CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

44e LÉGISLATURE, 1re SESSION

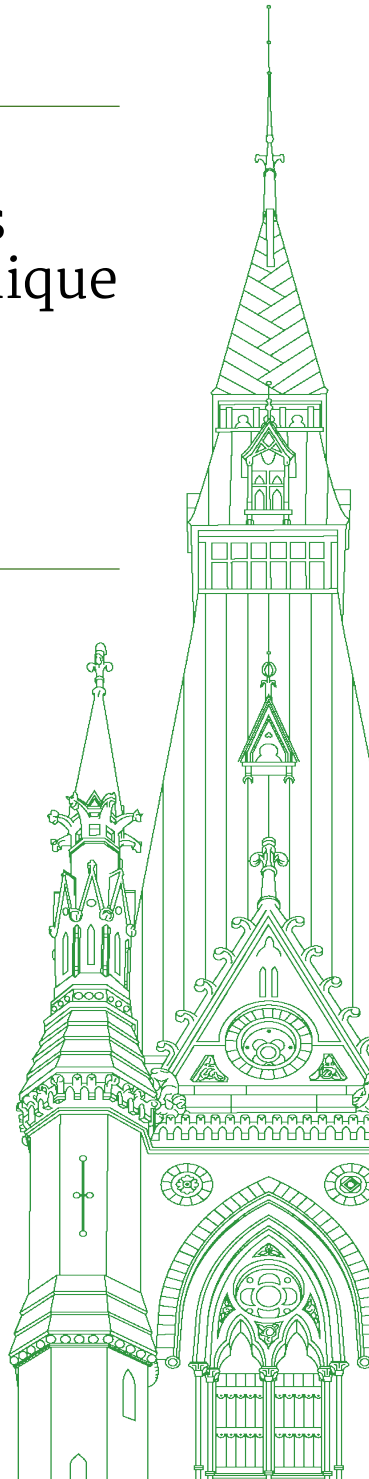
Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique

TÉMOIGNAGES

NUMÉRO 005

PARTIE PUBLIQUE SEULEMENT - PUBLIC PART ONLY

Le lundi 7 février 2022



Président : M. Pat Kelly

Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique

Le lundi 7 février 2022

● (1100)

[*Traduction*]

Le président (M. Pat Kelly (Calgary Rocky Ridge, PCC)): J'ouvre maintenant la séance.

[*Français*]

Je vous souhaite la bienvenue à la cinquième réunion du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes.

Conformément à l'article 108(3)h) du Règlement et à la motion adoptée par le Comité le jeudi 13 janvier 2022, le Comité reprend son étude de la collecte et de l'utilisation des données sur la mobilité par le gouvernement du Canada.

[*Traduction*]

La réunion d'aujourd'hui se déroule sous forme hybride, conformément à l'ordre de la Chambre adopté le 25 novembre 2021. Les membres peuvent participer en personne ou avec l'application Zoom. Les délibérations sont diffusées sur le site Web de la Chambre des communes. À titre d'information, la diffusion Web montre toujours la personne qui parle, plutôt que l'ensemble du Comité.

Je tiens à rappeler à tous les participants de la réunion qu'il est interdit de prendre des captures d'écran ou des photos de votre écran.

Compte tenu de la situation actuelle de pandémie et à la lumière des recommandations des autorités sanitaires ainsi que de la directive du Bureau de régie interne du 19 octobre 2021, pour rester en bonne santé et en sécurité, tous ceux qui participent à la réunion en personne doivent maintenir une distance physique de deux mètres et doivent porter un masque non médical lorsqu'ils circulent dans la salle. Il est fortement recommandé de porter le masque à tout moment, y compris lorsque vous êtes assis à votre place, mais c'est parfois plus facile si vous l'enlevez quand vous avez la parole. Je vais enlever mon masque quand je parle. Les participants doivent aussi avoir une bonne hygiène des mains et utiliser le désinfectant pour les mains fourni à l'entrée de la salle.

En tant que président, j'appliquerai ces mesures pendant toute la durée de la réunion, et je remercie d'avance les députés pour leur coopération.

Pour garantir le bon déroulement de la réunion, j'aimerais vous faire part de certaines règles.

Les députés et les témoins peuvent s'exprimer dans la langue officielle de leur choix. Des services d'interprétation sont disponibles pour la réunion. Vous avez le choix, au bas de votre écran, entre le parquet, l'anglais ou le français. Si l'interprétation est perdue, veuillez m'en informer immédiatement et nous veillerons à ce que l'interprétation soit correctement rétablie avant de reprendre les travaux. Veuillez utiliser la fonction « Lever la main » de la plateforme, accessible sur la barre d'outils principale, si vous souhaitez prendre la parole ou alerter le président.

Les députés qui participent en personne doivent faire comme ils le feraient habituellement si le Comité se réunissait dans une salle de comité. Gardez à l'esprit les directives du Bureau de régie interne concernant le port du masque ainsi que les protocoles en matière de santé.

Avant de prendre la parole, attendez que je vous nomme. Si vous participez par vidéoconférence, cliquez sur le micro pour désactiver le mode sourdine. Les micros des participants qui se trouvent dans la salle seront comme d'habitude contrôlés par l'agent des délibérations et de la vérification. Lorsque vous avez la parole, veuillez parler lentement et clairement. Lorsque vous ne parlez pas, mettez votre micro en mode sourdine.

Je vous rappelle que toutes les observations des députés et des témoins doivent être adressées à la présidence.

En ce qui concerne la liste des personnes qui prendront la parole, la greffière du Comité et moi-même ferons de notre mieux pour maintenir l'ordre de parole établi pour tous les députés, qu'ils participent à la réunion en personne ou à distance.

J'aimerais maintenant souhaiter la bienvenue à nos témoins. Nous accueillons les représentants du Commissariat à la protection de la vie privée du Canada, M. Daniel Therrien et M. Martyn Turcotte, directeur de la Direction de l'analyse des technologies.

Avant de céder la parole au commissaire pour sa déclaration préliminaire, je tiens à souligner qu'un certain temps sera consacré aux travaux du Comité lors de la deuxième partie de la séance. C'est un membre du Comité qui l'a demandé, et je crois qu'il est temps que nous discutions des travaux du Comité. Mon but, si nous réussissons à respecter notre horaire... Nous devrions avec un peu de chance pouvoir consacrer jusqu'à une demi-heure aux travaux du Comité, mais cela va dépendre en partie du respect de notre horaire.

Je vais maintenant vous céder la parole, monsieur le commissaire. Merci beaucoup d'être avec nous. Vous avez cinq minutes pour votre déclaration.

● (1105)

[*Français*]

M. Daniel Therrien (commissaire à la protection de la vie privée du Canada, Commissariat à la protection de la vie privée du Canada): Merci beaucoup, monsieur le président.

Je vous remercie de m'avoir invité à participer à votre importante étude.

Dès le début de la pandémie, le Commissariat à la protection de la vie privée du Canada a reconnu que les données peuvent servir l'intérêt public, par exemple, pour protéger la santé publique. À cette fin, nous avons publié un cadre qui précise comment y parvenir tout en respectant la vie privée. L'un des éléments clés de ce cadre est l'utilisation de données dépersonnalisées ou cumulatives dans la mesure du possible.

Notre cadre met en garde les institutions contre le risque toujours présent de repersonnalisation. Compte tenu de ce risque, notre cadre précise qu'il est nécessaire d'adopter des moyens techniques, entre autres, pour protéger les renseignements. En principe, l'utilisation de données dépersonnalisées ou cumulatives à des fins de santé publique peut donc se faire conformément à notre cadre si des normes techniques adéquates sont adoptées.

Depuis le début de la pandémie, nous avons régulièrement des réunions avec l'Agence de la santé publique sur des initiatives liées à la COVID-19. Ces interactions sont une bonne chose.

En ce qui concerne l'utilisation de données mobiles par le gouvernement, nous avons été informés de l'intention d'utiliser des données dépersonnalisées et cumulatives. Nous avons proposé d'examiner les moyens techniques utilisés pour dépersonnaliser les données et fournir des conseils, mais le gouvernement a fait appel à d'autres experts, ce qui est sa prérogative.

Comme nous avons maintenant reçu des plaintes formelles, nous allons enquêter et nous pencher sur les moyens choisis pour la dépersonnalisation afin de voir s'ils permettent de protéger adéquatement les données contre la repersonnalisation. Puisque cette question fait l'objet d'une enquête, nous ne serons malheureusement pas en mesure de vous fournir notre avis sur cet aspect de votre étude.

[*Traduction*]

J'aimerais maintenant faire quelques observations sur la façon dont cette affaire renvoie à des questions plus vastes, comme l'utilisation des données dans les secteurs public et privé et, à mon avis [*difficultés techniques*] le besoin urgent d'une réforme législative. Je souhaite également vous suggérer des questions que vous pourriez examiner au cours de votre étude.

Les organisations des secteurs public et privé réutilisent constamment des données à de nouvelles fins. Cette pratique suscite des préoccupations légitimes chez les consommateurs, en particulier lorsque leurs données personnelles sont utilisées à leur insu, à des fins autres que celles auxquelles ils s'attendaient. Est-ce que cela veut dire que ces pratiques ne devraient être autorisées qu'avec le consentement des consommateurs? Je crois que cela ne serait ni réaliste ni raisonnable, comme cette affaire l'a démontré.

La solution, à mon avis, est plutôt d'autoriser l'utilisation des données personnelles pour le bien commun ou les fins commerciales légitimes, à l'intérieur d'une loi fondée sur les droits, qui reconnaîtrait que le droit à la vie privée a la même valeur et est de la même nature que tout autre droit de la personne. Ainsi, le poids des renseignements personnels serait pris en compte dans tout exercice d'équilibre.

Le gouvernement fait valoir que son utilisation des données sur la mobilité ne tombe pas sous l'application de la Loi sur la protection des renseignements personnels, autrement dit, que cette loi ne s'applique pas. Étrangement, cette conclusion est probablement conforme à la loi actuelle, dans la mesure où les renseignements ont été correctement dépersonnalisés et agrégés, ce qui fait présentement l'objet d'une étude de votre part et, indépendamment, du Commissariat. Donc, la première question à se poser est de savoir si les données ont effectivement été correctement dépersonnalisées et agrégées.

Mais, même si elles l'ont été, une deuxième question que vous devriez examiner serait celle de savoir si c'est une bonne politique législative que de ne pas appliquer les lois sur la protection des renseignements personnels aux données dépersonnalisées. Nous sommes d'avis que l'exclusion des données dépersonnalisées du champ d'application des lois sur la protection des renseignements personnels n'est pas une bonne approche, puisqu'elle comporte des risques très sérieux.

Ensuite se pose la question de la transparence et du consentement. Le gouvernement ou ses partenaires commerciaux du secteur privé ont-ils adéquatement informé les usagers des services de téléphonie cellulaire que leurs données de mobilité seraient utilisées à des fins de santé publique? Les politiques de confidentialité de Telus font bien mention, quelque part, du programme Données au service du bien commun, et, même si le gouvernement fait des efforts pour informer les Canadiens de son utilisation de ces données, sur le site Tendances COVID, personne ne peut prétendre sérieusement que la majorité des usagers des services de téléphonie savaient comment leurs données de mobilité seraient utilisées.

Est-ce que cela a de l'importance? C'est à mon avis une autre question que vous devriez examiner. Il va sans dire que la transparence contribue à la confiance, et le gouvernement aurait certainement pu être plus proactif dans ses stratégies de communication pour informer les Canadiens de son programme, mais est-ce qu'un programme comme celui-ci exige un consentement valable?

● (1110)

Comme je l'ai dit plus tôt, je pense que, en raison des limites du consentement comme moyen de protéger la vie privée, il serait préférable de permettre l'utilisation des données personnelles à des fins commerciales légitimes ou pour le bien commun, à l'intérieur d'un cadre fondé sur le respect des droits. Cette loi devrait être appliquée par le Commissariat, organisme indépendant, qui serait doté des ressources et des pouvoirs nécessaires à la protection des Canadiens.

Le président: Excusez-moi, je ne vous ai pas averti, mais votre temps est pour ainsi dire écoulé.

M. Daniel Therrien: Je suis prêt à répondre aux questions.

Le président: D'accord. La parole va maintenant à M. Brassard pour six minutes.

M. John Brassard (Barrie—Innisfil, PCC): Merci, monsieur le président.

J'aurais préféré que M. Therrien puisse continuer, parce qu'il est clairement un expert dans son domaine et qu'il a beaucoup de choses à dire.

Monsieur Therrien, merci d'être avec nous aujourd'hui. Je crois qu'il s'agit d'une étude importante, parce que les Canadiens sont préoccupés par la question de la protection des renseignements personnels. Je crois, monsieur Therrien, que cette étude va aussi permettre au Comité d'examiner en profondeur les questions que vous avez soulevées dans votre déclaration et au sujet desquelles vous avez écrit aux autres commissaires à la protection de la vie privée. Vous avez écrit au gouvernement au sujet de la protection des renseignements personnels dans le contexte de la pandémie.

Le point que je tiens vraiment à clarifier concerne la consultation avec le Commissariat. Je crois — et j'imagine que beaucoup de Canadiens le croient également — que le Commissariat à la protection de la vie privée du Canada est la première organisation qui doit être consultée, avant toutes les autres. Pour dire les choses autrement, vous représentez les normes à respecter à l'égard de la vie privée au Canada. Cependant, nous entendons différents sons de cloche: certains disent que vous avez été consultés, et d'autres, non.

L'ASPC a fait savoir qu'elle allait consulter d'autres experts en sécurité et en protection des renseignements personnels. Qu'est-ce que ces autres experts en sécurité et en protection des renseignements personnels peuvent offrir de plus que le Commissariat à la protection de la vie privée du Canada?

M. Daniel Therrien: Pour répondre à la question de savoir si nous avons été consultés ou informés, et quelle était la teneur de ces discussions, je dirais que l'ASPC et un groupe du ministère de l'Innovation nous ont informés du fait que le gouvernement voulait utiliser des données dépersonnalisées à des fins que j'ai mentionnées plus tôt, c'est-à-dire utiliser les données de mobilité pour comprendre les tendances des déplacements, à des fins de santé publique.

Nous avons appris cela dans le cadre des réunions régulières que nous avons avec les organismes gouvernementaux pour discuter de toutes sortes de questions liées à Alerte COVID. À ce moment-là, nous avions une présence très forte, en ce qui concerne l'application Alerte COVID, entre autres, alors on nous a informés de ce projet en particulier.

Nous avons offert de fournir des conseils sur les mesures de précaution pour nous assurer qu'elles étaient adéquates et que les données étaient correctement dépersonnalisées, mais le gouvernement a décidé de se fier à d'autres, comme c'est sa prérogative.

M. John Brassard: Est-ce que c'est normal, monsieur Therrien? C'est sa prérogative, mais est-ce que c'est normal pour le gouvernement de demander des conseils à des experts externes en sécurité et en protection des renseignements personnels, alors que c'est votre commissariat qui a la responsabilité de protéger la vie privée et de fournir des conseils au gouvernement à ce sujet? Je trouve que le gouvernement a agi de façon très étrange.

M. Daniel Therrien: Nous avons offert de fournir des conseils. Est-ce normal que le Commissariat n'intervienne pas dans toutes les affaires? Je crois que, en réalité, le Commissariat ne peut pas préautoriser ou examiner tous les cas de collecte ou de divulgation de données au Canada. Nous formulons des conseils généraux, et nous espérons qu'ils seront suivis. Nous enquêtons sur les plaintes.

Je crois que, dans le cadre de la nouvelle loi, notre commissariat devrait avoir plus de pouvoirs afin de réaliser proactivement des audits sur les pratiques du gouvernement et du secteur privé, mais ce n'est malheureusement pas réaliste de s'attendre à ce que le Commissariat approuve toutes les utilisations ou divulgations de données au pays. Au bout du compte, l'accès aux données est une bonne chose pour le Canada, évidemment, tant que c'est à des fins acceptables, comme des intérêts commerciaux légitimes ou pour le bien public et non pour une surveillance illégitime, comme cela s'est vu dans certains cas.

Mais ce genre de choses se fait tout le temps, alors nous ne pouvons pas être là dans tous les cas.

● (1115)

M. John Brassard: D'accord, mais on peut raisonnablement croire — je parle au nom des Canadiens — que, lorsque le gouvernement ou, comme ici, les entreprises de télécommunications s'adressent à des experts externes en protection des renseignements personnels et en sécurité, cela ne garantit pas qu'ils vont suivre les lois sur la protection des renseignements personnels.

Est-ce que cela vous préoccupe, la possibilité que, quand on s'adresse à une autre organisation que l'expert de facto du pays...? C'est un peu comme essayer de trouver un avocat qui est d'accord avec vous. Il y en a un qui n'est pas d'accord, alors vous allez en voir un autre qui dit: « Oui, bien sûr, vous respectez la loi », mais cela ne veut pas dire que c'est vrai. Est-ce que cela vous préoccupe?

M. Daniel Therrien: Nous ne sommes pas les seuls experts. Les organisations n'ont pas toutes le même niveau d'expertise, mais, dans cette affaire, il s'agit du gouvernement du Canada, qui a ses experts, et des grandes entreprises de télécommunications, qui ont aussi les leurs. Nous avons offert notre expertise, mais on n'a pas retenu nos services. Nous ne pouvons rien y changer.

M. John Brassard: Merci, monsieur Therrien.

Vous avez parlé du consentement et de l'importance du consentement. C'est facile de dire que Telus offre une option de non-participation relativement à ses « données au service du bien commun ». Mais, dans la plupart des cas, et les témoins nous ont dit que dans certains cas...

Monsieur le président, mon temps doit être épuisé.

Le président: Votre temps est presque écoulé.

M. John Brassard: Je veux juste parler de l'importance du consentement éclairé par rapport à la collecte de données.

M. Daniel Therrien: Encore une fois, le consentement n'est pas une panacée ni une solution universelle. Il est clair, comme je l'ai dit dans ma déclaration, que la plupart des Canadiens dont les données ont été utilisées ne savaient pas que leurs données étaient utilisées. Les deux parties — le gouvernement et le secteur privé — auraient pu déployer plus d'efforts pour informer les utilisateurs que leurs données étaient utilisées à ces fins.

M. John Brassard: Merci.

Le président: Merci.

La parole va à M. Fergus pour six minutes.

[*Français*]

L'hon. Greg Fergus (Hull—Aylmer, Lib.): Merci beaucoup, monsieur le président.

J'aimerais aussi remercier M. Therrien de son témoignage aujourd'hui et de sa disponibilité pour offrir ses commentaires et son expertise.

Nous vous sommes très reconnaissants de votre travail, monsieur Therrien.

Le Comité a décidé de faire une étude « concernant la collecte, l'utilisation ou la possession par l'Agence de la santé publique du Canada des données privées des téléphones cellulaires des Canadiens ». Un porte-parole de l'Agence de la santé publique du Canada a précisé que seules des données dépersonnalisées ou anonymes sont utilisées.

Monsieur Therrien, selon votre évaluation des communications que votre bureau a eues avec l'ASPC, pouvez-vous nous dire si, de prime abord, le gouvernement a bel et bien reçu des données anonymes ou dépersonnalisées?

M. Daniel Therrien: Je ne le peux pas, parce que c'est l'objet de l'enquête que nous allons devoir mener à la suite des plaintes formelles que nous avons reçues en vertu de la loi.

Ce que je peux dire, c'est que nous avons eu des conversations avec l'Agence de la santé publique. Elle nous a informés encore une fois qu'elle avait l'intention d'utiliser des données dépersonnalisées ou cumulatives à des fins d'intérêt public, comme la santé publique. C'est conforme à notre compréhension des principes de protection de la vie privée.

Pour ce qui est de savoir si les données ont été dépersonnalisées correctement, nous ne le savons pas encore. Nous allons enquêter.

● (1120)

L'hon. Greg Fergus: Monsieur Therrien, il n'y avait pas de signaux d'alarme, en avril 2020, quand vous avez entamé ces conversations, n'est-ce pas? J'imagine que c'est parce que l'Agence faisait son travail et demandait de recevoir des données dépersonnalisées conformément aux principes importants que votre bureau et le gouvernement ont établis, n'est-ce pas?

M. Daniel Therrien: Ce dont on nous a informés était, en principe, conforme au cadre que nous avions établi. Nous avons offert d'aller voir sous le capot et de déterminer si les données avaient effectivement été dépersonnalisées correctement, mais le gouvernement a décliné cette offre. Du côté des principes, il n'y a pas de problème. Pour ce qui est de la pratique, nous allons enquêter. Je n'ai pas de raison de croire que les choses ont été faites correctement ou, à l'inverse, de façon inappropriée. Cela fera l'objet d'une enquête.

L'hon. Greg Fergus: Monsieur Therrien, apparemment, ces données ont été publiées de façon transparente. Encore une fois, je vous pose la question: avez-vous des raisons de craindre que les données publiées n'aient pas été adéquatement dépersonnalisées?

M. Daniel Therrien: Cela fera l'objet de notre enquête. Je ne peux pas me prononcer là-dessus pour le moment.

L'hon. Greg Fergus: Ces données sont-elles du domaine public depuis un certain temps, monsieur Therrien?

M. Daniel Therrien: Oui, il y a plusieurs mois qu'elles ont été publiées.

L'hon. Greg Fergus: À votre avis, combien de temps faudra-t-il à votre bureau pour mener à terme une évaluation appropriée et pour établir si le gouvernement a réussi ou non à protéger les renseignements personnels des Canadiens?

M. Daniel Therrien: Nous avons reçu des plaintes à la toute fin de 2021, c'est-à-dire il y a environ deux mois. Nous avons renvoyé des questions aux ministères concernés il y a quelques semaines, mais nous attendons toujours leurs réponses. J'aimerais bien pouvoir vous dire que nous serons en mesure de conclure l'enquête pendant que votre étude est en cours, mais je ne pense pas que ce soit possible.

Comme je vous l'ai dit, nous n'avons toujours pas reçu de réponse de la part des ministères. Je ne veux pas laisser entendre qu'il y a un retard. C'est simplement le cours normal des choses. Au cours des mois qui suivront la fin de votre étude, nous serons en mesure de conclure l'enquête.

L'hon. Greg Fergus: Monsieur Therrien, je tiens à vous dire encore une fois que j'apprécie énormément votre travail et celui de votre bureau. Je respecte assurément votre professionnalisme. Cela dit, s'il faut plusieurs mois pour déterminer si des données ont été dépersonnalisées, est-ce que cela peut expliquer que le gouvernement ait décidé de faire appel à d'autres experts dans le domaine, à votre avis?

La pandémie a touché tout le monde et il fallait en arriver à une conclusion. Cette situation était inusitée.

[*Traduction*]

Le président: Pouvez-vous conclure, monsieur Fergus? Votre temps est écoulé.

[*Français*]

L'hon. Greg Fergus: M. Therrien pourrait peut-être répondre par écrit à ma question.

[*Traduction*]

Le président: Oui, je vais le laisser répondre, mais votre temps est écoulé.

[*Français*]

L'hon. Greg Fergus: Merci, monsieur le président.

[*Traduction*]

Le président: Répondez brièvement, s'il vous plaît.

[*Français*]

M. Daniel Therrien: Dans le cadre d'une enquête formelle, si nous avions été consultés, nous aurions pu formuler des conclusions à partir de renseignements que, je le rappelle, le gouvernement ne nous a toujours pas fournis. En outre, dans le cadre d'une enquête, il faut entendre aussi bien le plaignant que les intimés, et cela allonge les délais.

[*Traduction*]

Le président: Merci.

[*Français*]

Monsieur Villemure, vous disposez de six minutes,

M. René Villemure (Trois-Rivières, BQ): Merci, monsieur le président.

Si le commissaire à la protection de la vie privée n'est pas intervenu, monsieur Therrien, ce n'était pas par choix. Est-ce exact?

● (1125)

M. Daniel Therrien: Comme je l'ai mentionné déjà, nous avons offert de donner des avis, mais le gouvernement a décidé d'aller les chercher ailleurs.

M. René Villemure: Très bien, merci.

Dans toute cette affaire, je m'intéresse beaucoup plus à la source des données qu'à leur destination. Vous avez dit tantôt qu'il était pratiquement impossible d'obtenir un consentement valable de la part des utilisateurs dont les données ont été utilisées.

Selon vous, est-ce qu'une présomption de consentement peut remplacer un consentement valable? Je ne veux pas dire ici au sens de la loi; je parle plutôt d'un consentement approprié.

M. Daniel Therrien: Dans ce cas-ci, je pars du principe qu'il y a une place pour le consentement dans la protection de la vie privée, mais qu'il n'est pas réaliste, dans le monde moderne d'aujourd'hui, de s'attendre à ce que tous les usages commerciaux ou gouvernementaux des données d'un client fassent l'objet d'un consentement. Voilà qui nous amène au concept de consentement souvent implicite.

Dans ce cas, le principe juridique qui s'applique est celui selon lequel des données correctement dépersonnalisées, ce qui est tout à fait possible, ne sont tout simplement pas des renseignements personnels au sens de la loi actuelle dans le secteur public. Le gouvernement peut donc les colliger et les utiliser comme bon lui semble, sans avoir à protéger la vie privée. Cela est tout à fait possible, même si nous n'avons pas encore de conclusion.

Ainsi, la règle qui semble applicable dans ce cas est celle selon laquelle les données, si elles ont été correctement dépersonnalisées, ne sont pas des renseignements personnels et que le consentement n'est pas nécessaire.

C'est l'une des raisons pour lesquelles nous recommandons que, même si les données sont dépersonnalisées, la loi soit modifiée afin de rester assujettie à la Loi sur la protection des renseignements personnels, afin qu'il y ait certains principes applicables, même si les données sont dépersonnalisées.

M. René Villemure: D'accord, je vous remercie.

Croyez-vous que l'utilisateur moyen d'un téléphone cellulaire comprend que ses données peuvent être utilisées à d'autres fins que l'amélioration des réseaux, par exemple? Je ne parle pas du fait que l'utilisateur le sait, mais qu'il comprend cet élément.

M. Daniel Therrien: Non. Les gens ne sont pas pleinement conscients de certains usages.

M. René Villemure: Les clients de Telus avaient la possibilité de retirer leur consentement. Il leur suffisait d'aller sur le site Web de Telus et de le faire. Encore là, fallait-il le savoir et le comprendre.

La possibilité qu'ont les clients de retirer leur consentement devrait-elle être plus claire?

M. Daniel Therrien: Cela revient effectivement à dire que les utilisateurs des services de téléphonie cellulaire n'étaient pas au courant de la pratique et n'étaient donc pas en mesure de retirer leur consentement. Les gens ne peuvent pas retirer leur consentement quand ils ne sont pas au courant qu'ils peuvent le faire.

Comme je le disais, à mon avis, il y aurait dû y avoir plus de mesures de la part de Telus et du gouvernement pour informer les Canadiens de l'utilisation qui était faite de leurs données.

M. René Villemure: Cela devrait-il faire partie de la révision proposée de la loi?

M. Daniel Therrien: Le principe de transparence devrait certainement faire partie de la Loi sur la protection des renseignements personnels. Il devrait y avoir une plus grande transparence.

M. René Villemure: Connaissez-vous des territoires dans le monde où les principes de transparence existent et sont mieux appliqués?

M. Daniel Therrien: Je dirais qu'en Europe, les lois sont certainement plus rigoureuses. Cela dit, nous pouvons vous répondre de façon plus précise par écrit, si vous le voulez.

M. René Villemure: Je vous remercie. Cela serait extrêmement intéressant.

Autrement dit, même si la lettre de la loi ou de la réglementation permettait à Telus de faire un tel usage des données de ses clients, l'utilisateur ne le comprendrait pas.

M. Daniel Therrien: C'est vrai.

Comme je le disais dans mes observations, je ne pense pas que la solution ultime consiste uniquement en une plus grande transparence et en l'obtention d'un consentement, étant donné le nombre extrêmement important d'utilisations qui est fait, parfois pour de bonnes raisons, parfois pour de mauvaises raisons.

Il faut donc des critères objectifs, comme l'usage commercial légitime et le bien public, qui seraient appliqués par une agence de réglementation. Le consentement est important, mais il faut aussi qu'une agence de réglementation joue son rôle pour bien protéger les Canadiens, étant donné la complexité de l'usage qui est fait de leurs données.

● (1130)

[*Traduction*]

Le président: Monsieur Villemure, j'ai bien peur que votre temps ne soit écoulé.

[*Français*]

M. René Villemure: D'accord.

[*Traduction*]

Le président: La parole va maintenant à M. Green, pour six minutes.

M. Matthew Green (Hamilton-Centre, NPD): Merci.

Par votre entremise, monsieur le président, j'aimerais d'abord me présenter à M. Therrien; je suis député d'Hamilton—Centre. Puisque j'ai seulement six minutes, je vais vous poser très rapidement quelques questions. Je m'excuse d'avance si j'ai l'air de mettre la pression lorsque vous répondez à une question pour passer à la suivante.

Tout comme les autres membres ici présents, un point qui me préoccupe est que nous avons obtenu des renseignements contradictoires lors de notre réunion du 3 février, la semaine dernière, quand les représentants de l'Agence de la santé publique du Canada sont venus témoigner — avec le ministre — au sujet de la participation du Commissariat. Vous dites maintenant que vous aviez été avisé. Je tiens à vous dire que, au cours des dernières réunions, on nous a laissé entendre qu'il y avait eu une collaboration ou une consultation.

J'aimerais qu'on distingue clairement ce qui se passe quand le Commissariat est tenu informé de façon continue de quelque chose et ce qui pourrait se passer si le Commissariat offrait activement des conseils au ministère au sujet de la protection des renseignements personnels. Pouvez-vous décrire brièvement les différences entre ces deux scénarios?

M. Daniel Therrien: Quand nous participons activement, que ce soit auprès d'une institution du secteur public ou d'une organisation commerciale, nous recevons des renseignements détaillés à propos des flux d'information et des façons dont l'information est protégée. Cela nous permet de dire, d'abord, que les renseignements personnels sont protégés, en principe, et, ensuite, que nous avons bel et bien vérifié « sous le capot » — permettez-moi l'expression — pour nous assurer que les renseignements personnels des Canadiens et des Canadiennes ont bel et bien été protégés.

Dans le cas présent, nous n'avons pas eu l'occasion de regarder sous le capot.

M. Matthew Green: Je tiens pour acquis que cela fera probablement partie de vos enquêtes en cours relativement aux plaintes et que vous allez regarder sous le capot pour voir si c'est conforme au cadre que vous avez publié, parce qu'il y était explicitement indiqué qu'il fallait que des mesures techniques et autres soient mises en œuvre pour protéger l'information. Ai-je raison?

M. Daniel Therrien: Oui, et la loi, évidemment... Nous allons vérifier notre cadre et la loi.

M. Matthew Green: Pouvez-vous fournir plus de détails sur votre cadre? Sans trop entrer dans les détails techniques, est-ce que tous les ministères, les organismes du gouvernement fédéral, sont au courant de votre cadre, compte tenu du fait que nous traversons une période très délicate, à cause de la COVID, en plus du partage de l'information et des conséquences sur la protection des renseignements personnels?

M. Daniel Therrien: Le cadre a été communiqué à tous les ministères, et nous en avons bien sûr discuté avec plusieurs d'entre eux, alors je dirais que, selon moi, oui, notre cadre est connu au gouvernement fédéral.

M. Matthew Green: Est-ce que les autres ministères vous consultent activement, dans un processus consultatif plus individuel?

M. Daniel Therrien: Il y a plusieurs ministères, peut-être pas la majorité, mais je dirais à coup sûr Santé Canada... C'est l'Agence de la santé publique qui nous a le plus consultés durant la pandémie, comme on pouvait s'y attendre. Un certain nombre d'autres ministères...

M. Matthew Green: Mais pas à ce sujet. Pour que ce soit clair, quand vous avez offert d'examiner ses moyens techniques pour la dépersonnalisation des données et de lui fournir des conseils, l'ASPC a décliné votre offre. Ai-je raison?

M. Daniel Therrien: Oui. On nous a informés du programme, mais on a décliné notre offre de regarder sous le capot.

M. Matthew Green: Changeons de vitesse. Une chose qui m'intéresse beaucoup, c'est que vous avez souligné l'urgence d'une réforme législative. Je suis tout à fait d'accord. Je ne veux pas que notre étude serve uniquement à trouver des coupables, et j'espère que notre comité pourra recueillir des faits et ensuite les utiliser pour formuler des recommandations qui serviront à combler les lacunes entre... ce que vous avez identifié comme étant des utilisations légitimes à des fins commerciales ou pour le bien commun.

Dans le temps qu'il me reste, pouvez-vous présenter au Comité, de façon préliminaire, quelques-uns des points de cette réforme législative urgente que vous voudriez examiner ou recommander?

● (1135)

M. Daniel Therrien: Je commencerais par le fait que les données, y compris les données personnelles, sont nécessaires au développement et à la croissance économiques et au bien social. Nous ne disons pas que les données ne devraient pas être utilisées. C'est la réalité du XXI^{e} siècle, c'est la réalité de l'avenir.

Malgré tout, le fait que les données peuvent être utilisées pour de bonnes raisons ne veut évidemment pas dire que cela est toujours le cas. Nous avons été témoins de nombreux cas, au fil des ans, où les données étaient utilisées de façon contraire aux intérêts individuels. Prenez le cas de Cambridge Analytica, par exemple, et à son lien avec la démocratie.

Le cadre doit laisser une marge de manœuvre et permettre d'innover au chapitre de l'utilisation des données à des fins commerciales légitimes et pour le bien public, mais le cadre doit protéger la vie privée en tant que droit de la personne. Il doit être appliqué par un organisme de réglementation qui est habilité à réaliser des audits ou des enquêtes pour s'assurer que, dans des circonstances particulières, les données sont effectivement utilisées correctement, et lorsqu'elles ne le sont pas, il devrait y avoir des pénalités conséquentes pour les acteurs, les entreprises, qui ont enfreint la loi.

C'est essentiellement le cadre que nous avons.

M. Matthew Green: J'ai une petite question.

Le président: Vous pouvez poser une petite question.

M. Matthew Green: Vous avez mentionné Cambridge Analytica, ce qui me fait penser à Facebook. Nous savons que présentement, avec ce qu'on appelle le « bouclier de protection des données », l'Europe impose des restrictions à l'utilisation par Meta des serveurs américains. Le Canada a-t-il besoin de son propre bouclier de protection des données lorsqu'il est question de serveurs internationaux?

Le président: Répondez très rapidement, je vous prie.

M. Daniel Therrien: Je dirais simplement ceci: on n'a pas nécessairement besoin d'un bouclier de protection des données, mais il nous faut des lois qui soient compatibles entre les pays et à l'intérieur du Canada.

M. Matthew Green: Merci beaucoup, monsieur le président.

Le président: Sur ce, nous commençons le deuxième tour.

Les intervenants auront cinq minutes, et nous commençons par M. Kurek.

M. Damien Kurek (Battle River—Crowfoot, PCC): Merci beaucoup, monsieur le commissaire. Je vous suis reconnaissant d'être avec nous aujourd'hui et de nous faire profiter de vos connaissances très utiles sur ce sujet si important. J'ai l'impression qu'il y a un indicateur clé ici: les données dépersonnalisées et agrégées semblent vraiment être le facteur déterminant de ce que nous essayons de faire.

Monsieur le commissaire, la semaine passée, le ministre a dit qu'il avait eu des rencontres bihebdomadaires avec le Commissariat à la protection de la vie privée. Je crois que c'est bien ce que le ministre a dit. Au cours de ces réunions, avez-vous parlé de ce que cela signifie concrètement, des données « dépersonnalisées » et « agrégées »?

M. Daniel Therrien: C'est vrai que nous avons eu des réunions pratiquement toutes les deux semaines avec l'Agence de la santé publique à propos des diverses mesures liées à la COVID et de leurs conséquences sur la vie privée. Au cours de cette période — c'était au début de la pandémie, en mars et en avril 2020 —, nous avons abordé énormément de sujets, comme l'application Alerte COVID. Nous avons été informés du programme sur lequel porte votre étude, et le gouvernement croyait qu'il obtenait des données anonymisées et agrégées. C'est dans cette optique que nous avons offert de fournir des conseils, mais on a décliné notre offre. Notre rôle n'est pas de préautoriser toutes les initiatives gouvernementales, alors nous n'avons pas poussé plus loin.

M. Damien Kurek: Merci, monsieur le commissaire.

Pouvez-vous nous parler de certains des risques qui sont associés aux données dépersonnalisées et agrégées? Personne ne nous a encore montré exactement à quoi ressemblent ce genre de données. Pouvez-vous décrire certains des risques liés à ce genre de données et peut-être nous donner une définition de ce que cela veut dire, en particulier dans ce contexte? On parle ici des données de mobilité d'environ — les estimations varient d'une source à l'autre — 33 millions d'utilisateurs.

M. Daniel Therrien: Les données sont dépersonnalisées parce qu'elles permettaient originalement d'identifier les personnes. Nous commençons par les renseignements personnels. Il est clair qu'une entreprise de télécommunications comme Telus a des renseignements sur les données de mobilité de ses utilisateurs, parce que Telus doit obtenir ce genre d'informations pour assurer la prestation des services qu'elle donne à ses clients. Vous commencez par des données clairement personnelles au sujet des gens qui utilisent les services de communications. Lorsque vous dépersonnalisez des données, vous transformez l'information personnelle par des moyens techniques — et si nous avons le temps, je vais demander à mon collègue M. Turcotte de décrire ces méthodes — pour réduire le risque que les personnes soient reconnues.

Ce qu'il faut comprendre, c'est que, même lorsque les données sont correctement dépersonnalisées, il existe toujours un risque qu'elles puissent être repersonnalisées par couplage de données. Cela peut se faire de toutes sortes de façons. Et c'est pourquoi, puisqu'il existe un risque de repersonnalisation dans chaque cas, nous croyons que ce n'est pas une bonne politique publique que d'exclure, selon le cadre législatif en vigueur, les renseignements dépersonnalisés du champ d'application de la Loi sur la protection des renseignements personnels.

● (1140)

M. Damien Kurek: Merci beaucoup, monsieur le commissaire.

Il ne me reste presque plus de temps, mais je tiens à poser une dernière petite question.

Votre commissariat a-t-il été consulté sur l'appel d'offres, qui a été mis en suspens, en vue de continuer cette pratique dans l'avenir? D'après l'explication fournie, cela ne sera pas seulement durant la pandémie de COVID-19, mais peut-être aussi après. Est-ce que votre commissariat a été consulté à ce sujet, et le cas échéant, qu'en est-il?

M. Daniel Therrien: On ne nous a pas consultés. Nous avons demandé de l'information vers la fin de 2021 à propos de ce processus, et on nous a donné certains renseignements, mais je ne dirais pas qu'il s'agissait d'une consultation. On nous a informés.

M. Damien Kurek: Merci beaucoup, monsieur le commissaire. Merci de votre réponse.

Le président: Merci.

La parole va maintenant à Mme Hepfner, pour cinq minutes.

Mme Lisa Hepfner (Hamilton Mountain, Lib.): Merci beaucoup.

Je veux remercier M. Therrien d'être avec nous aujourd'hui et de répondre à toutes ces questions très importantes. Je suis d'accord avec mes collègues.

J'aimerais revenir à la partie de votre déclaration préliminaire où vous avez parlé de transparence et du consentement. Vous demandiez si les Canadiens savaient clairement que leurs données étaient utilisées de cette façon.

Je crois que c'est dès le début de 2020 que le Cabinet du premier ministre a publié un communiqué de presse pour dire que la Santé publique allait commencer à utiliser les données de mobilité dépersonnalisées pour aider dans la lutte contre la COVID-19. Je n'étais pas députée à ce moment-là, mais je me rappelle en avoir entendu parler. Je me rappelle que l'administratrice en chef de la santé publique du Canada, la Dre Theresa Tam, envoyait régulièrement des gazouillis à propos de ces données et de ce que cela voulait dire. Nous savions, par exemple, que les mesures de santé publique étaient respectées parce que les données de mobilité montraient que les gens se déplaçaient moins, et ensuite, des tendances ont pu être cernées grâce aux données de mobilité. J'ai vu que le gouvernement publiait régulièrement de l'information sur la façon dont ces données étaient utilisées, et cela n'a pas semblé créer de préoccupations jusqu'à ce que l'opposition soulève la question il y a deux ou trois mois.

Quand vous dites que le gouvernement aurait pu être plus proactif dans ses communications sur l'utilisation des données de mobilité, qu'aurait-il pu faire de mieux, exactement, selon vous?

M. Daniel Therrien: Ce n'est pas facile d'être transparent. Comme je l'ai dit dans ma déclaration, le gouvernement a une page Web, TendancesCOVID, qui fait un assez bon travail pour expliquer aux Canadiens que leurs données de mobilité sont utilisées. Vous n'avez pas besoin de lire une politique de confidentialité de 60 pages pour le savoir, mais, pour accéder à cette page, vous devez d'abord savoir que ce programme existe et qu'il y a quelque chose qui s'appelle TendancesCOVID. Une fois que vous êtes rendu là, le gouvernement fait un travail correct en matière de transparence.

Au-delà de cette page Web, je crois que vous avez demandé — avec raison — comment le gouvernement pouvait être proactif. Il peut le faire au moyen de stratégies de communication et de conférences de presse de l'ASPC et d'autres organisations, par exemple. Ça, ce serait être proactif.

Selon moi, l'essentiel c'est que je doute énormément, que la majorité des utilisateurs de services mobiles savait que leurs données étaient recueillies, malgré les efforts que le gouvernement a faits.

La transparence, c'est important, mais ce n'est pas suffisant pour assurer une réglementation convenable des données. C'est pour cela que j'ai dit que, en plus de la transparence, en plus du consentement, il faut que l'organisme de réglementation ait le pouvoir de mener des enquêtes, comme nous le faisons présentement, sur ce genre de situations afin de garantir la protection des renseignements personnels.

● (1145)

Mme Lisa Hepfner: Merci.

Lorsque vous dites que la plupart des utilisateurs ne savaient pas que leurs données étaient utilisées de cette manière, sur quoi vous fondez-vous? Voulez-vous dire que les gens ne savent pas que leurs données sont utilisées ou que leurs données de mobilité sont utilisées?

M. Daniel Therrien: Je crois que c'est le cas, de manière générale, que les gens ne sont pas au courant des nombreuses manières dont leurs données sont utilisées. J'ose espérer que les utilisateurs de téléphones cellulaires savent que leurs données sont recueillies par Telus et peut-être par quelques entreprises comme Telus, mais ils ne savent pas en général que leurs données sont utilisées pour un programme comme celui-ci. Je crois que c'est assez clair.

Les Canadiens nous disent qu'ils partent du principe que leurs données sont utilisées aux fins pour lesquelles ils les ont fournies à l'entreprise ou au service en question, et peut-être à quelques autres fins. Mais ils ne savent à combien de fins elles peuvent être utilisées de nos jours. Les gens ne s'attendent pas à cela. Je crois que c'est assez clair.

Le président: Merci.

Je crains que nous n'ayons plus de temps.

Mme Lisa Hepfner: Nous n'avons plus de temps, d'accord.

Le président: Monsieur Villemure, vous avez maintenant la parole pour deux minutes et demie.

[*Français*]

M. René Villemure: Merci, monsieur le président.

Monsieur le commissaire, je vous remercie de votre franchise et de votre précision.

J'imagine que le commissariat à la protection de la vie privée existe pour maintenir la confiance du public en matière de vie privée. Vous avez parlé de la confiance lors de votre allocution, et nous savons tous que, quand la confiance n'est pas au rendez-vous, c'est la méfiance qui prend le relais, puis, éventuellement, la défiance.

Croyez-vous que ces incidents — je ne veux pas utiliser le mot « scandales » — autour de la vie privée effritent la confiance du public, en général, envers les autorités?

M. Daniel Therrien: Oui, et le gouvernement a déposé un projet de loi au cours de la précédente législature précisément pour rehausser la confiance des Canadiens pour ce qui est de l'utilisation de leurs données.

M. René Villemure: En effet, on a pu constater qu'elle était un peu déficiente, d'ailleurs.

Nous avons discuté de la réglementation européenne un peu plus tôt. Je crois que vous avez fait référence au Règlement général sur la protection des données de l'Union européenne.

M. Daniel Therrien: Oui.

M. René Villemure: Dans ce règlement, qu'est-ce qui pourrait être « importé » dans notre législation?

M. Daniel Therrien: Je vais reprendre un peu la réponse que j'ai donnée tantôt à M. Green. Dans nos rapports annuels, nous avons expliqué cela en général.

Je reprends la partie de votre question qui concerne la confiance. Le consentement et le contrôle sont des façons de s'assurer que les Canadiens ont confiance. Toutefois, je ne crois pas que les Canadiens ou que les usagers en général, de par le monde, veulent devoir consentir ou ne pas consentir à la myriade d'utilisations qui sont faites de leurs données. Les Canadiens veulent pouvoir utiliser les moyens technologiques modernes en ayant l'assurance que leurs droits ne seront pas violés. Cela repose en partie sur le consentement individuel, mais cela repose surtout sur l'assurance qu'ont les citoyens que quelqu'un est là pour protéger leurs intérêts. Or cette personne doit avoir les pouvoirs nécessaires pour le faire.

M. René Villemure: Au fond, les citoyens doivent donc être en mesure de comprendre cela et vous accorder et vous déléguer leur confiance.

● (1150)

M. Daniel Therrien: Oui. Ils doivent, d'une part, exercer leur consentement et, d'autre part, déléguer leur confiance.

M. René Villemure: Je vous remercie.

[*Traduction*]

Le président: Merci.

Nous donnons maintenant la parole à M. Green pour deux minutes et demie.

M. Matthew Green: Merci.

Des points très intéressants ont été soulevés ici, particulièrement en ce qui concerne l'idée d'une loi fondée sur les droits.

M. Therrien a souligné dans sa déclaration préliminaire que Justice Canada avait utilisé une approche semblable dans ses propositions pour la modernisation de la *Loi sur la protection des renseignements personnels.* Il a déclaré que certaines personnes préféreraient que les renseignements dépersonnalisés soient exclus du champ d'application des lois sur la protection des renseignements personnels. Selon M. Therrien, qui chercherait à tirer profit de l'exclusion des renseignements dépersonnalisés du champ d'application de ces lois?

M. Daniel Therrien: De toute évidence, ce serait des personnes qui souhaiteraient innover avec le moins de limitations ou de restrictions possible, comme l'idée que les renseignements dépersonnalisés ne seraient plus assujettis aux lois sur la protection des renseignements personnels.

M. Matthew Green: D'entrée de jeu, pour dépersonnaliser des renseignements, il faut d'abord en connaître la source.

M. Therrien pourrait-il peut-être commenter sur la question de savoir si, oui ou non, il aurait pu y avoir...? Peut-être que cela concerne de trop près l'enquête; je vais laisser tomber la question.

Il a évoqué l'idée d'élargir le pouvoir d'effectuer des vérifications proactives du gouvernement et du secteur privé. J'aimerais qu'il fasse part de ses réflexions, qu'il explique la forme que cela pourrait prendre et peut-être aussi qu'il en dise plus sur la définition des intérêts commerciaux légitimes. Je vous avoue que je suis très préoccupé par la marchandisation des renseignements privés et de la manière dont ils sont utilisés sous forme de métadonnées.

M. Daniel Therrien: Pour ce qui est des vérifications proactives, je dirai ceci. Le but n'est pas d'être une épine au pied du gouvernement ou des entreprises qui veulent innover de manière responsable. Le fait est que les flux de données sont si complexes et les modèles commerciaux sont si complexes que les Canadiens sont mal placés pour reconnaître les atteintes à la vie privée *[difficultés techniques]* et qu'un organisme comme le Commissariat est mieux placé, non pas pour poursuivre des milliers d'entreprises par année, mais, en fonction des risques, de, une fois de plus, regarder sous le capot à un certain nombre d'endroits où nous pensons qu'il pourrait y avoir des risques. Nous pourrons soit assurer les Canadiens quant au fait que la loi a été respectée ou intervenir et sanctionner les entreprises qui ne se sont pas conformées à la loi; tout cela, afin d'accroître la confiance dans le système.

Le président: Merci.

M. Matthew Green: Monsieur le président, pourrais-je poser...

Le président: Je crains que vous n'ayez plus de temps, monsieur Green.

M. Matthew Green: À titre de rappel au Règlement, pour ce qui est de l'information dont il a parlé, pouvons-nous lui demander, par votre entremise, de fournir par écrit le cadre explicite dont il a parlé?

Le président: Je crois que vous venez de le faire.

Une fois de plus, monsieur Green, je sais que vous aimez beaucoup n'utiliser...

M. Matthew Green: L'avoir par écrit.

Le président: ... un rappel au Règlement que lorsque l'on s'écarte vraiment des pratiques courantes ou de la règle du Comité. Merci, monsieur Green.

Nous allons donner la parole à M. Brassard. Je crois comprendre qu'il commencera et qu'il va peut-être diviser ses cinq minutes.

Allez-y, monsieur Brassard.

M. John Brassard: Merci, monsieur le président.

Monsieur Green, il était juste d'invoquer le Règlement, soit dit en passant.

Monsieur Therrien, tout d'abord, vous nous avez donné amplement de quoi réfléchir aujourd'hui. Je veux vous remercier de votre franchise.

Je veux parler des données qui sont adéquatement dépersonnalisées. Vous dites que le jumelage de données entraîne toujours un risque. Nous savons que, par ce processus, ou nous avons appris que, par ce processus... Telus a recueilli les données. Elles ont été transmises à une source secondaire appelée BlueDot, dont le travail consisterait à recueillir ces données, à les évaluer et à fournir des conseils à l'ASPC, qui a fini par devenir le client.

Quels sont les risques liés à la dépersonnalisation des données par une entreprise dont le travail a justement trait à ce genre de situation? Contentez-vous simplement de parler des risques, si vous le voulez bien.

M. Daniel Therrien: Je ne me pencherais pas sur les motifs d'une entreprise. Je me pencherais sur les mesures de protection que nous appliquons.

M. John Brassard: C'est là où je voulais en venir.

M. Daniel Therrien: C'est ce sur quoi nous ferions enquête.

M. John Brassard: En effet. Nous avons entendu des experts en sécurité et des experts en protection des renseignements personnels dire publiquement — nous ne l'avions pas entendu devant le Comité, à ce moment-là — que les mesures de protection et les protocoles adéquats doivent être mis en place à la source. S'ils ne le sont pas, il y a alors un risque important que ces renseignements soient repersonnalisés.

M. Daniel Therrien: Monsieur Turcotte, vous voudrez peut-être répondre à cette question.

● (1155)

[*Français*]

M. Martyn Turcotte (directeur, Direction de l'analyse des technologies, Commissariat à la protection de la vie privée du Canada): Oui, monsieur le commissaire.

Je vais essayer de parler lentement, parce que je crois avoir des problèmes de microphone.

Lorsqu'on parle du risque de repersonnalisation...

[*Traduction*]

Le président: Veuillez m'excuser. Je dois vous interrompre, monsieur Turcotte. Les interprètes n'arrivent pas à faire leur travail. Je comprends que vous ne disposez pas nécessairement du meilleur casque d'écoute pour cela.

Je vais peut-être renvoyer la question au commissaire Therrien pour qu'il y réponde.

M. Daniel Therrien: Nous pouvons répondre par écrit, mais je crois que M. *[difficultés techniques]*. Il serait bien placé lui aussi. Autrement, il nous ferait plaisir de répondre par écrit.

Le président: Sur ce, je crois que nous allons donner la parole à M. Paztzer.

Vous avez deux minutes et demie.

M. Jeremy Patzer (Cypress Hills—Grasslands, PCC): Merci beaucoup, monsieur le président.

Monsieur Therrien, je crois que les Canadiens ont en général été plutôt inquiets et surpris d'apprendre que, comme l'a dit, je crois, un article que j'ai lu, l'ASPC a eu accès aux données de 33 millions d'utilisateurs. D'où la question: combien d'autres ministères ont eu accès aux renseignements personnels des gens, au gouvernement fédéral?

M. Daniel Therrien: Ce que nous avons tout particulièrement constaté durant la pandémie, c'est que les gouvernements, non pas seulement le gouvernement du Canada, mais les gouvernements en général, demandent au secteur privé de développer des programmes numériques pour fournir des services. Ce n'est pas nécessairement une mauvaise chose, mais nous constatons que les secteurs public et privé interagissent de plus en plus entre eux au chapitre de la gestion des données.

Une fois de plus, ce n'est pas une mauvaise chose. Cela doit être correctement réglementé selon des critères établis et faire l'objet d'enquêtes, lorsqu'il le faut, mais il y a certainement d'autres ministères qui font cela.

M. Jeremy Patzer: Oui. Je crois que ce qui inquiète les gens, en général, toutefois, c'est que le gouvernement recueille leurs données personnelles, et puisse ensuite les utiliser contre eux. Est-ce une préoccupation? Existe-t-il des mesures de protection pour empêcher que cela se produise?

M. Daniel Therrien: S'il est question des renseignements personnels recueillis par le gouvernement fédéral, la *Loi sur la protection des renseignements personnels* prévoit certaines mesures de protection. C'est une loi largement dépassée, qui date d'environ 40 ans, mais il serait exagéré de dire qu'il n'existe aucune mesure de protection.

M. Jeremy Patzer: Oui. Je crois que c'est certainement problématique.

Ma dernière question renvoie à la fois où vous avez comparu, en 2020, devant le comité de l'industrie, dont j'étais membre à l'époque. Vous avez indiqué que, lorsqu'elles sont bien conçues, les applications de traçage peuvent à la fois remplir les objectifs en matière de santé publique et assurer la protection des droits. Je me souviens que, à l'époque, vous aviez certaines préoccupations à ce sujet, étant donné que le gouvernement ne vous avait pas consulté à ce moment-là. Comment ces préoccupations ont-elles été dissipées et qu'est-ce qui a été fait pour empêcher cela?

M. Daniel Therrien: Votre question concerne-t-elle l'application Alerte COVID?

M. Jeremy Patzer: Oui.

M. Daniel Therrien: Nous avons largement été consultés au sujet de l'application Alerte COVID, et j'ai pu constater que les mesures de protection des renseignements personnels de cette application en particulier étaient en fait plutôt rigoureuses.

Le président: Merci.

Notre dernier intervenant sera M. Bains, pour cinq minutes.

M. Parm Bains (Steveston—Richmond-Est, Lib.): Merci, monsieur le président.

Merci à nos témoins de s'être joints à nous aujourd'hui.

Je sais que beaucoup de questions ont été posées. Vous avez dit que vous doutez fortement que les gens savent si leurs données sont protégées ou non. La semaine dernière, j'ai parlé de quelque chose de semblable.

Je pense à toutes sortes d'applications que les gens utilisent, partout au pays, qui vont de Google Maps aux autres applications que les gens ont sur leur téléphone. Il y en a probablement des centaines. En général, l'application vous demandera d'avoir accès à vos renseignements et à votre caméra. Vous avez dit que quelque chose doit être fait pour renforcer cette protection. Est-ce quelque chose qui selon vous devrait être inclus dans cette fonctionnalité?

● (1200)

M. Daniel Therrien: Je vais faire la distinction entre deux choses. Je vous ai entendu dire — ou peut-être ai-je mal compris — qu'il y a la question de la connaissance ou de la conscience des Canadiens et la question de la protection. Quant à savoir si les données des Canadiens ont été correctement protégées, c'est l'objet de notre enquête, donc, je ne dis pas qu'elles étaient protégées ou qu'elles ne l'étaient pas. C'est ce sur quoi nous allons faire enquête.

Pour ce qui est de la connaissance, oui, je continue à dire que la plupart des utilisateurs des services de Telus ne savaient probablement pas que leurs données étaient utilisées de cette manière. Nous avons jeté un coup d'œil aux politiques en matière de vie privée de Telus, et il y a quelque chose dans ces politiques, comme c'est souvent le cas dans les politiques de confidentialité des entreprises, qui informe les Canadiens que leurs données de mobilité pourraient, de manière dépersonnalisée, être utilisées pour ce qu'on appelle « le bien public ». Le terme « bien public » n'était pas utilisé dans le sens de « utilisées par le gouvernement et l'ASPC». Quoi qu'il en soit, nous savons que personne ne lit ces politiques de confidentialité. Elles sont longues, elles sont compliquées, et même les avocats ont de la difficulté à les comprendre. Ce n'est pas une très bonne façon d'informer les Canadiens de la manière dont leurs données seront utilisées. Je crois que, dans ce cas-ci, le gouvernement a probablement mieux réussi à informer les Canadiens avec la page Web TendancesCOVID. Quoi qu'il en soit, je crois qu'il est juste de dire que, en général, les Canadiens n'étaient pas au courant et qu'il faudrait en faire plus.

En toute franchise, il ne sera jamais possible d'informer les gens de toutes les utilisations qui seront faites de leurs renseignements, parce que ces utilisations sont trop nombreuses et que bon nombre d'entre elles sont légitimes ou faites pour le bien public. Si des données doivent être utilisées pour le bien public, le consentement ne peut être une condition préalable pour toutes ces utilisations pour le bien public. Le consentement a sa place, et la transparence a sa place. L'amélioration des politiques de confidentialité a sa place, mais la vraie solution est d'avoir une garantie qui s'appliquerait en l'absence de consentement lorsque des critères objectifs ont été définis, comme les intérêts commerciaux légitimes — qui j'en conviens devraient être mieux définis — ou le bien de la société, et la mise en application devrait être confiée à quelqu'un qui peut protéger les intérêts des Canadiens.

C'est un domaine compliqué. Ne perdons pas de vue le fait que les données peuvent être utilisées à bon escient, mais cela doit être mieux réglementé.

Le président: Vous avez le temps de poser une dernière question, monsieur Bains.

M. Parm Bains: Quelle est votre norme concernant la protection adéquate des données?

Le président: En 10 secondes ou moins.

M. Daniel Therrien: Est-ce pour le bien de la société, ou pour favoriser des intérêts commerciaux légitimes, d'une part? D'autre part, cela viole-t-il la protection de la vie privée en tant que droit de la personne? Cela constitue-t-il de la surveillance? Vous trouvez un juste équilibre et vous déterminez si l'utilisation des données est adéquate de cette façon.

Le président: Merci beaucoup.

Sur ce, nous mettons fin à nos travaux pour le premier groupe de témoins de la réunion d'aujourd'hui. Je suis sûr que tous les membres se joindront à moi pour remercier le commissaire Therrien et M. Turcotte.

J'aimerais passer immédiatement au deuxième groupe de témoins. Je vais vous faire grâce des déclarations de procédure, car je pense que tout le monde était là, y compris notre témoin qui était observateur.

Je vais suspendre la séance pendant un bref instant pour une vérification du son, puis nous commencerons avec le deuxième groupe de témoins.

● (1200)

_____(Pause)_____

● (1205)

Le président: Nous reprenons la séance avec notre deuxième groupe de témoins.

Sans plus tarder, j'invite notre témoin, M. Khaled El Emam, à présenter sa déclaration liminaire d'un maximum de cinq minutes, après quoi nous ferons un seul tour de table de six minutes chacun.

Allez-y, monsieur El Emam.

M. Khaled El Emam (chaire de recherche du Canada en intelligence artificielle médicale, à titre personnel): Merci, monsieur le président et membres du Comité.

Le but de mes commentaires est d'offrir une vue d'ensemble de la dépersonnalisation. Comme j'ai travaillé dans ce domaine pendant près de 20 ans, tant dans le milieu universitaire que dans l'industrie, c'est peut-être à cet égard que je peux être utile à l'étude du Comité. Je ne peux pas commenter les détails de l'approche adoptée par Telus et l'ASPC, car je ne dispose pas de cette information. Je me concentre sur l'état du domaine et la pratique.

Il est important de clarifier la technologie. Des termes comme anonymisation, dépersonnalisation et agrégation sont utilisés de façon interchangeable, mais ils ne signifient pas la même chose. Il est plus précis de parler du risque de réidentification. Lorsque l'on partage des ensembles de données à des fins secondaires, comme c'est le cas ici, l'objectif est de s'assurer que le risque de réidentification est très faible.

Il existe de solides précédents concernant la définition d'un risque très faible, qui proviennent de la publication de données par, par exemple, Santé Canada, des conseils de la commissaire à la protection de la vie privée de l'Ontario et des applications des organismes de réglementation européens et des ministères de la Santé aux États-Unis. Par conséquent, l'acceptation d'un risque très faible n'est généralement pas controversée, car nous nous appuyons sur ces précédents qui ont très bien fonctionné dans la pratique.

Si nous disions que la norme est le risque zéro, alors toutes les données seraient considérées comme identifiables ou comme des renseignements personnels. Cela aurait de nombreuses conséquences négatives pour la recherche en santé, la santé publique, le développement de médicaments et l'économie des données en général au Canada. En pratique, un seuil de risque très faible est fixé, et l'objectif est de transformer les données pour atteindre ce seuil.

Il existe de nombreux types de transformations permettant de réduire le risque de réidentification. Par exemple, les dates peuvent être généralisées, la granularité des lieux géographiques peut être réduite, et du bruit peut être ajouté aux valeurs des données. Nous pouvons créer des données synthétiques, c'est-à-dire des données factices qui conservent les modèles et les propriétés statistiques des données réelles, mais pour lesquelles il n'existe pas de correspondance directe avec les données originales. D'autres approches faisant appel à des schémas cryptographiques peuvent également être utilisées pour permettre une analyse sécurisée des données. Tout cela pour dire qu'il existe une panoplie de technologies permettant de renforcer la protection des renseignements personnels en vue d'un partage responsable des données individuelles, et que chacune d'entre elles présente des avantages et des inconvénients.

Au lieu de partager des données individuelles, il est également possible de ne partager que des statistiques sommaires. Si cela est bien fait, le risque de réidentification est très faible. Étant donné que la quantité d'information dans les statistiques sommaires est considérablement réduite, elle ne répond pas toujours aux besoins d'une organisation. Si c'est le cas, cela peut être une bonne option, et c'est ainsi que nous avons tendance à définir les « données agrégées ».

En pratique, pour les ensembles de données qui ne sont pas diffusés au public, des contrôles supplémentaires en matière de sécurité, de confidentialité et de contrats doivent être mis en place. Le risque est géré grâce à une combinaison de transformations de données et de ces mesures de contrôle. Il existe des modèles permettant de garantir que la combinaison des transformations de données et des contrôles présente globalement un très faible de risque de réidentification.

Il existe d'autres pratiques exemplaires pour une réutilisation et un partage responsables des données, comme la transparence et la surveillance de l'éthique. La transparence consiste à informer les personnes des fins auxquelles leurs données sont utilisées et peut comprendre une option de refus. L'éthique suppose une forme d'examen indépendant des finalités du traitement des données afin que l'on s'assure qu'elles ne sont pas nuisibles, surprenantes, discriminatoires ou simplement effrayantes. En particulier pour les données sensibles, une autre approche consiste à lancer une attaque au chapeau blanc à l'égard des données: une personne est chargée de lancer une attaque de réidentification afin de tester de façon empirique le risque de réidentification. Cela peut s'ajouter aux autres méthodes et fournir une garantie supplémentaire.

Tout cela signifie que nous disposons de bons modèles techniques et de gouvernance pour permettre la réutilisation responsable des ensembles de données et que de multiples technologies de renforcement de la confidentialité, mentionnées plus tôt, permettent de soutenir la réutilisation des données.

Tout le monde adopte-t-il ces pratiques? Non. L'un des problèmes tient à l'absence de directives réglementaires ou de codes de pratique clairs et pancanadiens pour la création de renseignements non identifiables qui tiennent compte des avantages énormes de l'utilisation et du partage des données et des risques de ne pas le faire. Cela, ainsi qu'une plus grande clarté dans la loi, réduirait l'incertitude, fournirait une orientation claire sur ce que sont des approches raisonnables et acceptables, et permettrait aux organisations d'être évaluées ou vérifiées pour qu'elles puissent démontrer leur conformité. Bien que des efforts aient été déployés, par exemple par le Canadian Anonymization Network, il faudra sans doute attendre un certain temps avant qu'ils ne donnent des résultats.

● (1210)

Le président: Vous avez une minute, s'il vous plaît.

M. Khaled El Emam: J'ai rédigé un livre blanc contenant 10 recommandations pour réglementer les données non identifiables, que je peux transmettre au Comité si celui-ci souhaite l'examiner.

Pour conclure, bien que je n'aie pas évalué les mesures prises dans cette situation, j'espère que mes commentaires pourront aider le Comité à faire son travail.

Je vous remercie. Je suis prêt à répondre à vos questions.

Le président: Merci beaucoup.

Avant de commencer, je rappelle à tous les membres que nous allons faire un seul tour de six minutes, alors si quelqu'un souhaite partager son temps, qu'il le fasse savoir.

Sur ce, je vais commencer par M. Brassard.

M. John Brassard: Merci, monsieur le président.

Monsieur El Emam, je me réjouis vraiment de votre présence ici aujourd'hui.

Évidemment, nous sommes en train de déterminer certains des risques associés à la collecte de données sur la mobilité de l'Agence de la santé publique du Canada par l'entremise de quelques organisations. Je sais que vous êtes un expert dans ce domaine de la réidentification des données dépersonnalisées et désagrégées. Pouvez-vous nous parler des risques qui y sont associés?

M. Khaled El Emam: Si les données sont dépersonnalisées à l'aide de pratiques connues, de bonnes pratiques, alors les risques peuvent être très faibles. Il existe de nombreux précédents d'organisations réputées au Canada et à l'étranger quant à ce qui est considéré comme un risque acceptable, et nous pouvons mesurer ces risques et appliquer des techniques pour ramener le risque à un niveau acceptable. Les méthodes sont bien établies et sont utilisées dans la pratique depuis un certain temps.

M. John Brassard: Pouvez-vous parler de certaines de ces méthodes qui peuvent être utilisées pour réidentifier de telles données?

M. Khaled El Emam: Oui, certainement.

Pour dépersonnaliser les renseignements, il existe des transformations réelles comme réduire la granularité de la géographie, pour avoir des zones géographiques de plus en plus grandes, par exemple, ou réduire la granularité des dates pour avoir des intervalles de plus en plus grands; au lieu de jours, vous pouvez avoir des semaines ou une période plus longue. Vous pouvez utiliser des données synthétiques, c'est-à-dire créer des données factices qui ressemblent aux vraies données, mais qui ne concernent pas les individus. Vous pouvez utiliser des techniques cryptographiques, c'est-à-dire crypter les données et effectuer l'analyse sur les données cryptées.

Un certain nombre de technologies différentes ont été mises au point et peuvent être utilisées à cette fin. Le choix, bien sûr, dépendra des objectifs de l'Agence de la santé publique et du type d'analyse qu'elle effectue, mais il y a des options.

M. John Brassard: J'ai vu des études et des rapports. Une étude européenne a été réalisée. Le *New York Times* a réalisé une étude incroyable sur la facilité avec laquelle il est possible de réidentifier des données à partir d'un, de deux, de trois, de quatre ou de cinq points de données relevés.

Pouvez-vous nous parler de ces points de données et de la vulnérabilité que crée la réidentification de ces données?

M. Khaled El Emam: Si de bonnes méthodes ont été appliquées, le risque de réidentification peut être très faible. Je pense que, dans nombre de ces exemples, les bonnes méthodes n'ont pas été appliquées. Ils démontrent l'importance d'appliquer de bonnes méthodes et de bonnes pratiques.

Comme je l'ai mentionné, le risque ne sera pas nul. Il y a toujours un certain risque. Vous gérez ce risque résiduel en mettant en place des contrôles supplémentaires, tels que des contrôles de sécurité, des contrôles de confidentialité et des contrôles contractuels supplémentaires.

De façon générale, le risque peut être assez faible. Les approches fonctionnent bien dans la pratique lorsqu'elles sont appliquées correctement.

● (1215)

M. John Brassard: Tout au long du processus, on nous a dit que la question du consentement était importante. Souvent, il y a une exigence alambiquée pour fournir le consentement, et souvent, les gens ne sont pas conscients que leurs données font l'objet d'une surveillance.

Pouvez-vous également parler de l'importance du consentement?

M. Khaled El Emam: Comme l'a mentionné le commissaire Therrien, dans des cas comme celui-ci, il peut être peu pratique d'obtenir un consentement a priori. C'est pourquoi les méthodes de dépersonnalisation, les contrôles supplémentaires, la transparence et les examens éthiques permettent de garantir que les données ne sont plus identifiables et qu'elles sont utilisées de manière responsable.

M. John Brassard: L'autre domaine sur lequel vous vous êtes concentré... J'ai lu certains de vos travaux sur la génération de données synthétiques pour le partage des données sur la santé dans le respect de la vie privée. Le Comité ne se contente pas d'examiner ce qui s'est passé avec la Santé publique; il se tourne également vers l'avenir et pourrait présenter au gouvernement des recommandations sur les changements à apporter à la collecte de ces données pour préserver la protection de la vie privée des personnes.

Si vous n'y voyez pas d'inconvénient, pourriez-vous parler un peu plus de la génération de données synthétiques?

M. Khaled El Emam: Oui. L'idée est de commencer avec les données réelles et de construire un modèle d'apprentissage automatique ou d'IA qui apprend tous les modèles des données réelles, puis de générer de nouvelles données à partir de ce modèle.

Les données générées n'ont aucune correspondance avec les données d'origine. Elles ne correspondent pas à des personnes réelles. Ce sont des données factices générées à partir d'un modèle, mais elles conservent les propriétés et les caractéristiques des données réelles. Vous pouvez effectuer de nombreux types d'analyses et de surveillance — dans ce cas, la surveillance de la santé publique — en utilisant les données synthétiques, tout en assurant une forte protection des renseignements personnels.

M. John Brassard: Le risque pour la vie privée est-il réduit si vous utilisez ce type de génération de données?

M. Khaled El Emam: Oui. Les risques seront assez faibles.

M. John Brassard: Merci, monsieur le président.

Le président: Sur ce, nous passons à Mme Saks, pour six minutes.

Mme Ya'ara Saks (York-Centre, Lib.): Merci, monsieur le président.

Merci, monsieur El Emam, de vous joindre à nous aujourd'hui. D'emblée, j'aimerais dire que je suis sûre que le Comité et mes collègues ici présents seraient plus qu'heureux de voir les recommandations du livre blanc auxquelles vous avez fait allusion dans votre déclaration liminaire, afin de nous guider et de nous aider à être mieux informés à mesure que nos travaux progressent.

Vous avez mentionné ici dans les points clés de la collecte de données que la transparence est essentielle. Vous avez dit que les ensembles agrégés et la façon dont ils sont recueillis et présentés sont également essentiels, et que les entrepreneurs privés visent le bien de la société, qu'ils utilisent les garde-fous appropriés en travaillant sur ces données et qu'ils les fournissent à des fins d'utilisation.

Nous avons déjà établi que le gouvernement a été transparent tout au long du processus, à partir de mars 2020, avec ses indications concernant l'utilisation des données. Le commissaire nous a parlé d'un cadre publié disponible — pour répondre à la demande de M. Green — sur la meilleure façon d'utiliser les données anonymisées et agrégées. Merci d'avoir précisé la différence; c'est très utile.

En ce qui concerne l'importance pour les entrepreneurs avec lesquels nous travaillons pour recueillir ces données de viser le bien de la société, diriez-vous que Telus et BlueDot — et nous avons vu le rapport de BlueDot, qui a été soumis au Comité — sont généralement parmi ceux qui visent le bien commun dans la fourniture de données?

M. Khaled El Emam: Je n'ai pas les détails de l'utilisation que BlueDot et Telus font de leurs données, mais le cas actuel de l'Agence de la santé publique, qui utilise les données sur la mobilité pour comprendre les schémas de transmission est une utilisation raisonnable de données à des fins de surveillance de la santé publique.

Mme Ya'ara Saks: Vous diriez donc que, dans le cas de la pandémie et de la COVID-19, l'utilisation des données agrégées visait le bien de la société et constituait une bonne finalité.

M. Khaled El Emam: Oui. Comme on l'a dit à la réunion du Comité la semaine dernière, de nombreux pays dans le monde utilisent les données sur la mobilité à des fins de surveillance de la santé publique. Elles ont également été utilisées avant la pandémie par les Nations unies, par exemple, pour suivre le déplacement des personnes, et il n'est donc pas rare de le faire.

● (1220)

Mme Ya'ara Saks: Exact.

Pour clarifier, le but de notre étude était d'essayer de comprendre si les données que l'ASPC recevait, de la part tant de BlueDot que de Telus, répondaient aux critères de confidentialité dont vous avez parlé en nous assurant qu'elles étaient agrégées et anonymisées lorsque l'ASPC les recevait. Dans ce cas, en ce qui concerne les risques dont vous parliez et que mon collègue M. Brassard a mentionnés, est-ce que l'ASPC, à partir des données qu'elle a reçues, serait en mesure de réidentifier les données?

M. Khaled El Emam: Je ne pourrais pas vous donner cette réponse, parce que je n'ai pas examiné les données et que je n'ai pas fait cette analyse, mais je pense que c'est l'objectif de l'enquête du CPVP.

Mme Ya'ara Saks: Dans le même ordre d'idées, nous avons déjà discuté du fait que les données sont importantes pour la recherche en santé, et vous avez dit que vous étiez tout à fait en faveur de cela. Avez-vous vu, dans les discussions publiques et dans ce que la Dre Tam a publié sur l'outil de suivi de la COVID-19, quelque chose qui pourrait vous alarmer après vos nombreuses années de travail dans ce domaine?

M. Khaled El Emam: L'information qui a été présentée au sujet de la surveillance de la santé publique est typique du genre d'information qui serait utilisée par d'autres organismes de santé publique à cette fin.

Mme Ya'ara Saks: Dans ce cas, on a lancé beaucoup de chiffres et de renseignements. J'ai entendu 33 millions. Je pense que Telus serait ravie de savoir qu'elle compte 33 millions de clients. D'après ce que j'ai compris, les données recueillies auprès de Telus et de BlueDot étaient plutôt de l'ordre de 14 millions, si tant est que ce soit le cas. S'agirait-il d'un échantillon juste de données agrégées qui pourrait être utilisé à l'échelle nationale par l'Agence de la santé publique si elles sont agrégées et anonymisées?

M. Khaled El Emam: Si l'objectif était de faire de la surveillance de la santé publique à l'échelle nationale et si les données étaient distribuées pour que l'on dispose d'une couverture appropriée, alors oui, ce serait un ensemble de données utiles à cette fin.

Mme Ya'ara Saks: Vous avez parlé de surveillance, mais j'aimerais préciser qu'il ne s'agit pas de surveiller des Canadiens individuels; il s'agit de comprendre des ensembles de données sur les déplacements. Corrigez-moi si j'ai tort.

M. Khaled El Emam: Oui, il s'agit d'une surveillance de la santé publique pour comprendre les schémas de transmission de la COVID dans ce cas particulier.

Mme Ya'ara Saks: Dans ce cas, l'Agence de la santé publique du Canada ne surveillait pas des Canadiens individuels avec les ensembles de données qu'elle a reçus par l'entremise de BlueDot et de Telus.

M. Khaled El Emam: Encore une fois, je ne peux pas dire exactement ce que ces entreprises ont fait avec ces données, mais les cartes et les rapports publics qui sont accessibles sont agrégés, et ils ne concernent pas les individus.

Mme Ya'ara Saks: Alors, avons-nous répondu aux critères initiaux de transparence dans les ensembles agrégés en les partageant avec les Canadiens par l'intermédiaire de l'outil de suivi de la COVID-19 et d'autres méthodes?

M. Khaled El Emam: Pour les chiffres déclarés à ce niveau d'agrégation, il ne semble pas s'agir d'individus, mais pour ce qui est des données identifiables, je ne peux pas me prononcer sur le processus, ni sur les personnes qui s'en sont chargées, pas plus que sur les changements apportés en cours de route.

Mme Ya'ara Saks: D'accord. La protection des renseignements personnels est évidemment une grande préoccupation pour les membres du Comité et pour les Canadiens, qui veulent s'assurer que nous faisons bien les choses et que l'ASPC a suivi les lignes directrices du cadre présenté par le commissaire.

Le président: Votre temps est presque écoulé, madame Saks. Je ne suis pas sûr que nous ayons même le temps de poser une question de suivi. En fait, vous avez un peu dépassé le temps imparti.

Sur ce, je crains de devoir passer à M. Villemure.

[*Français*]

M. René Villemure: Merci, monsieur le président.

Monsieur El Emam, je vous remercie de vos lumières.

Je vous remercie surtout de ne pas répondre en confirmant les conclusions qui vous sont transmises sous forme de question.

Avez-vous déjà travaillé pour l'Agence de la santé publique du Canada ou pour le gouvernement du Canada?

[*Traduction*]

M. Khaled El Emam: Je travaille avec différents ministères depuis près de 20 ans. J'ai travaillé avec différentes parties du gouvernement ainsi qu'avec Santé Canada et l'Agence de la santé publique au cours de cette période.

● (1225)

[*Français*]

M. René Villemure: Bien évidemment. C'est normal.

Vous avez mentionné que vous avez participé à un comité récemment.

Avez-vous récemment été invité à participer à un comité au nom du gouvernement ou avez-vous été invité par d'autres partis politiques?

[*Traduction*]

M. Khaled El Emam: À quel comité faites-vous allusion?

[*Français*]

M. René Villemure: Vous avez dit plus tôt que vous aviez parlé de certaines choses récemment en comité. Je ne me souviens plus du propos exact, mais c'est votre phrase que je reprends.

[*Traduction*]

M. Khaled El Emam: Je faisais référence aux exposés présentés au Comité la semaine dernière au cours de la réunion avec le ministre de la Santé.

[*Français*]

M. René Villemure: D'accord. Merci.

Quand on parle de données ventilées ou de données anonymisées, on puise dans un lexique de spécialiste. Que peut comprendre le public dans cette affaire? Nous nous entendons tous pour dire que nous prenons au sérieux la protection de la vie privée et que nous visons à maintenir la confiance de la population, des citoyens ou des utilisateurs.

Alors, comment le public peut-il s'y retrouver dans un débat d'experts sur les données ventilées ou anonymisées? Le client qui utilise un téléphone cellulaire pour faire des appels ou pour faire des recherches sur le Web n'est pas au courant de cela.

[*Traduction*]

M. Khaled El Emam: Je pense que les points clés qui ressortent, c'est que nous savons très bien comment faire. Les méthodes et les technologies existaient déjà. Nous devons nous assurer que les organisations qui réutilisent les données à des fins légitimes et à des fins socialement bénéfiques utilisent et adoptent ces pratiques. Des codes de pratique, des normes et des lignes directrices précis ou applicables, ou applicables d'une manière ou d'une autre, seraient un moyen de s'assurer que ces bonnes pratiques sont adoptées chaque fois que des données sont réutilisées à des fins secondaires, et cela donnera une assurance au public.

[*Français*]

M. René Villemure: D'accord.

Les normes de pratique que vous évoquez constituent-elles le minimum requis ou assurent-elles, au contraire, une protection ultime?

[*Traduction*]

M. Khaled El Emam: L'Ontario a des normes en matière de dépersonnalisation. La commissaire à la protection de la vie privée de l'Ontario a publié de telles normes, par exemple nos lignes directrices. Ce sont de bonnes lignes directrices. Elles reflètent les bonnes pratiques actuelles. Il est toujours nécessaire de les mettre à jour régulièrement, mais je pense qu'une norme nationale serait très utile pour assurer l'uniformité à l'échelle du pays et pour les organisations qui exercent des activités à l'échelle nationale.

[*Français*]

M. René Villemure: Si on établissait des normes nationales, comme le réclame le commissaire à la protection de la privée du Canada, cela aurait comme conséquence souhaitée d'augmenter la confiance de la population à l'égard de l'utilisation secondaire des données.

[*Traduction*]

M. Khaled El Emam: Oui, tant que vous êtes également en mesure de démontrer que vous avez suivi ces normes, soit par des vérifications externes, soit par un autre mécanisme... Il est important de le démontrer.

[*Français*]

M. René Villemure: Je suis d'accord, la transparence et la démonstration sont en effet importantes.

On a beaucoup parlé de l'Agence de la santé publique du Canada. Parlons maintenant de Telus. Vous êtes dans ce domaine et vous connaissez donc bien la compagnie. Telus est-elle fiable en matière de vie privée dans le cadre de ses engagements à mettre les données au service du bien commun? S'agitil plutôt d'une jolie devanture?

[*Traduction*]

M. Khaled El Emam: Je ne peux vous faire part que de ce qui est connu publiquement. Le programme « Données au service du bien commun » de Telus s'est vu décerner cette année un prix pour la protection des renseignements personnels par l'International Association of Privacy Professionals, une association très respectée des professionnels de la protection de la vie privée dans le monde. C'est une indication que l'entreprise a mis en place de bonnes pratiques.

[*Français*]

M. René Villemure: Telus est donc reconnue et a gagné un prix cette année.

Le lien entre Telus et BlueDot comporte-t-il des risques?

[*Traduction*]

Le président: Monsieur Villemure, je crains que votre temps ne soit écoulé.

[*Français*]

M. René Villemure: D'accord.

[*Traduction*]

Le président: Si le témoin veut fournir une réponse écrite plus tard, il peut le faire, mais nous allons devoir maintenant passer à M. Green.

[*Français*]

M. René Villemure: Merci, monsieur le président.

[*Traduction*]

Le président: Allez-y, monsieur Green. Vous avez six minutes.

M. Matthew Green: Merci, monsieur le président. Comme toujours, j'apprécie qu'il soit possible de présenter des résultats et des réponses écrites plus étoffés.

Par votre entreprise, je tiens à souhaiter la bienvenue au Comité à l'expert en la matière que nous recevons ici aujourd'hui, M. El Emam. Je tiens à reconnaître que ce sujet est en grande partie nouveau pour moi et, j'en suis sûr, pour nombre de nos collègues, notamment la nature très technique de la technologie et là où nous nous situons en ce moment avec les mégadonnées.

Je vais m'en remettre à vous pour nous aider à y voir plus clair et me l'expliquer comme si j'avais cinq ans. Si vous avez déjà répondu à cette question, je vous demande d'essayer de la simplifier encore plus. Dans les exposés la semaine dernière, je suis sûr que vous vous rappellerez qu'on a utilisé un langage très spécifique au sujet des données anonymisées et dépersonnalisées... et bien sûr, de mon point de vue, la capacité d'obtenir des recommandations vraiment fermes de la part du Comité pour créer des normes de référence à l'échelle internationale en adoptant certaines des approches les plus rigoureuses fondées sur les droits à l'égard des données.

D'abord, je m'adresse à vous par l'entremise du président: compte tenu de votre rôle auprès de Replica Analytics, travaillez-vous avec des pays à l'échelle internationale, dans le monde entier, sur la technologie émergente que vous avez créée?

● (1230)

M. Khaled El Emam: Oui. J'élabore des technologies d'amélioration de la confidentialité depuis près de 20 ans et je les déploie par le truchement de logiciels et d'autres mécanismes dans le monde entier.

M. Matthew Green: À votre avis, quels sont les pays ou les régions — ou les lois, peut-être — que vous pourriez citer qui créent certaines des normes les plus élevées d'une formule fondée sur les droits?

J'ai beaucoup aimé que le commissaire à la protection de la vie privée parle de lois fondées sur les droits des consommateurs et de la possibilité d'offrir ces protections. Pourriez-vous fournir au Comité de bons exemples que nous pourrions inclure dans nos recommandations?

M. Khaled El Emam: En général, le RGPD en Europe est considéré comme l'un des règlements les plus stricts en matière de protection de la vie privée des individus. Je pense que le commissaire y a également fait référence dans ses réponses.

M. Matthew Green: Pour les besoins du Comité, pouvez-vous expliquer exactement ce que c'est et comment vous pensez que le règlement général sur la protection des données pourrait être appliqué à un contexte canadien?

M. Khaled El Emam: C'est une très bonne question. Le règlement lui-même définit certains paramètres généraux, et les organismes de réglementation ont élaboré des avis et des directives pour rendre opérationnels les principes et les concepts qui s'y rattachent. Il existe également le concept de codes de pratique, qui, à mon avis, peut être très utile pour définir des normes et des directives qui peuvent également être appliquées. Dans le cadre de notre discussion actuelle, il s'agit là de deux éléments à mentionner.

Le RGPD comporte de nombreux autres éléments qui, selon moi, sont bénéfiques, mais nous serions ici pendant longtemps si nous devions les passer tous en revue.

M. Matthew Green: Je vous en remercie. J'apprends aussi au fur et à mesure. Je vois que le RGPD comporte sept principes qui parlent de licéité, d'équité et de transparence; de limitation de la finalité; de minimisation des données; d'exactitude; de limitation du stockage; d'intégrité et de confidentialité; et de responsabilité.

Je sais que, dans le cadre de certains de mes travaux antérieurs sur les libertés civiles, en particulier sur la manière dont les forces de l'ordre utilisent les renseignements, nous avons entendu des histoires du secteur privé qui collecte des données en masse à des fins commerciales et permet ensuite une collecte subreptice de renseignements par le gouvernement.

Par conséquent, en ce qui concerne des choses comme la limitation du stockage, ou la limitation de la finalité ou de l'utilisation, y a-t-il des commentaires que vous voudriez fournir au Comité à partir de l'étude que nous avons devant nous aujourd'hui concernant les données sur la mobilité?

M. Khaled El Emam: La limitation de la finalité, je pense, est un principe important, et les limites de la conservation des données sont également importantes.

Il y a différentes façons de rendre cela opérationnel. L'une d'entre elles consiste à rendre les données anonymes ou à les dépersonnaliser après un certain temps, afin qu'elles ne soient plus des renseignements personnels. Cela recoupe notre discussion actuelle.

Pour ce qui est de la limitation de la finalité, nous devons également faire la distinction entre les renseignements personnels et les renseignements non personnels. Notre conversation d'aujourd'hui porte sur les renseignements non personnels...

M. Matthew Green: Je m'excuse de cette interruption.

Je pose la question parce que je pense que l'une des fausses définitions de la portée de cette question au cours des deux dernières réunions était cette idée que nous devrions limiter la conversation à la façon dont le gouvernement fédéral gère cette information.

Monsieur El Emam, je vous dirais que, à un moment donné, du côté commercial, avant de les acheter à Telus, il y aurait eu des processus pour la collecte de ces données. J'aimerais vous demander, dans vos commentaires, de réfléchir à la manière dont la collecte de données à la source pourrait être soumise aux mêmes normes que celles que nous aurions à l'interne au sein de mon propre gouvernement.

Je vais simplement vous faire part très clairement de mon inquiétude, à savoir que nous avons peut-être confié les atteintes à la vie privée à un secteur commercial qui n'a peut-être pas la même rigueur et, très franchement, les mêmes principes en matière de limitation de la finalité.

Pourriez-vous faire un commentaire rapide à ce sujet ou le mettre par écrit pour le bénéfice du Comité et pour les recommandations futures que nous pourrions formuler?

● (1235)

M. Khaled El Emam: Oui, bien sûr. Je vais dire rapidement deux ou trois choses.

Les entreprises ont besoin de recueillir des renseignements personnels pour mener leurs activités; c'est normal. Lorsqu'elles transmettent ces renseignements à d'autres entités, elles créent des ensembles de données non identifiables. En veillant à ce que cela soit fait correctement, et en y ajoutant la transparence et les contrôles éthiques, on obtient un bon modèle de gouvernance, de sorte que quiconque obtient les données a des contraintes ou des limites concernant ce qu'il peut en faire.

Ce modèle est bon lorsqu'il est mis en place. Il fonctionne bien dans la pratique. Nous devons simplement nous assurer qu'il est mis en place.

M. Matthew Green: Merci, monsieur le président.

Le président: Merci.

Je crois que j'ai passé tout droit et que je vous ai donné un peu plus de temps, monsieur Green.

J'aimerais maintenant remercier notre témoin de sa présence aujourd'hui.

Des voix: Bravo!

Le président: Nous allons maintenant passer aux travaux du Comité.

Plutôt que de passer directement à huis clos, je vais peut-être donner la parole aux députés s'ils souhaitent parler de notre plan de travail. Si nous voulons discuter de certains témoins, il serait peut-être préférable de le faire à huis clos, si tout le monde est d'accord. De cette façon, nous aurons la possibilité de discuter de choses qui ne devraient pas être publiques en ce qui concerne les témoins.

Allez-y, monsieur Brassard.

M. John Brassard: Merci.

Je propose que nous passions à huis clos pour en discuter.

Le président: Très bien.

M. John Brassard: Je tiens à dire à M. El Emam qu'il n'est pas fréquent qu'un témoin soit applaudi ici, mais sachez, monsieur, que vous avez été applaudi par nous tous. Merci de votre témoignage aujourd'hui.

Le président: Merci.

Sur ce, je vais suspendre la séance pour passer à un autre appel Zoom pour le huis clos.

[*La séance se poursuit à huis clos*.]