau de bord, il faudra qu'il soit factuel et basé sur des données scientifiques de la Santé publique. C'est parce qu'on peut bien avoir la solution qu'on voudra, si on n'a pas les bonnes prémisses de base, on risque de se ramasser devant un mur ou on risque, un moment donné, d'avoir certains problèmes.

Vous avez une appréhension, et on la sent, on la sent en vous lisant, on la sent dans vos propos, pas sur des dommages directs — ça ne sera pas de votre faute directement, l'application ne vient pas de chez vous, ne vient pas de vos gens ou des gens de l'industrie, elle vient d'ailleurs — c'est des dommages collatéraux que vous allez avoir ou que vous pourriez avoir et, particulièrement, une perception que la population va avoir, si ça ne marche pas.

Tous les experts qu'on a eus depuis hier, là, à date, on n'en a pas, de place où ça a marché. Je ne vous dis pas que ça ne marchera pas, parce qu'on va être défaitistes, là, mais tous les experts qu'on a eus depuis hier, toutes les applications ont toutes des problématiques, puis on n'a pas trouvé la solution miracle encore.

M. Lavoie (Alain) : O.K. Je vais me permettre... je m'excuse, le pourcentage, là, que ça marche ou ça ne marche pas, là, ça, c'est... on l'a dit, là, c'est... tout ce qui va être positif va être positif, O.K.? Ça, c'est la première chose qu'on amène.

Ce qui risque... par rapport à ce que vous avez dit par rapport à ce qui pourrait être dommageable, c'est plus le dérapage. C'est que ce n'est pas... dans la fonction objective qu'on disait, ce n'est pas que ça ait mené à un 3 %, ou un 5 %, ou un 10 %, c'est qu'il y ait eu une catastrophe, une fuite de données, qu'il y ait eu de quoi qui fait que ça paraît très mal. C'est plus ça qui nous préoccupe plus.

Quand on dit : Il faut faire bien les choses, il faut s'assurer que la confiance, surtout que c'est fait par le gouvernement... un lien de confiance, quand même, un gouvernement, bien, c'est... Donc, il faut que ça... il ne faut pas qu'il y ait des erreurs à ce niveau-là. Puis à la suite de ça vous comprenez que, s'il y a un dérapage, quand on va tomber... dans deux, trois ans, quand on va tomber à d'autres choses, ça peut avoir des effets collatéraux importants sur le développement économique, c'est ça qu'on dit.

Le Président (M. Bachand) : Sur ce, je tiens à vous remercier infiniment pour votre participation à la commission, ça a été très intéressant.

Alors, je suspends les travaux quelques instants. Merci beaucoup.

(Suspension de la séance à 17 h 25)

(Reprise à 17 h 30)

Le Président (M. Bachand) : À l'ordre, s'il vous plaît! Merci.

Donc, je souhaite la bienvenue à M. Steve Waterhouse, expert en sécurité informatique, que plusieurs connaissent. Je vous rappelle, M. Waterhouse, que vous avez 10 minutes de présentation, et après ça on aura un échange avec les membres de la commission. Merci beaucoup d'être présent aujourd'hui. La parole est à vous.

M. Steve Waterhouse

M. Waterhouse (Steve) : M. le Président, merci beaucoup. Messieurs dames, c'est un honneur et privilège de me présenter... présenter le contenu ici puis parler un peu du gros bon sens avec la technologie. Je vais passer l'introduction parce qu'on veut aller au vif du sujet. Vous avez tous devant vous le mémoire, avec d'où est-ce que je proviens, de la Défense... et maintenant que je suis consultant et formateur dans la vie de tous les jours.

Alors, 2020 a débuté sans que tout le monde ne se doute qu'elle marquerait l'évolution de notre société. Tous les scénarios que j'ai déjà étudiés pour préparer des systèmes d'information, ou des entreprises, ou des ministères que j'avais sous ma responsabilité, bien, celui de la fonction bactériologique, de se préparer contre ça, a toujours été sous-considéré et sous-estimé. Et, tel que constaté ces derniers mois, il y a des pratiques de base qui doivent être maintenues, telles que la gestion sécuritaire de l'information, et peu importe le contexte.

À partir de Tel-Aviv, en Israël, à la fin 2020, j'étais avec une délégation internationale de journalistes et de professionnels en sécurité de l'information, et peu se souciaient comment se développait la situation en Chine, qui dégénérerait à chaque jour. Il était facile à comprendre qu'à moins de fermer toutes les frontières terrestres, aériennes et maritimes, tous les pays seraient affectés en peu de temps, ce qui est arrivé, d'ailleurs. À mon retour au pays, devant le «buildup» de la situation en février, peu, aussi, se préoccupaient de cette continuité des opérations en cas d'isolement total, le scénario extrême, et surtout comment continuer le travail au quotidien.

Dans un contexte nucléaire, bactériologique, radiologique et chimique, que j'ai travaillé dans le passé, bien, la détection de contextes extrêmes de destruction avec du radiologique, du nucléaire ou du chimique, c'est plus facile à documenter, à discerner. Mais, en plein hiver, durant la saison de la grippe et du rhume, le bactériologique est quand même moins évident à percevoir. Alors, comment anticiper et documenter ce nouveau risque, et surtout comment continuer à travailler malgré cela?

Au début mars, alors que tous les cas en Europe se multipliaient rapidement, les pays avec une gouvernance plus ferme se sont tournés vers le service policier ou de renseignements pour voir comment suivre les infectés et ceux considérés non infectés, qui sont difficiles sans les tests, car peu ou pas de signes apparents. Les outils de traçabilité de première instance considérés à ce moment sont, évidemment, le thermomètre frontal à l'arrivée à l'aéroport, mesure utilisée lors des cas de contamination passés par le SRAS, le MERS et d'autres, le suivi par GPS, par téléphone cellulaire puis la caméra thermique, comme on a vu apparaître dans les épiceries ici, à Québec, d'ailleurs. Or, l'efficacité de ces moyens est limitée. Les thermomètres ont été prouvés et classés comme inefficaces à détecter les asymptomatiques. Quelqu'un peut ne pas faire de température et être porteur d'un virus, quel qu'il soit, et, après coup, même chose avec les caméras thermiques.

Cependant, les autorités de la Santé publique, devant aucun moyen de détection, ont choisi l'isolement, bien sûr, et les mesures de quarantaine. Dès le début, la question essentielle était sur toutes les lèvres : Comment assurer que les gens en quarantaine ou qu'un moyen... c'est-à-dire qu'un citoyen déclaré positif COVID-19 demeure isolé tout en respectant la confidentialité des renseignements personnels et sa vie privée? Alors, qu'est-ce qui devrait être fait? La commission d'éthique des sciences et des technologies a publié un rapport, à la fin avril, élaborant bien les considérations fondamentales en matière de protection de la vie privée et de la protection des renseignements personnels. Ce sont là des très bonnes bases pour le développement éventuel d'applications de recherche numérique de contacts, aussi appelées, comme vous le savez, de notification d'exposition. En partant de cette réflexion, les programmeurs ont des lignes directrices raisonnables pour démarrer la conception.

Cependant, la technologie étant ce qu'elle est, il y a matière à bien comprendre les enjeux quant aux limites de cette technologie. Sans dériver trop dans le catastrophisme, il y a quelques préoccupations quant aux limites des applications de recherche numérique de contacts ou bien, encore là, de notification d'exposition énumérées par le *Canadian Medical Association Journal*, qui sont résumées en cinq points, qui sont : un, l'efficacité des applications, qui dépend de leur adoption par la population — puis on parlera des chiffres tout à l'heure; les technologies qui sous-tendent les applications comportent des erreurs de mesure qui limitent l'efficacité à identifier les contacts; trois, les approches basées sur la technologie Bluetooth, qui n'utilisent pas le système Apple-Google — ou GAEN — seront limitées par les restrictions de balayage Bluetooth pour les téléphones intelligents fonctionnant avec iOS; quatre, de manière générale, par rapport à la recherche manuelle de contacts, la surveillance constante à grande échelle au moyen d'applications de recherche de contacts soulève plus de problèmes en ce qui concerne la protection des renseignements personnels; et, cinq, même si des études de modélisation ont laissé entendre que les applications de recherche de contacts permettaient de réduire la transmission, aucune étude n'a été publiée à ce jour.

Or, la Linux Foundation a colligé une majorité des méthodes de conception des applications et des documents de données, ainsi que les pays qui les utilisent, tel qu'illustré à l'annexe A, qui est ce tableau, ici. Certains de ces pays se sont pourvus de la méthode GPS pure et dure, comme le Bahreïn, le Koweït, la Norvège, l'Israël, même certains autres, comme l'Inde, ils en faisaient partie, et la Corée du Sud — j'allais l'oublier — alors que certains modèles plus orientés vers la protection de la vie privée et du renseignement personnel sont développés dans le cadre de GAEN, donc Google-Apple Exposure Notification. Malgré les différentes méthodes employées, seulement 9,3 % de la population parmi les 13 pays les plus peuplés de la planète a adopté une application soit de suivi, de notification ou d'exposition. Certains scientifiques ont avancé qu'il doit y avoir un taux d'adoption entre 60 % et 70 % dans la population pour avoir un résultat efficace, alors que certains autres mentionnent que seulement 15 % à 20 %, c'est suffisant. Les faits sont quand même éloquentes, alors que seulement cinq pays des 22 sondés, selon la référence, ont franchi la barre du 15 % d'adoption.

Le 31 juillet dernier, l'application canadienne COVID Alert a vu le jour... est un produit développé à partir du cadre GAEN et du code COVID Shield, contrairement à l'application albertaine ABTraceTogether, déployée le 1er mai, qui, elle, est basée sur le modèle déployé au Singapour, appelé TraceTogether, utilisant le protocole BlueTrace, donc Bluetooth avec une autre façon de le documenter. Comme vous avez pu voir aussi, le 9 août dernier, bien, l'Alberta va canner, comme on dit, son application et va s'en remettre à l'application canadienne. Le taux d'acceptation lorsque l'application de l'Alberta est sortie, c'était 5,3 % après trois mois d'opération, alors que COVID Alert, après six jours, était de 4 %. Le choix que l'Ontario et le gouvernement du Canada ont fait d'utiliser la technologie GAEN et COVID Shield semble rencontrer ce que désirent les citoyens et les commissaires à la protection de la vie privée et des renseignements personnels, c'est-à-dire de réduire au minimum les risques de fuites d'informations personnelles et d'identification des utilisateurs.

Alors, qu'est-ce qui peut mal aller? Bien, la fiabilité du signal Bluetooth, comme vous avez parlé ardemment depuis les deux derniers jours, est à retenir comme étant peu exemplaire en termes de précision, considérant

l'emplacement de l'appareil et de par la nature de la transmission omnidirectionnelle du Bluetooth. Il y a quelques mois, le collège de Trinity, à Dublin, en Irlande, a produit deux évaluations qui démontrent comment le signal se propage et la précision des résultats dans des environnements variables, incluant à l'intérieur de bâtiments, de pièces et même dans des autobus. La fiabilité du signal Bluetooth est à retenir... Oups! Excusez, ça, je l'ai lu.

Outre l'imprécision qu'offre la technologie Bluetooth, fondamentalement, les appareils opérant à partir des systèmes d'exploitation Android ont été démontrés... avec des façons de faire innées dans ce système d'exploitation laissant couler de l'information qui permet d'identifier l'utilisateur plus facilement. Ces failles, reconnues par Google, ne seront corrigées qu'à la prochaine version, soit Android version 11, vers la fin du mois de septembre. Il s'agit d'un facteur quand même assez important à considérer, car cela représente près de la moitié des utilisateurs au pays et à peu près 80 % des utilisateurs au monde... qui permettrait de les identifier dans l'utilisation de... avec cet appareil-là et qui seront, à ce moment-là, plus accessibles... moins identifiables, c'est-à-dire, avec les appareils iOS d'Apple.

Il y a aussi des considérations de nuisance malicieuse, évaluées à peu probables, qui pourraient se produire avec la technologie Bluetooth par induction d'interférence, puis ça, c'est au quotidien que vous avez du wifi qui... 2,4 gigahertz, des moniteurs de bébé, des caméras de surveillance, qui peuvent venir rendre la bande du 2,4 difficile à utiliser par le Bluetooth à cause de cette fréquence à 2,4 gigahertz et qui est toujours susceptible d'être interférée n'importe où.

On parle des attaques de personification, appelées BIAS, envers son protocole, évaluées aussi à peu probables, tout comme l'exploitation de la vulnérabilité du protocole Bluetooth, Bluetooth Low Energy, elle aussi évaluée à peu probable de se matérialiser. Par contre, tous les protocoles, les attaques avec les vieux protocoles, comme Bluebug, Bluesnarfing, Bluejacking ou Bluesmack, sont à toutes fins impraticables depuis la version 4 de Bluetooth sur les appareils modernes. Donc, les risques sont faibles de voir réussir des attaques avec ces vulnérabilités-là.

Alors, je propose que... Selon mes recherches, il y a trois choix qui s'offrent : un, développer, pour le MSSS, le service de santé, une application ou s'arrimer avec un modèle d'application déjà en production, tout en demeurant indépendant — ce choix implique l'isolation des données en provenance de l'extérieur, puisque les citoyens qui visitent d'autres lieux ou des pays auront à utiliser d'autres applications; b, de joindre l'initiative fédérale afin d'assurer la continuité d'échange des données, surtout pour l'interopérabilité entre les provinces; et, c, bien, simplement ne pas investir dans le développement et l'administration d'applications de notification d'exposition et continuer le suivi manuel comme c'est actuellement.

• (17 h 40) •

Une note comme ça, la Norvège, en juin dernier, a suspendu l'usage de son application sur les bases de faible taux d'infection dans le pays et du risque élevé de compromission à la vie privée citoyenne, tout comme le Royaume-Uni, l'Allemagne et l'Australie, qui vivent des difficultés techniques avec ces applications, remettent en question les résultats perçus.

Considérant l'absence de moyens fiables pour détecter ledit virus COVID-19, préalablement mentionnée, en considérant les besoins de connaître les tendances immédiates à anticiper ce qui est à venir, et considérant les cinq facteurs énoncés par le CMAJ, et surtout en considérant les failles technologiques présentes et à venir... pour miner la vie privée et les renseignements personnels du citoyen, je suis d'avis pour opter pour l'option c.

Dans l'éventualité que le choix d'utiliser une application de notification d'exposition soit considéré et décidé, je recommande l'option b, qu'elle soit retenue afin de rapidement effectuer le déploiement et assurer aux Québécois et aux autres citoyens du pays l'échange d'information nécessaire afin que tous soient avisés de leur niveau de risque d'infection.

En conclusion, ma crainte la plus grande dans la mise en circulation de ces applications demeure la diminution de la vigilance des gens, qui ne voudront se fier que sur l'avertissement procuré par l'application de notification d'exposition lors de contamination possible et qui vont, à ce moment-là, laisser tomber leurs bonnes pratiques de mesures d'hygiène de base, telles que le port du masque, le lavage des mains et la distanciation physique. L'application ne sera alors qu'une source de distraction davantage qu'une source d'information utile. Je suis disponible pour répondre à vos questions.

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

Mme Boutin : Merci beaucoup, M. Waterhouse, d'être ici, d'être le dernier, aujourd'hui, et non le moindre. Vraiment, j'apprécie beaucoup votre travail.

Premièrement, bien, moi, je veux aller sur deux angles, là, les risques, puis après ça sur votre choix, le choix c. On s'est beaucoup questionnés puis on a eu des préoccupations, tout le monde, ici, sur les risques de la technologie Bluetooth, parce que... bien, en fait, vous le savez, là, le gouvernement, même, fédéral, si... advenant qu'on aille dans une application, c'est le choix pour assurer la plus grande protection de vie privée, comparativement, mettons, à une technologie qui utiliserait le GPS ou autre technologie plus invasive au niveau de la vie privée. Vous en pensez quoi? Parce que, là, nous, on n'est pas des techniciens puis on n'est pas des experts en informatique non plus, là. Tu sais, j'écoutais, puis j'ai lu, puis... tous les types d'attaques potentielles, puis là ils disent... C'est BlackBerry qui dit que ça va être réglé plus vers fin septembre, les failles?

M. Waterhouse (Steve) : Aucunement. C'est Google qui est à la base du système d'exploitation Android dans toutes les... la majorité... la moitié des téléphones cellulaires sur le marché, actuellement, et ils l'ont même signifié

le 31 juillet, lorsque l'application est sortie au fédéral, réaffirmant qu'ils ont la problématique en main et qu'ils vont la traiter rapidement, mais ils vont la traiter dans le prochain déploiement, soit la version 11.

Pour revenir à Bluetooth, qu'est-ce que c'est? C'est un protocole de proximité, comme les autres collègues ont déjà dit par le passé, et c'est au détriment de prendre du wifi, que... Le wifi, lui, il a une portée beaucoup plus grande en termes de collectivité, mais le Bluetooth sert bien cette fonction-là de proximité, encore là, pas juste faire une détection, mais mesurer avec un autre appareil, s'il le détecte bien. Mais, fondamentalement, ce n'est pas un protocole qui est fait pour faire de la mesure. Et, quand je dis le terme «omnidirectionnel», c'est que ça transmet 360 degrés. Donc, le téléphone peut être ici, puis j'ai le bloc de bois qui va venir atténuer le signal, tout comme j'ai du métal qui va venir réfléchir le signal dans une autre direction. Donc, c'est là que ça rend impraticable, quasiment, de faire une détection pure et simple avec garantie de qu'est-ce que ça peut donner comme résultat.

Mme Boutin : Puis qu'est-ce qui pourrait arriver de pire, admettons, en termes de piratage informatique, avec du Bluetooth, là? J'imagine que ça dépend des données qui sont... Si les données sont encryptées, c'est des données plus comme des codes aléatoires. Bien, ce qui a été développé par le fédéral, là, qu'est-ce qui pourrait arriver, là, le pire, quel scénario?

M. Waterhouse (Steve) : Bien, premièrement, les données sont déjà anonymisées. La façon que le modèle de travail... Le concept d'opération de Google, le GAEN, le Google-Apple Exposure Notification, dans ce protocole-là, les données sont anonymisées, donc, s'il y a exposition des données, c'est du code, c'est du n'importe quoi. Par contre, ce qui est le danger, c'est de venir commencer à piéger l'appareil et de faire parler l'appareil, amener l'appareil à aller sur des sites malveillants et amener l'utilisateur à donner des fausses... donner de l'information à partir d'un faux site. Donc, ce n'est pas l'application comme telle qui peut être exploitée pour deviner c'est qui, la personne, et de prendre le contrôle de ses données personnelles, mais bien les appareils eux-mêmes, qui, eux, demeurent vulnérables.

Mme Boutin : ...comme ça nous arrive tous, là, je pense que... peut-être c'est juste à moi, mais des fois on reçoit comme un faux texto, là, de Revenu Canada...

M. Waterhouse (Steve) : Mais ça, ça n'a pas rapport avec le protocole Bluetooth.

Mme Boutin : Non? Bien, ce n'est pas comme ça, dans le fond, qu'ils pourraient hacker?

M. Waterhouse (Steve) : Ça, c'est le Bluesnarfing, si mon souvenir est bon, qui est le type d'attaque qui pourrait, à ce moment-là, lancer à proximité de quelqu'un un message en provenance d'un autre téléphone sous Bluetooth. Mais ça, à partir d'une certaine version, la version 4 de Bluetooth, ça a été corrigé pour empêcher qu'il y ait des connexions indues de cette nature-là. Ça fait que, là-dessus, s'il y a à avoir de l'usurpation, du «phishing» qui peut arriver par message texte, ça n'a aucun rapport avec l'application. Par contre, on en a vu, présentement, des applications aller dans les dépôts de logiciels, le Google Play Store, l'App Store, qui étaient des fausses applications de notification, que les gens étaient appelés à «downloader» ça puis qu'ils commettent de l'information personnelle, mais l'application officielle demeure intouchée encore, là.

Mme Boutin : J'ai une question par rapport à votre décision, parce que, tu sais, nous, on pense plus en politique publique, puis à chaque fois qu'on prend une décision, c'est toujours un coût d'opportunité, on pèse le pour et le contre, on mesure les risques. Admettons, l'application peut avoir, bon, un certain risque ou un certain niveau d'efficacité, il n'y a pas d'étude qui a été prouvée... puis, bon, nous, on a décidé de consulter quand même. Il y a plusieurs pays qui ont décidé d'y aller de l'avant rapidement en prévision d'une deuxième vague, parce qu'ils se sont sûrement dit : Écoute, ça peut peut-être contribuer à sauver quelques vies humaines, puis ils n'ont jamais testé l'efficacité. Ils doivent, j'imagine, la tester. Je ne peux pas croire que certains pays ne sont pas en train... Il y en a qui ont reculé également. Là, je me dis : Soit on a une application qui est imparfaite, qui comporte certains risques, puis, d'un autre côté, quel est le plus grand risque, d'y aller ou de ne pas y aller? Si, admettons, on décide de ne pas y aller... Puis là je réfléchis, là, comme politique publique, puis peut-être que ce n'est pas une bonne réflexion, mais moi, je me la fais, cette réflexion-là. On décide de ne pas y aller, puis il y a une deuxième vague, puis on se dit — puis il y a beaucoup de cas : Ah! peut-être que ça aurait pu aider, peut-être que ça aurait été efficace, peut-être que non aussi. Est-ce que... Tu sais, si on soupèse les risques, quel est le plus grand risque, d'y aller ou de ne pas y aller?

M. Waterhouse (Steve) : Le plus grand risque, c'est d'avoir de la mauvaise information puis prendre une mauvaise décision à ce moment-là. Ça fait que, tant qu'à prendre une mauvaise décision avec des fausses informations ou des informations qui sont mal corroborées, j'ai pour mon dire de ne pas utiliser un outil comme ça au lieu d'y aller avec les rapports de la Santé publique, puis, à ce moment-là, ça, c'est de l'information qui est vérifiable.

Mme Boutin : Puis qui devrait décider d'y aller ou pas?

M. Waterhouse (Steve) : Bien, ceux et celles qui ont mis le Québec en quarantaine.

Mme Boutin : La Santé publique?

M. Waterhouse (Steve) : Pardon?

Mme Boutin : La Santé publique?

M. Waterhouse (Steve) : C'est la Santé publique, à date, qui tire les ficelles sur comment on vit, présentement. Ça fait que c'est le Dr Arruda et son équipe qui devraient, à ce moment-là, selon moi, prendre la décision dans ce sens-là.

Mme Boutin : O.K. Puis j'ai juste une dernière petite question. Advenant que le gouvernement décide d'y aller, parce qu'on a parlé beaucoup de gouvernance, de mesures d'atténuation, et tout, qu'est-ce qui devrait être mis en place en amont, au niveau de la sécurité, au niveau de la gouvernance? On a parlé de comité d'experts indépendants, on a parlé de mesures de sécurité, d'audits, de mettre en place un processus d'évaluation en continu. Est-ce que vous avez des recommandations en ce sens-là également?

M. Waterhouse (Steve) : Bien, c'est certain que ça va créer de l'emploi pour bien du monde, puis il y a bien des gens qui vont être occupés à observer ça. Mais j'ai pour mon dire, oui, si on a à développer une application, s'il y a développement de l'application, bien, il faut que ça soit fait en milieu clos, puis après ça ne pas se servir de la population comme rats de laboratoire. Excusez de dire ça comme ça, mais, présentement, c'est ça qu'on a vu et observé dans le monde.

L'Angleterre, c'est le premier exemple qui me vient en tête où est-ce que le NHS ont déployé une application puis ils se sont crucifiés du reste du monde. Puis là, après ça, le consortium Apple-Google, ils sont arrivés avec quelque chose qui respecte la vie privée des gens, puis ils ont dit : Non, non, non, ça ne vaut pas de la schnout, pour être très poli, et après ça ils sont revenus sur leur idée, ils ont dit : Bien, finalement, ça a de l'allure.

Ça fait que, donc, il faut arrêter de regarder juste dans sa petite cour et dire qu'il n'y a rien qui est bon ailleurs, oui, peut-être considérer d'autres options puis, après ça, les travailler et les essayer. Mais actuellement, avec tous les pays qu'on peut voir et la liste de tous ceux qui se sont engagés à mettre quelque chose à la population, présentement, c'est pour donner quelque chose que les gens puissent regarder. Ça fait que les statistiques qui ont passé, et passé, et repassé à la télévision, les gens en ont soupé, puis là ça serait peut-être le temps de leur servir quelque chose d'autre — c'est une réflexion comme ça, il faut comprendre — d'avoir une application. Ça fait qu'il y en a, des pays, je crois que c'est comme ça qu'ils l'ont apporté.

Si je prends, par exemple, la Corée du Sud, qui, eux, ils ont vécu beaucoup d'infections dans leur population, bien, ni une ni deux, eux autres, ils ont amendé leur constitution en 2015, puis, lorsque ça a été le temps de travailler ça au mois de mars, bien, ils ont fermé boutique puis ils ont dit : Vous installez l'application, personne ne pose de questions. Ils l'ont fait parce que la population a été non pas juste rassurée, mais ils savaient que, dès les premiers temps, c'est ça qui pourrait, à ce moment-là, être le premier canal de communication pour connaître le reste.

Mme Boutin : Eux, c'était obligatoire?

M. Waterhouse (Steve) : Comme dans beaucoup d'autres pays, comme la Chine. Bien là, la Chine, on ne parlera pas de ça, c'est un autre cas extrême.

Mme Boutin : Ce n'est peut-être pas un exemple à prendre.

M. Waterhouse (Steve) : Puis, après ça, bien, si on prend juste Israël, là, d'où j'arrivais, bien, eux autres, ils se sont tournés vers les services de renseignements. Heureusement, le Parlement ne leur a pas donné un deuxième mandat, puis, après coup, bien, au mois d'avril, ils sont revenus, ils ont retravaillé leur formule puis ils ont dit : Oui, on n'a pas le choix, Santé publique avec services de renseignements, ils vont faire le travail qui s'impose. Donc, ceux qui sont identifiés, pour la COVID, positifs, le service de renseignements connaît leurs noms, les adresses, ils font la vérification en arrière-plan. Mais il reste toujours bien qu'ils sont en deçà de 20 % d'adoption de l'application de la population. Ça fait que c'est pour ça qu'ils ont été avec un modèle de suivi par GPS, pour être capables de s'assurer que ça ne va pas nulle part. Mais ça, c'est une culture, dans ce pays-là, que ça ne leur dérange pas d'être suivis comme ça parce qu'ils sont déjà dans un contexte quasi de conflit permanent.

Mme Boutin : Je peux te poser une dernière petite question? Là, c'est plus fort que moi. C'est quasiment... Ce n'est pas une pelure de banane du tout, O.K., vraiment pas, mais je me pose la question, parce que vous avez basé votre mémoire, tu sais, sur le document de consultation, qui proposait seulement une technologie, mais vous, si vous aviez carte blanche, compte tenu de votre expertise, là, en crise sanitaire, et tout, est-ce que vous utiliseriez la technologie? Si oui, quel type de technologie?

M. Waterhouse (Steve) : Pour être capable d'aider la population, je veux dire, ce serait à développer... ce serait intéressant de regarder une technologie qui serait capable d'aller davantage à marier... de comprendre certaines régions géographiques qui sont impactées, parce que d'avoir une carte... le service de Santé publique, d'avoir une carte au mur et dire : Bien, voici une éclosion qui se déclare dans une région plus qu'une autre, comme ça a été proposé dans l'application initiale à Ottawa, de juste avoir les trois premières lettres du code postal pour comprendre dans quelle région que ça commence ou c'est plus... que ça rentre plus dans l'équation, ça a été rejeté parce que, encore

une fois, il y avait une possibilité d'aller encore cibler la personne. Mais, parce qu'on veut respecter la vie privée des gens, l'anonymisation, à date, c'est la seule voie que je vois possible.

Mais, autre que ça, marier le GPS... Déjà là, je l'ai mentionné dans mon mémoire, il transpire de l'information, actuellement, avec Google, c'est-à-dire avec les... Android. Ça fait que, donc, dès que ça soit colmaté, cette brèche-là, est-ce que ça va être complètement hermétique? Il va toujours y avoir quelque chose qui va ressortir. Donc, il n'y a pas de solution magique, il n'y a pas de solution exacte, mais ça serait intéressant de développer davantage là-dessus, oui.

Mme Boutin : O.K. Merci.

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

M. Lévesque (Chapleau) : Merci, M. le Président. Merci, M. Waterhouse. Petite question pour vous, là, peut-être en lien avec ce que la collègue de Jean-Talon disait : Est-ce qu'il y a une application qui se rapproche de ce que vous décrivez comme l'idéal qui est soit en développement ou qui est développée?

M. Waterhouse (Steve) : Bien, il y a présentement une douzaine d'autres pays qui sont dans le même cas que nous autres : le Danemark, l'Allemagne, l'Irlande, l'Italie, le Japon, la Lettonie, la Pologne, l'Espagne, la Suisse, l'Uruguay, le Brésil, l'État de Virginie, aux États-Unis.

M. Lévesque (Chapleau) : Oui. Est-ce qu'un de ces pays-là a une application qui ressemble plus à votre idéal?

M. Waterhouse (Steve) : Ça répond présentement à comment l'application COVID Alert du Canada a été développée, ça prend le COVID Shield en arrière-plan, que les deux gars de Spotify ont développé, et ça utilise le Google-Apple... GAEN. Ça fait que c'est les mêmes concepts d'opération avec lesquels nous autres, on évolue, présentement, au Canada, et après ça, bien, ils ont développé juste la devanture, que j'appelle. Ça fait que n'importe qui va développer une nouvelle devanture qui prend les mêmes moteurs en arrière, ça va donner pas mal le même résultat.

• (17 h 50) •

M. Lévesque (Chapleau) : Le même résultat? O.K. Dans l'éventualité où le gouvernement décidait, justement, de mettre en application une telle application, je vois qu'il y a un principe-phare, là, qui semble guider votre réflexion, notamment en lien avec une instance indépendante qui assurerait, dans le fond, la surveillance du déploiement. Qui vous voyez dans cette position-là? Et quel serait son rôle, vraiment, là, de façon générale?

M. Waterhouse (Steve) : De surveiller le développement ou de surveiller le déploiement?

M. Lévesque (Chapleau) : Le déploiement.

M. Waterhouse (Steve) : Bien, le déploiement, je veux dire, c'est pas mal automatisé, d'où est-ce que... alors que c'est déposé vers Google et Apple, puis après ça les usagers, d'eux-mêmes, téléchargent les applications.

De surveiller, après ça, n'importe quelle organisation qui voudrait juste faire un suivi, que ça soit par sondage, faire du suivi actif, bien là, à ce moment-là, on sonde directement les personnes. On va un peu sur la ligne difficile à franchir, d'aller directement vers l'utilisateur. Ça va faire perdre confiance parce que, là, les personnes vont se sentir épiées, vont se sentir avec un message dirigé vers eux, ils vont dire : Bien là, ça ne vaut pas la peine, ils vont faire aussitôt «delete», puis il n'y en aura plus, de téléchargements. Ça fait que les statistiques de téléchargement vont être là, il va y avoir eu des millions de téléchargements, alors qu'il va y avoir juste des centaines de personnes qui vont s'en servir.

M. Lévesque (Chapleau) : O.K. Maintenant, vous avez également abordé, là... La Commission de l'accès à l'information sont venus nous parler ce matin. Vous dites qu'elle devrait avoir une capacité de vérification accrue. Peut-être nous parler de ça, là. En termes de réglementation, qu'est-ce qui manque? Est-ce qu'il manque quelque chose, premièrement?

M. Waterhouse (Steve) : La seule référence que j'ai faite avec la commission... des technologies... C'est bien qu'ils ont élaboré les lignes directrices, les cinq points principaux avec lesquels les programmeurs peuvent développer le matériel pour faire une application qui respecte... Ça fait que le premier papier qu'ils ont... le premier jet de papier qu'ils ont fait, c'était envers l'application COVI, de Mila, et, après coup, les travaux se sont poursuivis, comme M. Maclure a précisé. Mais, après coup, moi, je verrais toujours qu'ils soient, justement, l'émetteur de lignes directrices, en collaboration avec la Santé publique, pour être capables d'avoir ça dans le respect de qu'est-ce qu'on veut, c'est-à-dire la protection de la vie privée et des renseignements personnels.

M. Lévesque (Chapleau) : Ils ont réclamé peut-être plus de pouvoirs, plus de ressources. Est-ce que c'est quelque chose qui serait envisageable, qui serait pertinent, pour vous, pour faire ces suivis-là?

M. Waterhouse (Steve) : Un pouvoir de recommandation, je crois que c'est totalement adéquat. Ce que j'aimerais beaucoup mieux voir avec un plus grand mordant, plus de pouvoirs officiels, bien, c'est la Commission d'accès à l'information.

M. Lévesque (Chapleau) : O.K. Donc, c'est là où j'allais, justement, quels pouvoirs vous envisageriez pour eux?

M. Waterhouse (Steve) : Bien, au même titre que le commissaire Therrien, du Canada, le dit souvent, je veux dire, aussitôt qu'il y a enquête, puis il trouve qu'il y en a qui ont mal fait... autrement dit, ils ont contrevenu à des lois et règlements puis ils ont été à l'encontre du sens de la loi, bien, il n'a pas de pouvoir d'accusation, il n'a pas de pouvoir de punition. Oui, le projet de loi n° 64 s'en vient, ça va aider. Mais, en même temps, si la CAI pourrait avoir ce levier-là, bien, déjà là, ça ferait réfléchir certains malfaisants, surtout des compagnies qui, eux autres, davantage, collectent beaucoup d'informations et qui s'en sortent toujours sans aucune impunité.

M. Lévesque (Chapleau) : O.K., parfait. Maintenant, je vous amènerais peut-être sur le code source ou, du moins, l'application en développement. Vous dites que ça devrait être rendu public pour permettre à des experts indépendants, donc, d'évaluer ce code source là. On a eu la proposition peut-être que des hackers pourraient... disons, amicaux, là, viendraient tester ces applications-là pour essayer de trouver les failles, les vulnérabilités. Est-ce que, vous, par expérience, c'est une solution, c'est un élément de... une piste à envisager?

M. Waterhouse (Steve) : Bien, c'est la marche à suivre, parce que ce qu'on appelle des «white-hat hackers», donc des hackers à bonnet blanc, qui sont légitimes et ils travaillent avec un cadre légal, et tout, bien, à ce moment-là, ils vont utiliser des techniques vues... comment est-ce que les malfaisants peuvent utiliser contre ce genre d'application là et dans des simulations réalistes, de ce qui se rapproche de la vraie vie... que les malfaisants vont pouvoir les exploiter. Donc, dans la communauté... puis je pense, en disant ça, à la communauté du Hackfest, qui est ici, à Québec, qui est quand même le plus grand festival de hackers, ici, de l'est de l'Amérique du Nord, pourrait venir faire ce travail-là, peut avoir ce mandat. Puis la communauté se sentirait... justement, d'avoir un travail communautaire à rendre à la population, puis ça serait un méchant beau programme à partir. Et, de cette façon-là, bien, il y aurait beaucoup plus en termes de retour sur la vérification, et surtout la validation du contenu.

M. Lévesque (Chapleau) : O.K. Puis ce n'est pas ce qui a été fait. Est-ce qu'il y a des pays dans le monde où est-ce qu'ils ont réussi à faire ça?

M. Waterhouse (Steve) : Pas à ce que je sache. De tout ce que j'ai pu lire et documenter, c'est vraiment dans un circuit fermé, pour ne pas dire universitaire, que le travail s'est fait, de recherche, et officialisé.

M. Lévesque (Chapleau) : O.K., parfait. Merci beaucoup. C'est tout pour moi. Merci.

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

Mme Rizqy : Merci beaucoup. Bonjour. Merci d'être présent. 23 ans au service des Forces armées canadiennes et à la Défense, merci pour vos services. Merci à ceux, aussi, qui sont venus nous prêter main-forte durant la pandémie dans nos CHSLD, on avait eu bien besoin d'eux.

Alors, moi, je veux aussi vous dire que je vous écoute très souvent à la radio. Vous vulgarisez super bien vos propos pour ceux qui sont comme moi, qui ne connais pas grand-chose en cybersécurité. Et vous avez bien expliqué, tantôt, au niveau des... que même... vous avez du bois devant vous, ça peut bloquer la technologie Bluetooth, mais vous pouvez avoir du métal qui va pouvoir augmenter le signal. Derrière vous, il y a un homme qui est derrière une vitre — je vais reprendre mon exemple que j'ai utilisé hier — si l'homme en question télécharge l'application, prenons celle d'Alerte COVID, et que nous tous, on a téléchargée, et que lui, il a un diagnostic positif, est-ce qu'il est peut-être possible que nous, malgré qu'il y a un mur vitré, on reçoive aussi cette notification et qu'on nous demande d'aller nous faire tester?

M. Waterhouse (Steve) : La façon que l'application fonctionne avec le protocole Bluetooth, c'est toujours par une proximité. Donc, au-delà de 15 minutes, à deux mètres près, c'est comme ça qu'il est évalué. Donc, en arrière, la magie, comment elle s'opère, c'est avec la mesure du signal, donc avec... Le signal, si on est près, il devrait nous indiquer une valeur... Si c'est une valeur en haut de moins 50 dBm, ça va être très près. Donc, si la personne à l'arrière est détectée à une force de signal de moins 80, bien, ça n'a pas rapport... ce n'est pas aussi près qu'on s'attend.

Donc, l'atténuation peut se créer aussi... Quand je disais... l'exemple, tantôt, avec les murets... chaque matériau, lorsqu'il y a une transmission d'un signal radiofréquence, va créer une atténuation. Donc, si on est deux personnes et qu'il y a une cloison de gypse... Donc, une maison mitoyenne, par exemple, deux cloisons de gypse, ça fait à peu près un pouce, et du matériau, ça va créer une atténuation d'à peu près 10 dBm, mais c'est peut-être assez près parce que les deux... les têtes de lits sont à proximité, le signal va être très près l'un de l'autre. Et, oui, ils vont être, à ce moment-là, identifiés comme étant... ils ont été 10 heures un à côté de l'autre, ça fait que, oui, le facteur de risque, pour eux, va augmenter. Mais c'est la façon que la technologie RF fonctionne.

Mme Rizqy : Mais, dans ce cas-ci, ça fait à peu près 27 minutes qu'il est derrière vous, même un peu plus longtemps que ça, donc ça serait possible, et par conséquent nous, on pourrait recevoir, par... pas par erreur, mais on pourrait être notifiés d'y aller, alors qu'on n'a jamais été en contact avec cette personne. Et, si on se rappelle bien, au mois de mars et au mois d'avril, le Dr Arruda, à ce moment-là, voulait vraiment tester les bonnes personnes, car, à ce moment-là, on n'avait pas assez de tests, il manquait même un ingrédient pour le test, et on n'avait pas assez de ressources, aussi, humaines pour tester. Alors, est-ce que ça pourrait aussi avoir comme effet qu'il y ait trop de monde qui reçoive une notification et faire un effet d'étranglement dans le système de santé, cette technologie?

M. Waterhouse (Steve) : ...par l'imprécision de la technologie, que, là, à un moment donné, pour ne pas nommer une compagnie, tout le monde se retrouve à un Costco un dimanche après-midi puis que, là, le lundi matin, tout le monde apprend qu'il faut qu'il se présente, justement, à la Santé publique pour se faire tester. Ça, ça peut être des milliers de personnes, multiplié par le nombre de Costco. Je donne le nom, encore une fois, mais sans nommer cette cible-là. Mais ça veut dire que, oui, ça peut créer un goulot d'étranglement puis créer un épuisement des ressources, aussi, qui n'était pas nécessairement voulu, de tester tout ce monde-là.

Mme Rizqy : Puis on sait que, le test, plus il va y avoir du monde qui sont testés en grand nombre, le résultat peut prendre du temps avant de l'avoir, et les gens doivent rester à la maison, ainsi que les membres de leur famille, à la maison, en confinement, et là il peut aussi y avoir d'autres impacts comme l'absence au travail.

M. Waterhouse (Steve) : Oui, puis ça va aussi jammer, excusez le terme, tous les laboratoires avec lesquels les résultats soient pondus, là. Ça fait que c'est là que... Il faut-tu créer d'autres laboratoires? On va demander plus de gens qui sortent du cégep ou de l'université en microbiologie pour faire de l'analyse en laboratoire juste parce qu'on va créer ce genre de situation là. Ça fait que c'est pour ça que j'ai pour mon dire que, par cette imprécision technologique là, ce n'est peut-être pas tout aussi indiqué que de se fier là-dessus.

Mme Rizqy : Donc, c'est pour ça que vous arrivez avec, probablement, la conclusion c. Et, pour que les gens comprennent bien, ceux qui nous écoutent à la maison, c'est quoi... pouvez-vous nous dire c'est quoi, la conclusion c?

• (18 heures) •

M. Waterhouse (Steve) : Bien, l'option c, c'est ne pas, tout simplement, s'embarquer dans le développement d'une application puis de continuer... et emphaser le traitement actuel, manuel, le suivi manuel par les autorités de la santé. Actuellement, si le besoin est, que les gens ne se sentent pas bien, encore une fois, qu'ils se présentent à aller faire le test. De cette façon-là, les résultats, encore une fois, vont être réels, ils vont être mesurés, et il n'y aura pas, à ce moment-là, de demi-mesures.

Le seul facteur qui demeure, présentement, c'est peut-être le temps d'attente, mais qui, à ce moment-là, peut être, je crois, amélioré avec un temps... et non pas qui pourrait être, à ce moment-là, impacté par une surenchère de la demande de faire des tests avec une application qui, là, demanderait à tout le monde d'aller se présenter du jour au lendemain.

Mme Rizqy : J'ai une question, puisque vous êtes un expert de cybersécurité, je vais me permettre d'aller un peu plus loin avec vous. Identité numérique, c'est quelque chose qui est aussi discuté, en ce moment, au Québec, par le ministre délégué à la Transformation numérique. Est-ce que vous savez si, oui ou non, il existe des organismes, soit gouvernementaux ou paragouvernementaux, qui peuvent tester ces différentes applications d'identité numérique?

M. Waterhouse (Steve) : De tester l'identité numérique, premièrement, il faut que le cadre soit compris, il faut que le cadre soit défini, et, à ce moment-là, oui, il existe plusieurs organisations. Autant il y a des organisations officielles... je reviens avec l'exemple qu'on mentionnait tout à l'heure, d'utiliser des organismes comme... un hackfest, là, ça a l'air drôle comme expression, mais c'est une communauté de personnes avec des techniques de... qui sont des gens techniques avec lesquels ils pourraient justement s'adonner à un projet puis dire : Bien, voici, on fait de l'identité numérique, donnez-nous qu'est-ce que vous avez sous la main, que ça fonctionne ou que ça ne fonctionne pas.

Comme souvent j'ai dit, à la Défense, j'utilisais ce système-là d'infrastructure avec les publics. Il y a 20 ans, j'ai aidé à l'implémentation à Montréal, en 1999. Puis là on est en 2000, on s'en vient... en 2020, c'est-à-dire, on s'en va en 2021, puis on n'a toujours pas rien. Pourtant, c'est toujours en fonction au gouvernement fédéral, à la Défense. Ça fait que c'est pour dire qu'il y a eu des erreurs, par le passé, je crois, d'orientation, qui auraient dû être considérées, mais on est rendus aujourd'hui qu'on peut toujours l'anticiper puis le considérer, oui, pour l'implanter. Est-ce que c'est le même genre d'affaire qui devrait être fait? Beaucoup d'administrations américaines se servent de la même chose. Je veux dire, ce n'est pas que ce n'est pas disponible, c'est là, puis il faut juste l'utiliser pour qu'on puisse, à un moment donné, faire quelque chose de tangible.

Mme Rizqy : Puis tantôt vous avez parlé de Singapour. Singapour a obligé l'application qu'on appelle soft, c'est-à-dire Bluetooth, qu'elle soit téléchargée par leurs citoyens. Par la suite, Singapour, les autorités ont dit que ça n'a pas été très efficace et ils sont allés beaucoup plus loin, ils ont dit : Nous, ça va être la géolocalisation et

carrément aller avec le bracelet pour ceux qui sont infectés pour s'assurer qu'ils restent confinés. C'est bien ça qui est arrivé là-bas?

M. Waterhouse (Steve) : Et aussi, à ceux qui n'avaient pas... qui n'ont pas de téléphone intelligent, bien, ils se sont fait remettre un appareil complètement... j'appelle ça «dummy», qui n'a aucune intelligence et qui, à ce moment-là, fait tout simplement répondre en radiofréquence avec le réseau cellulaire pour dire où est la présence de la personne, c'est un petit peu un dérivé du bracelet. Ce n'est pas pour l'accrocher avec un «dummy», mais ça donne ça.

Une voix : ...

M. Waterhouse (Steve) : Un appareil dépourvu d'intelligence, voilà. Protection de la vie privée, on garde ça là. Et par ça, donc, ils ont voulu vraiment contourner... pas contourner, mais c'est-à-dire contenir la situation dans la population et éviter tout débordement. C'est un peu le même concept que la Corée du Sud, j'ai pu lire, a pu faire, donc d'imposer à chaque visiteur tout comme citoyen d'implanter une application de notification, même de suivi de traçabilité par GPS, dans leur téléphone à l'arrivée dans le pays. Donc, ils ont pris les moyens qu'ils croyaient, à ce moment-là, justes et équitables pour, justement, contenir la situation, tout comme la Nouvelle-Zélande a fait aussi.

Mme Rizqy : D'accord. Je vais essayer de garder mon sérieux, mais j'ai vraiment envie de rire à cause de l'expression utilisée. Dites-moi, il y a quand même une fracture numérique qui existe au Québec. Si jamais le gouvernement décide de ne pas entendre la majorité des experts qui disent de ne pas aller de l'avant et décident, eux autres, d'aller de l'avant, est-ce que le gouvernement devrait s'engager alors de fournir des téléphones «dummy» aux gens qui n'ont malheureusement pas les moyens ou qui n'ont même pas accès, nécessairement, à ce type de téléphone?

M. Waterhouse (Steve) : Ce serait une belle opportunité, justement, d'avoir, à ce moment-là, un autre point de vue sur... Justement, on disait, je crois, le... vingtaine de pour cent qu'il y a n'a pas de... de personnes qui n'ont pas de cellulaire. Ça serait significatif, à ce moment-là, d'aller chercher ce 20 % là pour compléter la documentation. Les gens vont-ils embarquer? Parce que les gens vont-ils dire : Ah! c'est ça, là, ils mettent un tag puis ils vont me chercher? Le GPS, c'est toujours une question de perception. Et, s'il n'y a pas d'adoption parce que les gens n'ont pas confiance, ça va aller aux poubelles, tout simplement. Ça fait que c'est là qu'il faut qu'il y ait un travail de fond qui soit fait, c'est-à-dire d'apporter l'information à la population et de les convaincre, vraiment, les informer correctement dans quoi que le gouvernement... avec quoi le gouvernement peut les aider.

Mme Rizqy : Tantôt, vous avez dit que la Santé publique devraient être ceux en charge de décider d'aller de l'avant ou de ne pas aller de l'avant. Lorsqu'on est dans un état d'urgence sanitaire qui est décrété, à ce moment-là, beaucoup de... en fait, nous, on n'existe à peu près... à toutes fins pratiques, presque plus, donc on ne siège pas. Est-ce que vous êtes d'avis qu'on devrait quand même avoir d'avance un protocole de sortie qui soit clairement établi pour ne pas, justement, que le décret d'urgence sanitaire soit prolongé inutilement?

M. Waterhouse (Steve) : Bien, je ne connais pas tous les tenants et aboutissants de la question, mais j'ai pour mon dire, oui, d'avoir des plans avec révision annuelle ou semi-annuelle, selon l'importance du plan, c'est toujours une question de travail, oui. Déjà là, j'en faisais l'expérience avec la première politique de cybersécurité, l'année passée, puis je suis content d'avoir contribué à ce qu'il y ait un début, comme ça, de nouveaux documents pour que ça puisse orienter le gouvernement à travailler avec des valeurs du XXe siècle, alors qu'il n'y a même pas de classification d'information.

Ça fait que, tu sais, là, dans cette optique-là, je dis : Oui, il faudrait peut-être se faire un petit cartable, puis, si jamais il arrive tel incident... comme j'ai déjà travaillé, exemple, sur un plan de recouvrement en exercice, même, avec la ville de Baie-Comeau si Manic-5 aurait à briser. Donc, ça créerait, une situation x, y, z, c'est quoi, le plan d'urgence, c'est quoi, le recouvrement, etc. Donc, dans cette optique-là, oui, c'est bon de faire des scénarios de ce sens-là et d'être prêts pour, après ça, s'en servir et d'avoir au moins des lignes directrices sur lesquelles s'aligner.

Le Président (M. Bachand) : Merci beaucoup. Malheureusement, le temps est écoulé, je suis désolé. M. le député de Gouin, s'il vous plaît.

M. Nadeau-Dubois : Merci, M. le Président. Bonjour. Merci d'avoir pris de votre temps pour partager votre expertise et votre expérience avec nous. J'ai très peu de temps, je vais aller droit au but. Est-ce que la technologie Bluetooth a été inventée pour mesurer les distances?

M. Waterhouse (Steve) : Aucunement.

M. Nadeau-Dubois : Est-ce que cette technologie est précise et fiable pour mesurer des distances?

M. Waterhouse (Steve) : Aucunement.

M. Nadeau-Dubois : Est-ce qu'on peut donc en conclure qu'il y a de fortes chances qu'une application basée sur la technologie Bluetooth génère beaucoup de cas de faux positifs, des notifications injustifiées?

M. Waterhouse (Steve) : Les deux. Il y a de fortes chances que ça ne donne pas des bons résultats et ça va créer, justement, des fausses situations.

M. Nadeau-Dubois : Merci. Vous êtes expert en cybersécurité — vous êtes le premier cybersoldat, d'ailleurs, que je rencontre, je suis un peu stressé — diriez-vous que vous êtes technophobe, quelqu'un qui a des préjugés contre la technologie?

M. Waterhouse (Steve) : Aucunement.

M. Nadeau-Dubois : Diriez-vous que vous êtes un peu dogmatique puis antitechnologie?

M. Waterhouse (Steve) : Aucunement.

M. Nadeau-Dubois : Pourtant, vous nous recommandez, aujourd'hui — c'est votre première recommandation au gouvernement du Québec — de ne pas opter pour une application de notification d'exposition.

M. Waterhouse (Steve) : Exact.

M. Nadeau-Dubois : Merci.

Le Président (M. Bachand) : C'est ce qu'on appelle des réponses claires. M. le député de René-Lévesque.

Une voix : ...

M. Ouellet : Écoute, moi, comme député de René-Lévesque, Baie-Comeau, je veux savoir il se passe quoi si le barrage Manic-5...

Des voix : Ha, ha, ha!

M. Ouellet : Juste de même...

Une voix : Sais-tu nager?

M. Ouellet : Oui, je sais nager, ça va. Je vais utiliser un peu votre expérience et votre champ d'expertise, notamment sur Bluetooth, parce que vous avez donné un peu, tantôt, je vous dirais, un tableau de ce qui pourrait se passer avec les notifications, mais vous avez insisté sur le fait que le Bluetooth, pour la notification dans l'application COVID-19, il faut qu'on soit ensemble pendant 15 minutes. C'est ça que j'ai compris?

M. Waterhouse (Steve) : Oui, c'est ça, le paramètre.

M. Ouellet : Donc, le téléphone va interagir avec l'autre téléphone pendant 15 minutes, puis, quand ça, ça va être franchi, ils vont dire : Là, j'ai une situation de 15 minutes de proximité, je l'archive. Et si, effectivement, il y a COVID, cette proximité-là de plus de 15 minutes sera notifiée. Comment ça marche? Il faut que ce soit 15 minutes dans les mêmes distances? Parce que le collègue de Gouin, tout à l'heure, parlait un peu de là... le manque de précision de Bluetooth, mais j'essaie juste de comprendre, là. 15 minutes, là, on est ensemble, je me rapproche, je me recule, tu sais, ce n'est pas fiable.

M. Waterhouse (Steve) : Sur un téléphone intelligent, il y a trois radios, là-dessus : il y a un radio cellulaire, un radio wifi Bluetooth puis un autre pour faire le paiement de proximité, donc trois champs de fréquences différents. Celui du Bluetooth va... il a son identifiant, ce qu'on appelle une «MAC Address», donc une identité unique pour le transmetteur, et c'est cette adresse unique là qui fait en sorte qu'ils vont mesurer une adresse unique là, là et là et, de cette façon-là, vont enregistrer la force du signal. Donc, oui, on s'approche, on s'éloigne, la force du signal va varier. C'est là où je parlais, tantôt, du moins de x nombre de dBm, là, à proximité de tout ça, puis les interférences qu'il peut y avoir, un mur, on se revire de bord, parce que le «body», le corps est un atténuateur, on est 80 % d'eau, donc le signal ne percera pas le corps directement, mais il va être dirigé dans d'autres lieux, c'est comme ça que ça rend le système imprécis. Là, présentement, il va mesurer d'une telle façon. Je le mets dans ma poche, il va mesurer d'une autre façon, parce que, là, je suis positionné différemment et je me tourne, etc. Ça fait que c'est tous ces facteurs-là qui vont faire en sorte que ça va donner des lectures assez mitigées.

Mais, si on est deux personnes en face de l'autre à deux mètres près pendant 15 minutes, là, la force du signal devrait être assez constante pour dire : Oui, c'est pas mal ça, 15 minutes, check. Là, à ce moment-là, le message va partir disant que les deux appareils avec tel identifiant, voici la signature, puis le message va partir, puis là tout le monde, à ce moment-là, va être mis en notification comme quoi que, potentiellement... pas tout le monde, c'est-à-dire, nous deux, on devrait se présenter pour se faire tester parce qu'on a été potentiellement à risque. Et, si un de nous deux devient positif COVID, on rentre notre code, et là ça part, puis tout le monde va être notifié.

M. Ouellet : Donc, c'est 15 minutes et plus à moins de deux mètres. À plus de deux mètres, techniquement, on ne peut pas...

M. Waterhouse (Steve) : Ça serait une folie.

• (18 h 10) •

M. Ouellet : O.K., c'est ça, ça ne fonctionnera pas.

M. Waterhouse (Steve) : Bien non, toute la pièce ici serait notifiée, il faudrait peut-être qu'ils se fassent tester, là.

M. Ouellet : O.K. Donc, si on se croise moins de 15 minutes, mais que vous avez la COVID, à moins d'un mètre et demi, je me suis mis à risque quand même. Tu sais, je veux dire, je ne serais pas notifié, mais je serais à risque quand même.

M. Waterhouse (Steve) : Oui, mais le téléphone ne sait toujours pas qu'on porte un masque. Ça fait que, déjà là, il y a une grosse atténuation, côté risque de contamination. Ça fait que c'est un élément technologique qui va juste nommer... nominativement indiquer qu'on a été dans un contexte favorable à l'infection, c'est tout.

M. Ouellet : Et, en terminant, pour la technologie Bluetooth, il faut que je l'active, mon... Même si j'ai l'application, il faut que je l'active.

M. Waterhouse (Steve) : Oui.

M. Ouellet : Moi, il m'arrive de ne pas l'activer parce que ça cherche mes appareils constamment dans la maison, je le ferme. Donc, même si l'application... je peux penser être protégé, mais, si je n'ai pas activé la notification Bluetooth, je ne serai pas notifié parce qu'elle ne sera pas en fonction.

Le Président (M. Bachand) : Merci, M. le député. Je dois passer la parole à M. le député de Chomedey, s'il vous plaît.

M. Ouellette : Mon collègue de Baie-Comeau est tout excité parce qu'il vient juste d'avoir l'Internet, là, ça fait que c'est pour ça...

Des voix : Ha, ha, ha!

M. Ouellette : C'est un sentiment... Je comprends que son appareil le cherche partout, là, parce que ça vient d'arriver.

M. Waterhouse (Steve) : Voilà, ça vibre tout le temps.

Une voix : ...

M. Ouellette : Ça aussi. Ah! moi, je ne sais pas nager, ça fait que c'est... Garde-le, ton barrage.

M. Ouellet : Bien, je vais te couper le courant...

M. Ouellette : Oui, oui, c'est ça. Bien, bienvenue. Je pense que vous nous avez... Vous êtes notre neuvième audition aujourd'hui, puis je pense que, pour les citoyens qui nous écoutent, là, vous avez vulgarisé très bien les petits bogues qu'on peut avoir ou les petites appréhensions qu'on peut avoir.

Le Pr Gingras, hier, a été le premier à venir nous dire : Bien, peut-être qu'on n'en a pas besoin, mais il n'a pas eu le temps de nous expliquer pourquoi peut-être on n'en aurait pas besoin, ce que vous avez fait après-midi. Et je pense que ça pourrait être... vous pourriez... on pourrait prendre plusieurs segments de votre présentation et les faire écouter aux gens pour leur faire apprécier.

Si jamais... parce que tout va être basé sur la science et non pas sur les sondages, si jamais le gouvernement décidait d'aller dans un sens, bien, vous avez... vous nous avez démontré des arguments, je pense, très factuels, pourquoi vous en êtes arrivé à la recommandation c, qui est ne pas investir puis d'aller beaucoup plus sur des choses qui sont mesurables puis des choses que... bien, je vous dirais, des choses factuelles. Parce que le Québec est grand, la moitié de la population est concentrée... ce n'est pas à vous que je vais apprendre ça, mais qui est concentrée dans la région de Montréal, Laval, la Montérégie, et ça va être plus difficile en région. Ça ne veut pas dire qu'il n'y a pas autant de cas de COVID qu'il peut y en avoir dans une région plus urbaine.

Bien, merci de cet exposé qui va aider plusieurs citoyens à bien comprendre. Puis là, avec ce que vous nous avez démontré, que tout ce que c'est qu'on a là-dessus, là... déjà, on était stressés par le Bluetooth, mais on a deux autres affaires qu'il faut se stresser aussi, ça fait que... Bien, merci.

M. Waterhouse (Steve) : Ça fait plaisir.

Le Président (M. Bachand) : Sur ce, au nom de la commission, merci beaucoup, M. Waterhouse, d'avoir été ici.

Et la commission ajourne ses travaux jusqu'à demain, vendredi 14 août, à 9 heures. Merci beaucoup.

(Fin de la séance à 18 h 14)