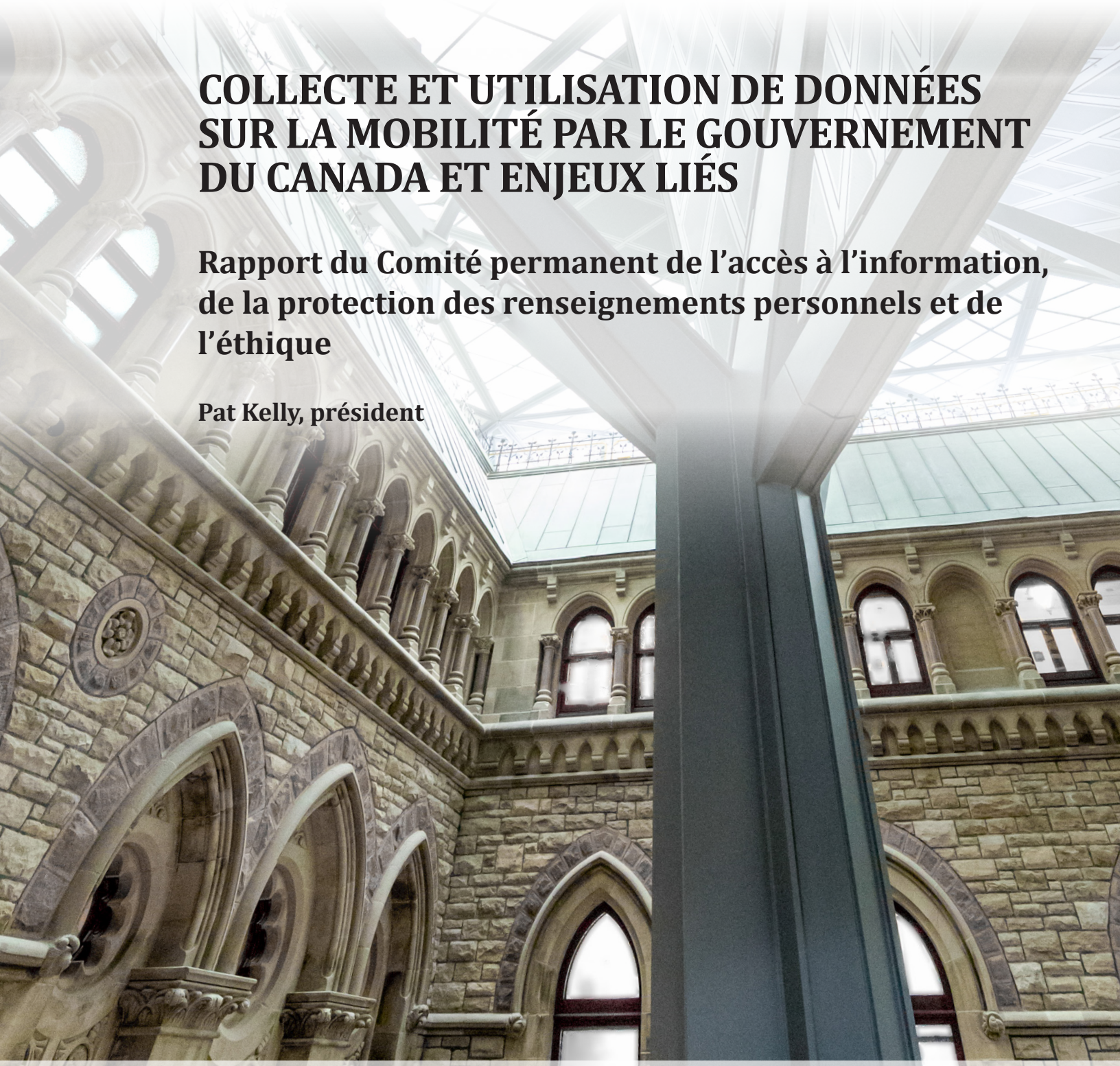
CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA



# COLLECTE ET UTILISATION DE DONNÉES SUR LA MOBILITÉ PAR LE GOUVERNEMENT DU CANADA ET ENJEUX LIÉS

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

**Pat Kelly, président**

**MAI 2022**
**44e LÉGISLATURE, 1re SESSION**

# COLLECTE ET UTILISATION DE DONNÉES SUR LA MOBILITÉ PAR LE GOUVERNEMENT DU CANADA ET ENJEUX LIÉS

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

**Le président**
**Pat Kelly**

**MAI 2022**

**44e LÉGISLATURE, 1re SESSION**

## AVIS AU LECTEUR

**Rapports de comités présentés à la Chambre des communes**

C'est en déposant un rapport à la Chambre des communes qu'un comité rend publiques ses conclusions et recommandations sur un sujet particulier. Les rapports de fond portant sur une question particulière contiennent un sommaire des témoignages entendus, les recommandations formulées par le comité et les motifs à l'appui de ces recommandations.

# COMITÉ PERMANENT DE L'ACCÈS À L'INFORMATION, DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET DE L'ÉTHIQUE

**PRÉSIDENT**

Pat Kelly

**VICE-PRÉSIDENTS**

Iqra Khalid

René Villemure

**MEMBRES**

Parm Bains

James Bezan

L’hon. Greg Fergus

Matthew Green

Lisa Hepfner

Damien C. Kurek

Ya’ara Saks

Ryan Williams

**AUTRES DÉPUTÉS QUI ONT PARTICIPÉ**

Richard Bragdon

John Brassard

Blaine Calkins

Julie Dabrusin

James Maloney

Jeremy Patzer

Sherry Romanado

Lianne Rood

Gerald Soroka

Len Webber

**GREFFIÈRE DU COMITÉ**

Nancy Vohl

**BIBLIOTHÈQUE DU PARLEMENT**

**Services d'information, d'éducation et de recherche parlementaires**

Sabrina Charland, analyste

Alexandra Savoie, analyste

# LE COMITÉ PERMANENT DE L'ACCÈS À L'INFORMATION, DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET DE L'ÉTHIQUE

a l’honneur de présenter son

**QUATRIÈME RAPPORT**

Conformément au mandat que lui confère l’article 108(3)h) du Règlement, le Comité a étudié la collecte et l’utilisation de données sur la mobilité par le gouvernement du Canada et a convenu de faire rapport de ce qui suit :

# TABLE DES MATIÈRES

# SOMMAIRE

Pendant la pandémie de COVID-19, le gouvernement du Canada et plusieurs autres gouvernements à travers le monde ont utilisé la technologie pour les aider à prendre des décisions en matière de santé publique.

Un exemple d'une telle utilisation est celle de l'Agence de la santé publique du Canada (ASPC), qui a utilisé des données sur la mobilité pour évaluer les tendances des déplacements des populations pendant la pandémie. Le 17 décembre 2021, un appel d'offres visant à lui permettre de continuer d'avoir accès à ce type de données a été publié. C'est dans ce contexte que le Comité a voulu entreprendre une étude sur la collection et l'utilisation de données sur la mobilité par le gouvernement du Canada.

Les représentants gouvernementaux ont affirmé que l'utilisation de données sur les mobilités s'est faite dans le respect du droit à la vie privée puisqu'il s'agissait de données dépersonnalisées et agrégées et qu'elles ont été utilisées pour suivre la corrélation entre la propagation de la COVID-19 et le mouvement de la population. Ils ont indiqué qu'il était impossible de repersonnaliser les données reçues afin d'identifier des Canadiens. Ils ont aussi indiqué avoir fait preuve de transparence, en rendant entre autres publique de l'information relative aux données sur la mobilité sur le site Web *TendancesCOVID*.

Les entreprises qui ont donné à l'ASPC accès à des données sur la mobilité ont rassuré le Comité qu'aucunes données identifiant un individu n'ont été partagées avec le gouvernement. Elles ont dit utiliser les meilleures normes de l'industrie pour partager des données dépersonnalisées de façon responsable.

D'autres témoins ont convenu que d'après les informations publiques disponibles sur l'affaire de l'ASPC, il ne semblait pas que le gouvernement ait utilisé autre chose que des données correctement dépersonnalisées pour évaluer les tendances de déplacement des populations.

Bien qu'il y ait eu un large consensus parmi les témoins pour dire que l'utilisation des données sur la mobilité à des fins de santé publique était louable, plusieurs témoins étaient d'avis que l'ASPC n'a pas fait preuve de suffisamment de transparence.

Un expert a expliqué qu'il existe des techniques fiables pour dépersonnaliser ou anonymiser les données de sorte que le seuil de réidentification soit très faible. Certains experts en matière de protection de la vie privée ont fait remarquer que puisque le risque de réidentification n'est jamais nul, les données dépersonnalisées devraient

tomber sous le champ d’application des lois fédérales en matière de protection des renseignements personnels.

Certains témoins ont mis en lumière les défis que crée l’utilisation des données sur la mobilité et les mégadonnées. Ils ont aussi discuté des impacts sociaux que la surveillance peut avoir.

Enfin, la plupart des témoins ont convenu que les lois fédérales en matière de protection des renseignements personnels ont grand besoin d'être modernisées.

À la lumière de ce que le Comité a entendu, il fait plusieurs recommandations visant à assurer qu’un cadre juridique approprié pour l’utilisation des données au Canada soit en place.

# LISTE DES RECOMMANDATIONS

*À l'issue de leurs délibérations, les comités peuvent faire des recommandations à la Chambre des communes ou au gouvernement et les inclure dans leurs rapports. Les recommandations relatives à la présente étude se trouvent énumérées ci-après.*

# COLLECTE ET UTILISATION DE DONNÉES SUR LA MOBILITÉ PAR LE GOUVERNEMENT DU CANADA ET ENJEUX LIÉS

## INTRODUCTION

Le 11 mars 2020, l'Organisation mondiale de la santé a annoncé que la COVID-19 pouvait être qualifiée de pandémie[1].

En raison de la pandémie, l'Agence de la santé publique du Canada (l'ASPC) a utilisé des données sur la mobilité pour évaluer les tendances des déplacements des populations. Les données sur la mobilité consistent en des indicateurs agrégés dérivés des données de localisation des tours de téléphonie cellulaire et des opérateurs, ou parfois de données de géolocalisation dépersonnalisées et agrégées, qui permettent une analyse de la mobilité (ou du mouvement) des populations au Canada[2]. Des questions relatives à cette utilisation et à l'intention de l'ASPC de continuer d'y avoir recours à l'avenir ont mené le Comité à entamer la présente étude.

Le 13 janvier 2022, le Comité a adopté à l'unanimité une motion visant à entreprendre son étude sur la collecte et l'utilisation de données sur la mobilité par le gouvernement du Canada.

En marge du cas d'étude impliquant l'ASPC, le Comité s'est intéressé aux enjeux liés à l'utilisation des données dépersonnalisées et des mégadonnées et à la modernisation des lois fédérales en matière de protection des renseignements personnels. Il aussi discuté des impacts de la surveillance et de l'importance de la transparence des institutions gouvernementales pour assurer la confiance du public. Ce rapport résume les témoignages entendus et inclut des recommandations visant à assurer un cadre juridique approprié pour l'utilisation des données au Canada.

1 Organisation mondiale de la santé, *Allocution liminaire du Directeur général de l'OMS lors du point presse sur la COVID-19 - 11 mars 2020*.

2 Achatseteventes.gc.ca, *Données et services de localisation basés sur les opérateurs pour l'analyse de la mobilité en matière de santé publique (1000236419)*; ETHI, *Témoignages*, Kamran Khan (président-directeur général et fondateur de BlueDot).

En tout, le Comité a tenu six réunions publiques et entendu 20 témoins. Il a aussi reçu 3 mémoires. Le Comité remercie tous ceux et celles qui ont participé à l'étude.

## CHAPITRE 1 : UTILISATION DES DONNÉES SUR LA MOBILITÉ PAR L'AGENCE DE LA SANTÉ PUBLIQUE DU CANADA

Le Tableau 1 présente un aperçu chronologique des événements clés entourant l'utilisation de données sur la mobilité par le gouvernement du Canada pendant la pandémie, dont il sera question dans le présent chapitre.

### Tableau 1— Événements clés liés à l'utilisation de données sur la mobilité par le gouvernement du Canada

| Date | Événement |
|---|---|
| 23 mars 2020 | Communiqué de presse du premier ministre annonçant que le gouvernement du Canada fournira un soutien à BlueDot et, par l'intermédiaire de l'Agence de la santé publique du Canada (ASPC), utilisera sa plateforme d'analyse des maladies pour soutenir la modélisation et la surveillance de la propagation de la COVID-19 et pour éclairer la prise de décisions gouvernementales au fur et à mesure que la situation évolue. |
| 24 mars 2020 | La Division de la gestion de la protection des renseignements personnels de Santé Canada et de l'Agence de la santé publique du Canada (DGPRP) indique qu'il n'y a pas de préoccupations en matière de protection des renseignements personnels en ce qui concerne les données qui seront fournies par BlueDot compte tenu du fait que ces données sont anonymisées et irrévocablement dépouillées d'identificateurs directs, qu'un code n'est pas conservé pour permettre un recouplage futur et que le risque de réidentification des personnes à partir des renseignements restants est très faible. Elle détermine qu'aucuns renseignements personnels ne seront reçus. |
| 21 avril 2020 | Le Centre de recherches sur les communications (CRC) d'Innovation, Sciences et Développement économique informe le Commissariat à la protection de la vie privée du Canada (le commissariat) de son intention d'accéder aux données dépersonnalisées de Telus afin de répondre aux questions de l'ASPC sur les tendances en matière de mobilité. |
| 22 avril 2020 | L'ASPC avise le commissariat de ses travaux sur les données relatives à la mobilité. Le commissariat indique que l'ASPC l'a contacté pour l'informer de son intention d'utiliser des données sur la mobilité en réponse à la COVID-19 et du fait que cette activité n'engageait pas la *Loi sur la protection des renseignements personnels*. |
| 24 avril 2020 | Un contrat est conclu entre Santé Canada et BlueDot. La date de début de la période contractuelle est le 26 mars 2020. |

| Date | Événement |
|---|---|
| 22 septembre 2020 | La DGPRP communique son analyse confirmant que les données de Telus (programme *Les données au service du bien commun*) ne sont pas considérées comme étant des renseignements personnels et n'engagent pas la *Loi sur la protection des renseignements personnels*. La DGPRP conclut que la publication subséquente de ces données n'entraînera pas de préoccupations ultérieures en matière de vie privée. |
| 21 décembre 2020 | La DGPRP, s'appuyant sur son opinion antérieure, indique que les données fournies par Telus par l'entremise du CRC ne constituent pas des renseignements personnels. |
| 24 décembre 2020 | Un contrat est conclu entre l'ASPC et Telus. La date de début de la période contractuelle est le 24 décembre 2020. |
| 25 janvier 2021 | L'ASPC consulte le Groupe consultatif en matière d'éthique en santé publique pour discuter de l'éthique de l'utilisation des données sur la mobilité. |
| Octobre 2021 | Le contrat de Telus expire. |
| Octobre 2021 | L'ASPC consulte le DGPRP pour la préparation d'une demande de proposition pour les données sur la mobilité. |
| 17 décembre 2021 | La demande de proposition (DP) est publiée sur le site achatsetventes.gc.ca. La DP précise les mesures de sécurité et de protection de la vie privée que les soumissionnaires doivent respecter. L'appel d'offres devait prendre fin le 21 janvier 2022. |
| Janvier 2022 | Le commissariat reçoit des plaintes à l'égard de la collecte et de l'utilisation de données sur la mobilité par l'ASPC et entame une enquête. |
| 6 janvier 2022 | L'ASPC fournit une séance d'information technique au commissariat. |
| 12 janvier 2021 | Un amendement à la DP repousse la date de fermeture de l'appel d'offres au 4 février 2022. |
| 4 février 2022 | Un amendement à la DP repousse la date de fermeture de l'appel d'offres au 18 février 2022 |
| 18 février 2022 | L'appel d'offres expire. |
| 18 mars 2022 | Le contrat de BlueDot expire. |

Source: Tableau préparé par la Bibliothèque du Parlement en utilisant de l'information que le Comité permanent de la Chambre des communes sur l'accès à l'information, la protection des renseignements personnels et l'éthique (ETHI) a obtenu et des sources publiques; Bureau du premier ministre du Canada, communiqué, 23 mars 2020; ETHI, *Témoignages*, 3 février 2022 (L'Hon. Jean-Yves Duclos, ministre de la Santé); ETHI, *Témoignages*, 7 février 2022 (Daniel Therrien, commissaire à la protection de la vie privée du Canada); Agence de la santé publique du Canada, réponse écrite distribuée au comité le 25 février 2022; Agence de la santé publique du

Canada, Lettre à ETHI, 11 mars 2022; Commissariat à la protection de la vie privée du Canada, Lettre à ETHI, 14 mars 2022; Gouvernement du Canada, appel d'offre, 3 février 2022; Gouvernement du Canada, demande de proposition; Gouvernement du Canada, *Bluedot Inc. - Détails du contrat*; Gouvernement du Canada, *Telus Communications Company - Détails du contrat*; Agence de la santé publique du Canada, communication, 5 avril 2022.

## Appel d'offres de décembre 2021

Le 17 décembre 2021, le gouvernement a publié un appel d'offres visant à permettre à l'ASPC d'avoir accès à des données de localisation des tours de téléphonie cellulaire anonymisées pour contribuer à la réponse à la pandémie de COVID-19 et pour d'autres applications de santé publique. La demande de proposition prévoit que la période du contrat débutera à sa date d'attribution et se terminera le 31 mai 2023, avec 3 périodes optionnelles supplémentaires d'un an.

Christopher Allison, vice-président par intérim chargé de la Direction générale de la sécurité des données organisationnelles de l'ASPC, a indiqué que l'idée derrière ce nouveau contrat est que les données sur la mobilité peuvent être très utiles pour l'examen d'une gamme de problèmes de la santé publique et pourraient être utiles pour l'ASPC à mesure qu'elle renforce son expérience dans l'utilisation efficace et éthique des données, tout en protégeant la vie privée. Le but est d'explorer ce qui pourrait être fait après la pandémie, sans préjuger toute décision que pourrait prendre l'ASPC.

Ann Cavoukian, directrice générale du International Council on Global Privacy and Security by Design et ancienne commissaire à l'information et la protection de la vie privée de l'Ontario, a dit qu'il est essentiel de fixer des limites spécifiques à l'utilisation des données en vertu de ce nouveau contrat, car sinon elles seront toujours utilisées à d'autres fins. Le commissaire à la protection de la vie privée du Canada (le commissaire), Daniel Therrien, a indiqué qu'il n'a pas été consulté à l'égard de cet appel d'offres, mais qu'il a demandé et reçu certaines informations à l'égard de l'appel d'offres concernant le processus de l'ASPC.

L'hon Jean-Yves Duclos, ministre de la Santé, a indiqué qu'un retard dans l'acquisition de données sur la mobilité pourrait avoir des répercussions sur les activités de suivi épidémiologique de la pandémie en cours. D^re^ Theresa Tam, l'administratrice en chef de la santé publique, a dit que des lacunes au niveau des données sur la mobilité réduiraient la capacité de l'ASPC à examiner d'importantes mesures stratégiques mises en place, mais qu'il est possible de les examiner rétrospectivement. Elle a toutefois souligné qu'une analyse rétrospective est moins bonne qu'une analyse prospective.

L'appel d'offres devait prendre fin le 21 janvier 2022. Par amendement daté du 12 janvier 2022, la date de fermeture a été repoussée au 4 février 2022.

Le 31 janvier 2022, le Comité a adopté la motion suivante à l'unanimité :

> Que le Comité demande au gouvernement de suspendre l'appel d'offres sur l'obtention des données cellulaires de l'Agence de la santé publique du Canada dès l'adoption de la présente motion, et que l'appel d'offres ne soit pas relancé avant que le Comité ne rapporte à la Chambre qu'il est convaincu que la vie privée des Canadiens ne sera pas affectée, et que le Comité fasse rapport à la Chambre de l'adoption de cette motion dès la première occasion.

Le 2 février 2022, le premier rapport du Comité a été présenté à la Chambre des communes. Il rapporte l'adoption de la motion susmentionnée.

Le 4 février 2022, un nouvel amendement à l'appel d'offres a repoussé la date de fermeture au 18 février 2022.

Le 8 février 2022, la Chambre des communes a adopté une motion visant à ce que le premier rapport du Comité soit agréé. Le vote était divisé : les partis de l'opposition votant pour la motion et le parti au pouvoir votant contre.

Le gouvernement n'a pas mis pause à l'appel d'offres. L'appel d'offres a expiré le 18 février 2022.

## Observations et recommandations du Comité

Le Comité reconnaît que la demande de proposition de décembre 2021 prévoyait dans ces critères techniques obligatoires que les plans des soumissionnaires devaient contenir « la possibilité pour les utilisateurs de se retirer facilement du programme de partage des données sur la mobilité ».

Le Comité est d'avis qu'il est important de s'assurer que dans tout processus d'appel d'offres les Canadiens comprennent qu'ils peuvent refuser de participer à une initiative de collecte de données. Il note également que, comme il sera expliqué dans ce rapport, il est souvent difficile pour les individus de comprendre les politiques de confidentialité. Il recommande donc :

**Recommandation 1**

**Que le gouvernement du Canada stipule dans toutes les futures demandes de propositions pour la collecte de données de Canadiens, que les Canadiens ont la possibilité de se retirer de la collecte de données, et que les instructions sur la méthode de retrait soient facilement comprises, largement communiquées et restent accessibles au public.**

Toutefois, le Comité reconnaît que dans certain cas, le refus de donner son consentement à une initiative de collecte de données pourrait desservir l'intérêt public. Le chapitre 3 du rapport discute de l'utilisation des données à des fins socialement bénéfiques et le chapitre 4 discute des modifications aux lois fédérales en matière de protection des renseignements personnels qui permettraient de mieux encadrer, entre autres, l'utilisation de données dépersonnalisées.

## Accès initial aux données sur la mobilité

Le ministre Duclos a expliqué qu'en mars 2020, l'ASPC a commencé à utiliser des données sur la mobilité. En partenariat avec le Centre de recherche sur les communications (CRC) relevant de l'Innovation, Sciences et Développement économique (ISDE), l'ASPC a utilisé des données de localisation anonymisées, dépersonnalisées, et regroupées. Les données étaient fournies dans le cadre d'un contrat à fournisseur unique avec le programme de Telus *Les données au service du bien commun*, qui a pris fin en octobre 2021. Un autre contrat a été conclu entre l'ASPC et BlueDot. Ce contrat devait prendre fin le 18 mars 2022.

Le ministre Duclos a dit qu'en avril 2020, il a été déterminé que les renseignements utilisés n'étaient pas des données personnelles et confidentielles selon les lois et règlements du Canada. Dans une lettre au Comité datée du 14 février 2022, D$^{r}$ Harpreet S. Kochhar, président de l'ASPC, a confirmé que les spécialistes de la protection des renseignements personnels du gouvernement ont effectué une évaluation de la protection des renseignements personnels visant à déterminer si les données que l'ASPC se proposait de recevoir devraient être considérées comme étant des renseignements personnels sous la *Loi sur la protection des renseignements personnels*. Ils ont conclu que les données ne contenaient pas de renseignements personnels et que leur utilisation ne contrevenait pas à la *Loi*.

L'ASPC a fournis au Comité des documents relatifs à l'évaluation des facteurs relatifs à la vie privée qui a été réalisée à l'égard de l'utilisation des données sur la mobilité par le gouvernement. Ils montrent qu'en mars 2020, la Division de la gestion de la protection des renseignements personnels de Santé Canada et de l'ASPC (DGPRP) a déterminé que le contrat avec BlueDot ne soulevait aucune préoccupation en matière de protection des renseignements personnels vu la nature des données (anonymisées) et le fait que Santé Canada n'allait pas recevoir des renseignements personnels. La DGPRP a noté que si des

renseignements personnels étaient reçus, certaines mesures auraient alors dû être incluses dans le contrat[3].

En septembre 2020, l'analyse de la protection des renseignements personnels de la DGPRP à l'égard du projet de tableau de bord des données sur la mobilité de l'ASPC a conclu qu'étant donné le processus d'agrégation exhaustif de Telus, les données reçues par l'ASPC ne correspondaient pas à la définition de « renseignements personnels » sous la *Loi sur la protection des renseignements personnels* (LPRP) et que la loi ne s'appliquait donc pas. La DGPRP était d'avis que la publication des données n'entraînerait pas de problèmes ultérieurs en matière de protection de la vie privée[4]. La DGPRP a réitéré que les données fournies par Telus par le biais du CRC ne constituaient pas des renseignements personnels en décembre 2020[5].

M. Allison a aussi mentionné que les experts consultés par l'ASPC et le Groupe consultatif en matière d'éthique en santé publique (GCESP) ont conclu qu'aucun renseignement personnel ou privé ne faisait partie des données sur la mobilité auxquelles l'ASPC a accès ni celles visées par l'appel d'offres de décembre 2021. D[re] Tam a confirmé que le GCESP a pris acte du fait que l'ASPC utilise des données anonymisées et agrégées pour prévenir toute atteinte à la vie privée.

Kathy Thompson, première vice-présidente de l'ASPC, a confirmé que l'agence a veillé à ce que les contrats conclus respectivement avec Telus et BlueDot, ainsi que la demande de proposition publiée en décembre 2021, soient assortis d'un certain nombre de conditions pour garantir la protection de la vie privée des Canadiens, de sorte qu'il soit impossible d'identifier qui que ce soit.

En octobre 2021, la DGPRP a déterminé, en évaluant l'énoncé des travaux pour une demande de proposition anticipée, qu'à moins que le processus d'obtention de données sur la mobilité ne soit modifié, son analyse antérieure s'appliquait. Il n'y avait pas, selon elle, de problèmes de protection des renseignements personnels liés aux données sur la

3 Agence de la Santé publique du Canada, Lettre au Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (ETHI), 11 mars 2022, p. 16.

4 *Ibid.*, pp. 40-42. La Division de la gestion de la protection des renseignements personnels de Santé Canada et de l'Agence de la Santé publique du Canada a fait référence à l'*Avis de mise en œuvre de la protection des renseignements personnels 2020-03 : protection des renseignements personnels lors de la diffusion de renseignements à propos d'un petit nombre de personnes* du Secrétariat du Conseil du Trésor.

5 *Ibid.*, p. 54.

mobilité auxquelles le gouvernement aurait accès à l'issue de cette demande de proposition[6].

Selon le ministre Duclos, les deux conditions permettant au gouvernement de protéger la vie privée sont remplies en l'espèce : le respect des lois et l'assurance « que les données recueillies ne peuvent pas créer d'enjeu ni de risque en lien avec la protection de la vie privée ». À savoir si les actions du gouvernement était éthique, le ministre Duclos a répondu que « dans le contexte de la COVID-19, le gouvernement canadien a l'obligation éthique, morale, économique et sanitaire de protéger la sécurité et la santé des gens, tout en protégeant absolument la vie privée des gens ».

## Telus et BlueDot : Type d'accès

M. Allison a noté que les données d'environ 9 millions d'abonnés font partie du programme *Les données au service du bien commun* de Telus. Les données sur la mobilité d'environ 5 millions d'appareils mobiles ont été utilisées par BlueDot pour fournir des rapports à l'ASPC[7].

Pamela Snively, vice-présidente et Chef des données et du Bureau des relations de confiance de la Société Telus Communications, a dit que le programme *Les données au service du bien commun* a été lancé en avril 2020. Elle a précisé que Telus n'a pas fourni « un iota » de renseignement personnel au gouvernement. Les ensembles de données n'ont jamais quitté les systèmes de Telus. Son programme exploite la plateforme Insights, qui utilise des ensembles de données dépersonnalisées tirées du réseau de Telus pour dresser un portrait des tendances et schémas de déplacement, sans compromettre la vie privée des gens.

M^me^ Snively a expliqué que Telus accorde un accès guidé et supervisé sur la plateforme Insights aux experts en science des données de ses partenaires. Ils peuvent y effectuer des requêtes conformes à l'utilisation et à la finalité prévue, tant qu'elles correspondent au programme. Ils sont en mesure de créer des données dérivées ou « aperçus » comme une carte de points chauds ou un graphique, un diagramme à colonnes ou un graphique linéaire, qui montre les habitudes ou tendances de mobilité. Ces « aperçus » peuvent être téléchargés, après que Telus les aient examiné pour s'assurer qu'ils soient cohérents, qu'ils respectent les paramètres de risque de repersonnalisation et qu'ils soient conformes à l'objet du contrat.

6 *Ibid.*, pp. 43-66.

7 Dr Kamran Khan, président-directeur général et fondateur de BlueDot, a confirmé ce nombre.

M^me^ Snively a expliqué que Telus a mis en place une plateforme et des règles techniques permettant de dépersonnaliser les données et de supprimer les identifiants. Des règles régissent la façon dont les requêtes sont effectuées et en contrôlent la fréquence. Des contrôles administratifs, comme l'accès supervisé et guidé, et des contrôles contractuels rigoureux qui interdisent la repersonnalisation, sont en place[8]. De plus, M^me^ Snively a confirmé que des essais et attaques de repersonnalisation rigoureux ont été faits par Telus et des experts pour garantir que le processus était étanche. Elle a aussi confirmé que Telus ne fournit jamais de données en temps réel, car cela augmenterait le risque de repersonnalisation.

M^me^ Snively a noté qu'Insights est la seule plateforme d'analyse de données sécurisée de ce type au Canada qui détient une certification « Privacy by Design », une norme internationale qui dépasse les exigences législatives au pays et qui ancre la démarche de protection de la vie privée dès la conception dans la conception et le fonctionnement des systèmes de technologie de l'information, des réseaux et des pratiques commerciales des organisations[9]. Le concept a été créé par M^me^ Cavoukian qui a souligné qu'il est intégré dans le Règlement général de la protection des données (RGPD) de l'Union européenne et permet « d'enchâsser les mesures de protection de la vie privée dans les codes de fonctionnement d'une organisation ».

D^r^ Khan, président-directeur général et fondateur de BlueDot, a indiqué que les données de localisation que BlueDot reçoit sont dépersonnalisées; parfois aussi préagrégées; parfois fournies au niveau des appareils. Il a souligné que BlueDot a mis en place de nombreuses procédures, tant administratives que de sécurité, pour gérer et conserver les données dans un environnement sécurisé. Il est donc impossible, selon lui, d'imaginer que les extrants que BlueDot analyse, produit et livre à l'ASPC puissent être associés de nouveau à une personne. Les deux fournisseurs de données de BlueDot sont Pelmorex Corp et Veraset LLC[10].

D^r^ Khan a expliqué que les informations que détient BlueDot sont dans des environnements infonuagiques hautement sécurisés, accompagnés de niveaux de cryptage rigoureux. Il a ajouté que l'entreprise travaille avec des tiers indépendants pour améliorer ses pratiques en matière de sécurité des données.

---

8 ETHI, *Témoignages*, Pamela Snively (vice-présidente et Chef des données et du Bureau des relations de confiance de la Société Telus Communications).

9 Pour plus d'information sur cette norme : Alexandra Savoie, « La protection de la vie privée dès la conception : origine et objectif », Bibliothèque du Parlement, 9 décembre 2021.

10 Noms obtenus suite à l'adoption d'une motion par le Comité le 3 mars 2022.

Alex DeMarsh, directeur, Sciences des données, chez BlueDot, a confirmé que l'entreprise fournit des rapports analytiques à l'ASPC. Des mesures semblables sont accessibles par le biais d'un tableau de bord, que l'ASPC peut utiliser pour consulter directement ce type d'analyses. Seules des mesures sommaires figurent au tableau de bord[11].

M. DeMarsh a expliqué que lorsque BlueDot reçoit les données d'un appareil individuel, elles contiennent seulement une localisation approximative et un horodatage (aucun renseignement permettant d'identifier une personne). Il a clarifié que la référence à un « domicile » dans les rapports de BlueDot signifie la localisation principale d'un appareil. L'analyse vise à faire la distinction entre les appareils qui restent près de leur localisation principale, et ceux qui se déplacent, pour évaluer les taux de contact dans la population.

Même dans un milieu rural, M. DeMarsh a expliqué que la plus petite zone géographique serait définie par la population sous-jacente calculée par Statistiques Canada et donc relativement grande. Il a aussi rappelé que les rapports de BlueDot n'incluent que des sommaires statistiques, le nombre d'appareils et les proportions et pourcentages; ils ne contiennent rien qui puisse vraisemblablement être identifié ou associé à un appareil précis.

## Utilité des données sur la mobilité et efficacité de l'initiative

Le ministre Duclos a souligné que l'utilisation des données sur la mobilité se fait partout dans le monde[12]. Il a dit que des experts et des chercheurs du Center for Disease Control and Prevention des États-Unis et du Centre commun des recherches de la Commission européenne estiment que « la mobilité explique la transmission et la propagation de la maladie, et les données s'y rattachant permettent de réduire la mortalité et d'atténuer la nécessité du confinement ». Il a souligné qu'au Canada, où le taux de mortalité liée à la pandémie a été plus bas que tous les autres pays du G7 à l'exception du Japon,

11 Le Comité a reçu deux exemplaires de rapports hebdomadaires préparés par BlueDot pour l'Agence de la santé publique du Canada (ASPC) intitulés « Tendances de la mobilité au Canada ». Le premier, daté du 4 octobre 2021, couvre la période du 19 au 25 septembre 2021. Le deuxième, daté du 13 décembre 2021, couvre la période du 28 novembre au 4 décembre 2021. Ces rapports offrent des statistiques sur la mobilité au Canada. Avant de joindre BlueDot, M. DeMarsh a travaillé au centre des opérations d'urgence de l'ASPC, où il élaborait et perfectionnait des systèmes de données utilisées pour les données de santé publique plus traditionnelles. Il a confirmé n'avoir aucunement été impliqué dans les démarches menant au contrat conclu avec BlueDot.

12 ETHI, *Témoignages*, l'Hon. Jean-Yves Duclos (ministre de la Santé). Le ministre a nommé les pays suivants : États-Unis, Royaume-Uni, Australie, Espagne, Allemagne, Argentine, Brésil, Colombie, Équateur, Pays-Bas, Italie, Grèce, Autriche, Bulgarie, Croatie, Danemark, Estonie, Finlande, Portugal, Slovénie, Suède et Norvège.

l'utilisation d'information et de données scientifiques a permis de sauver des dizaines de milliers de vies.

Le ministre Duclos a enchéri que les données sur la mobilité anonymisées et agrégées servent à suivre la trajectoire de la pandémie et déterminer la meilleure façon d'y réagir. Elles permettent aux gouvernements de comprendre comment la population réagit aux directives de santé publique de sorte à pouvoir adapter les méthodes et les communications.

Dre Tam a dit les données sur la mobilité sont utiles pour lutter contre la pandémie. Elle a indiqué que des données dépersonnalisées et agrégées sur la mobilité représentent un outil important à l'heure actuelle et pour l'avenir. Elles aident à déterminer s'il y a une éclosion à un certain endroit. Elles permettent de savoir comment évoluent les tendances de la mobilité entre différentes régions et d'examiner le potentiel de propagation d'une maladie. Elles peuvent aussi aider les administrations à examiner l'efficacité de leurs mesures de santé publique.

Dre Tam a souligné qu'en général, la santé publique manque de renseignements. Selon elle, la santé publique dispose de moyens insuffisants, surtout en ce qui a trait à l'utilisation de mégadonnées. Dre Tam a répété que la santé publique a besoin de plus de capacité, de plus d'outils et de plus de plateformes, y compris des plateformes de données, pour éclairer ses décisions. Elle a noté que l'application des mégadonnées en santé publique en est à ses balbutiements.

Dre Tam a précisé que vu la nouveauté des données sur la mobilité, les indicateurs de réussite de ce type de données en sont aux premiers stades de configuration. Elle a aussi dit ne pouvoir indiquer une politique précise de l'ASPC qui aurait été élaborée à l'aide des données sur la mobilité, indiquant que ce sont les provinces qui reçoivent ces données et s'en servent pour leurs propres applications.

Khaled El Emam, titulaire de la Chaire de recherche du Canada en intelligence artificielle médicale, a confirmé que de nombreux pays dans le monde utilisent les données sur la mobilité à des fins de surveillance de la santé publique[13].

Dr Khan a dit être convaincu que les analyses et la technologie peuvent aider à rester à l'affût des éclosions auxquelles il faut réagir, tout en protégeant : des vies; des modes de vie et la confidentialité des données. Il a expliqué que les données sur la mobilité,

13 Khaled El Emam a confirmé qu'en raison de son type d'expertise, il a eu l'occasion de travailler avec de nombreux ministères et différentes parties du gouvernement fédéral au cours des 20 dernières années, incluant Santé Canada et l'Agence de la santé publique du Canada.

contrairement aux données traditionnelles de santé publique comme le nombre de cas ou d'hospitalisations, permettent de passer d'une attitude réactive à une attitude proactive et préventive. L'objectif est d'estimer les taux de contact de la population; un indicateur clé de ce qui s'en vient. Le but est de tenter d'empêcher une éclosion, plutôt que de devoir y réagir.

Selon Dr Khan il y a eu de nombreux cas dans les deux dernières années où les analyses que BlueDot a fournies à l'ASPC ont été « des précurseurs de flambées subséquentes ou ont fourni des renseignements exploitables vraiment importants ». Selon lui, ne pas disposer de ces données, c'est comme lutter contre une pandémie les yeux bandés.

## Consultation avec le commissaire à la protection de la vie privée

Le ministre Duclos a indiqué que le gouvernement a collaboré avec le commissaire depuis le début de la pandémie. Il a dit :

> Les experts juridiques du gouvernement du Canada, avec la collaboration de divers autres experts et compte tenu des observations et avis du Commissariat à la protection de la vie privée, ont conclu que ces renseignements n'étaient pas des données confidentielles et qu'ils ne relevaient donc pas de la *Loi sur la protection des renseignements personnels*. Malgré cela, des rencontres bimensuelles ont eu lieu avec le commissaire à la protection de la vie privée depuis avril 2020 et se poursuivent encore aujourd'hui[14].

Le ministre Duclos a dit que le commissaire a été informé de l'initiative relative aux données sur la mobilité et qu'ils en avaient parlé dès le début de la pandémie, en avril 2020. Il a indiqué que le commissaire et le commissariat jouent un rôle extraordinairement important et que leurs conseils, leurs commentaires et leurs instructions sont indispensables au gouvernement. Il a répété que l'ASPC a communiqué avec le commissariat dès le début de la pandémie, à partir du mois d'avril 2020, et toutes les deux semaines par la suite. Il a ajouté : « Nous continuerons de travailler avec le Commissariat à la protection de la vie privée pendant que nous traversons la crise. »

M. Therrien a dit :

> 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.

14 ETHI, *Témoignages*, L'Hon. Jean-Yves Duclos (ministre de la Santé).

M. Therrien a spécifié :

> 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.

M. Therrien a précisé que le 21 avril 2020, le CRC a informé le commissariat de son intention d'accéder aux données dépersonnalisées de Telus afin de répondre aux questions de l'ASPC sur les tendances en matière de mobilité. Le commissariat a écrit au CRC pour lui expliquer qu'avant de déterminer si des garanties adéquates avaient été adoptées et si son *Cadre pour l'évaluation par le gouvernement du Canada des initiatives en réponse à la COVID-19 ayant une incidence importante sur la vie privée* (cadre d'évaluation du commissariat) avait été respecté, il devait procéder à un engagement formel mené par la Direction des services-conseils du commissariat. Le CRC a choisi de ne pas suivre ce processus[15].

M. Therrien a indiqué que le 22 avril 2020, l'ASPC a communiqué avec le commissariat pour l'informer de son intention d'utiliser les données de localisation mobile en réponse à la COVID-19 et du fait qu'elle estimait que l'activité ne relevait pas de la LPRP[16]. M. Therrien a noté : « [N]otre rôle n'est pas de préautoriser toutes les initiatives gouvernementales, alors nous n'avons pas poussé plus loin. »

Selon l'ASPC, le commissariat a été avisé de ses travaux sur les données relatives à la mobilité en avril 2020. Il n'a ni exprimé une inquiétude ni demandé de renseignements supplémentaires. L'ASPC a continué de rencontrer le commissariat toutes les deux semaines pour lui fournir diverses mises à jour, y compris sur l'initiative susmentionnée. L'ASPC note que mis à part des préoccupations à l'égard des plans de publication des

15 Commissariat à la protection de la vie privée du Canada (CPVP), *Lettre au Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique au sujet de l'étude sur la collecte et l'utilisation de données sur la mobilité par le gouvernement du Canada*, 14 mars 2022 (Lettre du commissariat du 14 mars 2022). Le cadre d'évaluation du commissariat a été publié en avril 2020.

16 *Ibid.*

données de Statistiques Canada soulevée lors d'une rencontre, le commissariat n'a posé aucune autre question sur l'initiative avant décembre 2021[17].

M. Therrien a expliqué que lorsque le commissariat participe activement à une initiative, il reçoit des renseignements qui lui permettent de dire que les renseignements personnels sont protégés en principe, mais aussi qu'il a également vérifié « sous le capot » pour s'assurer que les renseignements personnels sont bel et bien protégés. M. Therrien a rajouté :

> 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.

M. Therrien a confirmé que ce dont le commissariat a été informé dans le cas de l'ASPC était en principe conforme au cadre d'évaluation du commissariat, mais qu'il a 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[18] ».

M. Therrien a toutefois fait remarquer qu'il n'est pas le seul expert en matière de protection de la vie privée; le gouvernement et les entreprises de télécommunications ont aussi des experts.

M. Therrien a indiqué que le commissariat a reçu des plaintes à l'égard de l'utilisation des données sur la mobilité par l'ASPC. Il a expliqué :

---

17 Agence de la santé publique du Canada, réponse écrite préparée par l'Agence de santé publique du Canada distribuée au comité le 25 février 2022.

18 ETHI, *Témoignages*, Daniel Therrien (commissaire).

> 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.

M. Therrien a dit qu'il ne pouvait confirmer que le gouvernement avait bien reçu des données anonymisées ou dépersonnalisées :

> 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.

### Observations et recommandations du Comité

Le Comité prend note des commentaires du commissaire quant à son rôle, mais demeure d'avis que lorsque le gouvernement s'engage dans un programme de collecte de données il devrait consulter le commissariat de façon substantive. Il recommande donc :

**Recommandation 2**

**Que le gouvernement du Canada consulte de façon complète et significative le commissaire à la protection de la vie privée du Canada avant de s'engager dans un programme de collecte de données et qu'il continue de le faire de façon continue pendant toute la durée du programme.**

## Transparence et confiance

### Transparence du gouvernement

Selon le ministre Duclos, le processus entourant l'accès par l'ASPC à des données sur la mobilité pendant la pandémie était tout à fait transparent puisqu'il a été annoncé par le premier ministre en mars 2020 et que les données sont présentées publiquement sur le

site Web *TendancesCOVID*[19]. Il a souligné que depuis 2020, 1,7 million de Canadiens ont pu consulter les données qui se trouvent sur ce site Web et que le processus est public[20]. En dépit des efforts du gouvernement, plusieurs des témoins étaient d'avis que le processus n'avait pas été entièrement transparent.

M. Therrien a dit :

> 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.

M. Therrien a noté que « le consentement n'est pas une panacée ni une solution universelle ». Selon lui, « la plupart des Canadiens dont les données ont été utilisées ne savaient pas que leurs données étaient utilisées ». Il était donc d'avis que « [l]es 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^me^ Cavoukian s'est dite prête à confirmer que le gouvernement ne surveillait pas les Canadiens. Elle a aussi vanté les mérites du programme *Les données au service du bien commun* de Telus, soulignant que la plateforme Insights ne lui pose aucun problème. Elle a indiqué que ses préoccupations sont liées au manque de transparence du gouvernement.

Selon Ann Cavoukian, l'ASPC a fait preuve d'un manque total de transparence. Elle a indiqué que si elle n'avait pas été consultée au sujet d'une telle initiative lorsqu'elle était commissaire à l'information et à la protection de la vie privée de l'Ontario, elle aurait été extrêmement préoccupée. Elle a expliqué :

---

19 Le 23 mars 2020, le premier ministre du Canada a publié un communiqué sur le plan de mobilisation des sciences pour lutter contre la COVID-19 dans lequel on indique qu'il a annoncé: « Un soutien à BlueDot… Le gouvernement du Canada, grâce à l'Agence de la santé publique du Canada, utilisera sa plateforme d'analyse des maladies pour soutenir la modélisation et la surveillance de la propagation de la COVID-19. De plus, cela permettra d'éclairer la prise de décisions gouvernementales au fur et à mesure que la situation évolue. » Le communiqué ne mentionne pas Telus.

20 Selon Christopher Parsons, associé de recherche principal au Citizen Lab du Munk School of Global Affairs and Public Policy de l'Université de Toronto, le site *TendancesCOVID* n'a commencé à publier de l'information publique quant à la source des données sur la mobilité qu'en décembre 2020.

> Je tiens à reconnaître sans conteste qu'ils se sont donné beaucoup de mal pour dépersonnaliser les données et les utiliser sous forme agrégée. Cela réduit beaucoup le risque de repersonnalisation. Je ne voudrais pas laisser entendre le contraire. Je dis simplement que les données relatives à la mobilité — les données de votre cellulaire, qui vous accompagne partout — sont tellement sensibles, elles renseignent sur tous les endroits où vous vous rendez et les personnes que vous fréquentez. Si ces données pouvaient être repersonnalisées et que des liens étaient établis par le gouvernement, je pense que ce serait extrêmement troublant.
>
> Donc le gouvernement aurait au moins dû informer le public en lui disant: « Voici ce que nous faisons. Voici pourquoi nous le faisons. Nous voulons suivre vos déplacements en ces temps de pandémie de COVID. » Est-ce une raison suffisante? Les gens auraient-ils estimé que l'avantage était assez grand? Il faudra en débattre. L'ASPC ne peut pas simplement décider de le faire, […] sans le dire à personne. C'est ce à quoi je m'objectais le plus — le manque total de transparence.

M^me^ Cavoukian a suggéré qu'alerter le commissaire, lui demander des conseils et son assistance pour faire en sorte que la population soit bien au fait de ce qui arrive, aurait permis au commissaire de confirmer que les données ont été bien dépersonnalisées et agrégées ou même de donner son approbation.

David Murakami Wood, directeur du Surveillance Studies Centre et professeur agrégé au département de sociologie de l'Université Queen's, a souligné qu'à aucun moment il n'y a eu soupçon de suivi ou de surveillance individuelle des Canadiens, et que rien n'indique que ces données sur la mobilité aient été désanonymisées ou désagrégées[21]. Cependant, il a souligné que le problème dans le cas concernant l'ASPC est « un manque de communication cohérente et de transparence de la part de tous les paliers de gouvernement concernés ».

Jean-Pierre Charbonneau, ex-parlementaire du Québec et conférencier sur l'éthique, a suggéré que si le gouvernement avait été transparent, le Comité n'aurait probablement fait son étude relative à l'utilisation des données sur la mobilité. Il était d'avis que le gouvernement aurait dû utiliser le mécanisme en place, le commissaire à la protection de la vie privée, pour vérifier que les processus étaient adéquats. Il a suggéré que la réticence du gouvernement à impliquer le commissariat pouvait peut-être s'expliquer par le fait que ce soit un peu compliqué ou parce qu'il avait peur des avis qui pourraient être données. Il a dit : « Si on n'a pas peur, qu'on agisse de façon transparente. »

21 Dr. Harpreet S. Kochhar, président de l'Agence de santé publique du Canada (ASPC), a indiqué dans une lettre au Comité datée du 14 février 2022 que: « L'ASPC n'a donc pas la capacité de faire l'ingénierie inverse sur ces données et n'a aucun intérêt à le faire, car la valeur des données réside dans la mobilité de la population. »

Michael Geist, professeur de droit à l'Université d'Ottawa et titulaire de la chaire de recherche du Canada en droit d'Internet et du commerce électronique, a noté que le commissaire aurait dû participer plus activement au processus. Il a aussi dit que la notification publique aurait pu être plus visible, offrant l'appli AlerteCOVID comme exemple d'une initiative qui a été mieux communiquée et expliquée aux Canadiens. Selon lui, pour que les citoyens fassent confiance aux programmes, il faut expliquer dans autant de forums que possible et aussi clairement que possible quelles données sont recueillies et ce qui est utilisé. À son avis, ce processus n'a pas été respecté par l'ASPC.

Martin French, professeur agrégé au département de sociologie et d'anthropologie à l'Université Concordia, a suggéré que l'ASPC et les gouvernements font du bon travail, mais qu'ils pourraient en faire plus en matière de communication, donnant lui aussi comme exemple l'appli AlerteCOVID dont la politique de protection des renseignements personnels, affichée en ligne, est beaucoup plus lisible que la majorité des politiques.

Daniel Weinstock, professeur de philosophie à l'Université McGill, a suggéré que si le gouvernement s'était livré au même genre d'exercice de justification auquel il se livre lorsqu'il impose des restrictions, il est fort possible que le problème de confiance et de méfiance n'aurait pas existé.

M. Weinstock a dit ne pas faire « l'hypothèse que l'utilisation qui est faite des données à l'heure actuelle par le gouvernement est mauvaise et condamnable », mais se demander « quelles sont les conditions qui peuvent inspirer confiance à la population ». Selon lui, un représentant élu devrait informer le public, car « les décisions en lien avec des questions aussi cruciales et sensibles que celle de l'utilisation des données sont confiées aux politiciens élus ». Il a aussi noté que l'exclusion du commissariat engendre le soupçon, alors qu'il pourrait n'y avoir rien à cacher et dit : « Il est de plus en plus paradoxal que le gouvernement choisisse d'exclure une institution qui aide à augmenter la confiance en lui. »

M. Murakami Wood a convenu qu'il était nécessaire que l'ASPC utilise les données sur la mobilité pour la santé publique, mais il a affirmé que les mesures de protection en place à l'égard de ces données n'ont pas été rendues publiques ni accessibles de manière adéquate. David Lyon, professeur émérite de l'Université Queen's était d'accord avec ces propos.

Christopher Parsons, associé de recherche principal du Citizen Lab de la Munk School of Global Affairs and Public Policy de l'Université de Toronto, a affirmé qu'en début de la pandémie le partage de renseignements a été chaotique pour tous les paliers de gouvernement. Par exemple, il a noté que l'annonce officielle du premier ministre du

23 mars 2020, dans laquelle on indiquait que le gouvernement s'associait à BlueDot, ne faisait pas explicitement référence aux données sur la mobilité[22].

M. Parsons a indiqué à l'égard de ses commentaires portant sur la nature chaotique de l'information en début de pandémie :

> Je ne soulève pas ces points pour suggérer que le gouvernement a pour ainsi dire trompé les Canadiens, mais pour dire que le contexte de l'information était chaotique et n'a pas encore été corrigé de façon adéquate. Pour amorcer cette correction, je suggère au Comité de recommander que le site Web *TendancesCOVID* soit mis à jour, afin d'indiquer clairement les sources particulières de données sur la mobilité que le gouvernement utilise, et d'inclure une option de retrait du programme « data for good » de Telus et de permettre aux personnes de ne pas participer à la collecte de renseignements effectuée par BlueDot. En outre, le Comité devrait recommander à Telus d'intégrer le mécanisme de non-participation à tous ses portails clients, tant pour Telus que pour Koodo, et ce de manière bien visible, afin que les personnes sachent qu'elles ont cette option.

M. Geist a fait la même suggestion. En ce qui concerne le droit de se retirer d'un programme de collecte de données durant une situation temporaire comme une pandémie ou une situation d'urgence, il a dit :

> Je crois que cela dépend quelque peu du type de données. La question est intéressante à poser: peut-on ne pas participer à la collecte? Eh bien, on peut sans contredit se retirer, ou on devrait avoir le droit de se retirer d'un tel programme, je dirais […].
>
> Nous tenons à obtenir plus de données. L'option de se retirer dans ces circonstances me semblerait appropriée. Par contre, il y a peut-être des scénarios où les besoins de la santé publique nécessitent certains types de divulgation.

Alain Deneault, professeur de philosophie à l'Université de Moncton, a lamenté l'opacité des activités du gouvernement en ce qui concerne l'utilisation des données sur la mobilité, notant qu'en raison de ce manque de transparence, il est difficile de savoir si les données ont été utilisées d'une manière juste ou si elles servent à d'autres fins que celles auxquelles elles sont destinées.

## Transparence des fournisseurs de données sur la mobilité

En ce qui concerne Telus, M$^{me}$ Snively a souligné que les messages publics à l'égard du programme *Les données au service du bien commun* étaient réfléchis et explicites. Telus a publié cinq grands engagements pour l'utilisation des données dépersonnalisées et la

22 Christopher Parsons, *Mémoire au comité ETHI : Étude sur la collecte et l'utilisation des données sur la mobilité par le gouvernement du Canada*, 18 février 2022, pp. 2-5 (mémoire de Christopher Parsons).

protection de la vie privée sur son site Web, en plus d'une description complète du programme et d'une foire aux questions.

M^me^ Snively a indiqué que Telus avait aussi publié des lettres d'opinion, donné des entrevues avec le *Globe and Mail* et d'autres médias canadiens, publié des communiqués de presse et fait une annonce publique à l'égard d'un prix en matière de protection des renseignements personnels remporté en 2020.

M^me^ Snively a aussi indiqué que Telus a consulté le commissariat concernant sa stratégie de transparence en lui fournissant un aperçu de ses cinq engagements et en intégrant les commentaires du commissariat dans sa démarche[23].

M. Therrien a confirmé que Telus a avisé le commissariat, le 8 avril 2020, de son intention de communiquer des données dépersonnalisées et agrégées aux gouvernements, aux autorités sanitaires et à des chercheurs universitaires en vue d'appuyer les travaux de gestion de la crise liée à la COVID-19[24]. Le commissariat a revu la déclaration publique que Telus entendait publier et a offert ses commentaires. Il lui a dit qu'il pourrait être utile de consulter sa Direction des services-conseils à l'entreprise si elle avait des propositions concrètes avec des gouvernements, chercheurs ou tiers. Il a aussi soulevé un intérêt à recevoir une séance d'information technique sur la méthode d'agrégation et de dépersonnalisation de Telus. Aucune consultation ni session d'information n'a eu lieu[25].

## Augmenter la confiance du public envers les institutions gouvernementales

Selon M. Weinstock, ce qui permet d'accroître la confiance du public à l'égard du processus, c'est l'existence de limites très claires et auto-imposées par le gouvernement. Par exemple, il a reconnu que les données qui selon les Canadiens devraient être privées peuvent trouver des utilisations importantes dans diverses circonstances. La publicité sur la destination des données, les limites comme la durée de leur utilisation, l'indicateur qui permettra de déclarer la fin de la situation d'urgence qui justifie l'utilisation extraordinaire des données, pourraient contribuer à dissiper l'incertitude qui règne chez certains.

23 ETHI, *Témoignages*, Pamela Snively (Telus).

24 Lettre du commissariat du 14 mars 2022.

25 *Ibid.*

La polarisation peut aussi avoir un impact sur la confiance du public. M. Weinstock a suggéré que cet enjeu se joue à plusieurs et que les médias y sont pour quelque chose, puisqu'ils « cherchent souvent la petite bête dans le but d'augmenter la polarisation ou d'attirer l'attention ». À son avis, les représentants élus doivent prendre des mesures pour réduire la polarisation; jeter de l'huile sur le feu ne fait que créer des scandales ou il n'y en a pas. Par exemple, dans le cas de l'ASPC, M. Weinstock a souligné que l'utilisation des données est fort probablement parfaitement anodine, mais « en cachant des choses et en mettant de côté le commissaire à la protection de la vie privée, on crée des apparences qui n'ont pas lieu d'être et qui ont tendance à nourrir la polarisation plutôt qu'à la réduire ».

M. Murakami Wood a fait des commentaires similaires à ceux de M. Weinstock, notant que le cas de l'ASPC risque d'éroder la confiance du public en raison des actions du gouvernement, qui amène les gens à penser que des actes répréhensibles auraient pu être commis, mais aussi en suscitant la méfiance de façon indirecte. Il a noté que les politiciens se permettent parfois de grandes déclarations et toute sorte d'exagérations à des fins purement politiques. Il donne comme exemple les reportages publiés selon lesquels 33 millions de Canadiens font l'objet d'une surveillance, qui font en sorte que les gens commencent alors à croire que leurs conversations personnelles sont sous écoute, alors que ce n'est pas le cas.

M. Murakami Wood a ajouté que la partisanerie et la santé publique se livrent malheureusement un combat épique ce qui à son avis n'est pas bénéfique. Selon lui, la partisanerie influe sur certaines perceptions à l'égard du cas concernant l'ASPC. Selon M. Weinstock, dans des situations d'urgence prolongée, « la population s'attend à ce que les politiciens s'élèvent au-dessus de la mêlée partisane ».

M. Charbonneau a dit que sur le plan de l'éthique, le gouvernement a agi en catimini. Comme indiqué ci-dessus, selon lui, le gouvernement a empêché le commissariat de jouer son rôle de surveillance en le mettant à l'écart.

M. Charbonneau a dit :

> Je souligne encore une fois que le Commissariat à la protection de la vie privée existe. Ultimement, le but de cette institution est d'aider les dirigeants politiques et les citoyens à y voir clair et, éventuellement, à trouver des compromis ou à évaluer les risques pour les citoyens. Il est impossible que chaque citoyen d'une population comme celle du Canada donne son avis. Il faut faire en sorte qu'une entité représente les citoyens, soit chargée de la surveillance, de la protection de la vie privée...

M. Charbonneau a noté que pour qu'on fasse confiance à un dirigeant politique, il faut que son comportement soit digne de confiance. Il s'est donc demander comment on

peut faire confiance au gouvernement lorsqu'il met de côté la principale institution qu'a créée le Parlement pour faire en sorte de protéger la vie privée des Canadiens. Il a noté : « Ce n'est pas a posteriori qu'on doit justifier la façon dont on se comporte. Dès le départ, on doit être transparent. »

M. Charbonneau était aussi d'avis que le gouvernement a tenté de banaliser la question de l'utilisation des données sur la mobilité, ce qui a miné la confiance des citoyens envers les institutions politiques. Selon lui, chaque fois que les citoyens se trouvent devant des affaires qui vont à l'encontre de la façon dont les dirigeants devraient se comporter, la confiance des citoyens diminue ou stagne. Il a ajouté : « [L]a confiance est l'un des piliers d'une véritable démocratie. Il y a un contrat social qui lie les citoyens et les dirigeants politiques, les élus. Cette confiance est fondamentale. Plus elle est minée, plus les gens se sentent autorisés à faire ce qu'ils veulent. »

M. Geist a noté que le respect de la loi ne favorise pas toujours la confiance. M. Therrien a noté que les incidents liés aux renseignements personnels effritent la confiance du public. M$^{me}$ Cavoukian a noté qu'il est essentiel pour le gouvernement de gagner la confiance du public, qui est en train de s'éroder.

M. Weinstock a aussi rappelé au Comité à l'égard de l'information publique relative à l'utilisation des données sur la mobilité que :

> Deux ans de pandémie, c'est très long, et je crois que des choses qui ont été dites il y a deux ans gagnent à être rappelées régulièrement […] [J]e crois que cette question ne pouvait pas tout simplement être évacuée du débat public une fois pour toutes, au début de la pandémie, pour ne jamais y revenir.

## Observations et recommandation du Comité

Le Comité reconnaît que de l'information publique à l'égard des données sur la mobilité se trouve sur le site Web *TendancesCOVID*. Toutefois, le Comité convient que plusieurs des témoins ont indiqué que le gouvernement aurait pu être plus transparent. Le Comité recommande donc:

**Recommandation 3**

**Que le gouvernement du Canada insère dans la *Loi sur la protection des renseignements personnels* des obligations explicites en matière de transparence.**

**Recommandation 4**

**Que le gouvernement du Canada mette immédiatement à jour le site Web *TendancesCOVID* pour indiquer d'où proviennent les données, quel(s) fournisseur(s) de données fournit(ssent) les informations au gouvernement, et les détails sur les endroits où les Canadiens peuvent se retirer du programme de collecte de données et de surveillance.**

**Recommandation 5**

**Que le gouvernement du Canada prenne des mesures pour informer les Canadiens des programmes de collecte de données sur la mobilité sur une base continue et qu'il le fasse d'une manière qui expose clairement la nature et le but de la collecte de données.**

## Consentement

Aux questions relatives au consentement, M. Allison a mentionné que Telus et BlueDot recueillent des données dans le cadre de leurs activités et qu'elles prévoient des options en matière de consentement. Il a dit :

> [J]e ne peux pas vraiment me prononcer sur la validité du consentement. Telus est transparent au sujet de ce qu'il fait. Le gouvernement du Canada fait preuve de transparence au sujet de ce qu'il fait et de la façon dont il utilise les données sur la mobilité, mais au bout du compte, il incombe aux utilisateurs du service de décider de refuser ou non de donner leur consentement à Telus.

M. Allison a reconnu qu'à moins d'en avoir été informé ou d'avoir visité le site Web de Telus, l'utilisateur moyen d'un appareil mobile n'aurait probablement pas été au courant de son droit de retrait du programme *Les données au service du bien commun*.

M$^{me}$ Snively a confirmé que Telus offre à ses clients la possibilité de se soustraire au programme *Les données au service du bien commun*.

M$^{me}$ Snively a expliqué que les données sur lesquelles le programme *Les données au service du bien commun* repose sont recueillies dans le cadre de la prestation de services de mobilité, de sorte que le consentement s'applique à l'utilisation des services de mobilité et à la prestation de ceux-ci. Une fois que ces données sont dépersonnalisées, elles ne sont plus des renseignements personnels. Au lieu de s'appuyer sur le consentement, Telus prend soin de dépersonnaliser les données. M. El Emam a aussi indiqué qu'anonymiser ou dépersonnaliser les données fait en sorte qu'ils ne sont plus des renseignements personnels.

Au sujet du consentement des clients de Telus à ce que leurs renseignements soient dépersonnalisés, M[me] Snively a noté que beaucoup de renseignements sur la dépersonnalisation se trouvent en ligne dans la politique de confidentialité de l'entreprise. M. Therrien a toutefois remarqué qu'une politique de confidentialité qui mentionne que les données de mobilité pourraient être utilisées pour le bien public n'est pas une bonne façon d'informer les Canadiens de la manière dont leurs données sont utilisées, puisqu'elles sont souvent longues, compliquées et difficiles à comprendre. M. Therrien a néanmoins reconnu que si les renseignements sont correctement dépersonnalisés, le consentement n'est pas nécessaire.

M[me] Snively a noté que contacter tous les clients activement pour les informer du programme *Les données au service du bien commun* n'est pas une décision facile à prendre. Par exemple, Telus avise généralement à ces clients de ne pas répondre à un message qu'il n'attend pas sous risque d'hameçonnage et plusieurs ne veulent pas recevoir des textos.

En ce qui concerne BlueDot, D[r] Khan a dit que les utilisateurs des applications qui fournissent des données à son entreprise donnent leur consentement exprès pour permettre à cette application d'accéder à leurs données de localisation et peuvent retirer leur consentement en tout temps[26]. M. DeMarsh a ajouté :

> Dans le contexte qui nous occupe, puisque les données sont uniquement des renseignements anonymisés sur la localisation, il n'y a pas de niveau de consentement pour l'obtention de renseignements supplémentaires. Nous ne recevons jamais rien d'autre que des données anonymisées ou des mesures sommaires agrégées liées aux déplacements. Dans ce cas, il n'y a aucune notion de niveau de consentement ou de renseignements supplémentaires que nous pourrions obtenir par appareil ou sous forme agrégée.

Selon Christopher Parsons, les activités de Telus et BlueDot « témoignent de la volonté apparente du gouvernement de recevoir des données sur la mobilité sans s'assurer au préalable que les personnes ont consenti de manière valable à leur divulgation ». M. Parsons a suggéré que les utilisateurs de téléphonie cellulaire s'attendent à ce que leurs données sur la mobilité puissent être utilisées pour assurer la qualité du service et opérer leurs réseaux, mais pas nécessairement à ce qu'elles soient partagées avec de tierces parties pour d'autres fins – même si elles font partie d'un ensemble de données agrégées et anonymisées et que c'est techniquement permis dans une politique de confidentialité.

26 ETHI, *Témoignages*, Kamran Khan (BlueDot).

Ann Cavoukian était aussi d'avis qu'il n'y a pas eu de consentement dans le cas de l'utilisation des données sur la mobilité en l'espèce. Toutefois, M. Weinstock a fait remarquer que la finalité en l'espèce ne peut être servie que si une vaste proportion de la population est embrigadée, rendant la question du consentement individuel et explicite difficile.

## Partage des données

M. Allison a dit que l'ASPC a des ententes de partage de données avec des provinces, des territoires et des établissements de recherche. Dans le cas des données sur la mobilité, il a expliqué que les données communiquées par les fournisseurs ne sont pas partagées, mais que les rapports et les résumés de ces rapports sont transmis aux provinces, aux territoires et à d'autres organisations pour les besoins pour lequel ces renseignements ont été recueillis : la lutte contre la COVID-19. D^re^ Tam et M^me^ Thompson ont dit la même chose[27].

Pamela Snively a confirmé que Telus savait que l'ASPC diffuserait plus largement les données obtenues en vertu de son programme *Les données au service du bien commun*. Si la communication s'inscrivait dans l'intérêt du bien commun visé par le programme (limiter la propagation de la COVID-19), la communication était autorisée.

D^r^ Khan a souligné que son travail avec l'ASPC visait à lui permettre d'appuyer les décisions aux niveaux local, national et provincial, mais il n'était pas entièrement au courant de la façon dont l'ASPC aurait pu partager avec d'autres administrations au pays les données auxquelles elle a eu accès par l'entremise de son contrat avec BlueDot.

En ce qui concerne l'utilisation future du gouvernement de données sur la mobilité, M. Geist a indiqué :

> Disons d'abord que les entreprises et les administrations publiques, peut-être, essaient de laisser la porte ouverte à toutes les éventualités pour l'utilisation ultérieure des données. C'est en partie la cause réelle des problèmes qui commencent à surgir. Dans certaines circonstances, ce choix se défend, mais c'est quand on essaie de conserver

27 Le Comité a reçu un exemple d'un rapport du Centre des recherches sur les communications d'Innovation, Sciences et Développement économique Canada intitulé « Tendances de la mobilité hebdomadaire au Canada pour la semaine du 02 au 08 mai 2021 » qui a été transmis aux provinces. Ce rapport donne des statistiques sur la mobilité et le taux de déplacement pendant la semaine donnée à l'aide de graphiques et les cartes de densité. Il indique que les mesures de mobilité sont dérivées de l'emplacement de tours cellulaires plutôt que de l'emplacement géographique d'un appareil. Un mouvement est déduit lorsqu'un appareil mobile passe d'une zone de tour cellulaire à une autre.

> toujours une pleine liberté d'agir qu'on commence vraiment à solliciter outre mesure la confiance du public dont il vient d'être question.
>
> Quand les règles juridiques en vigueur sont efficaces, ça devient simplement impossible, parce que, alors, il faut justifier l'emploi des données en essayant d'en circonscrire certaines, pour mieux les définir et pour que le consentement lui-même ne soit valable que pour des groupes restreints d'utilisations, par opposition, essentiellement, au maintien d'une porte ouverte à d'autres utilisations éventuelles qui serviront au cas où on en aurait besoin.

## Observations et recommandations du Comité

Le Comité estime que les Canadiens devraient avoir l'assurance que le partage de leurs données, mêmes lorsqu'elles sont dépersonnalisées ou agrégées, est limité. Par conséquent, il recommande :

**Recommandation 6**

**Que le gouvernement du Canada veille à ce que l'utilisation de l'information recueillie dans le cadre de programmes de collecte de données sur la mobilité soit limitée au ministère ou à l'agence qui en fait la demande et à tout autre ministère ou agence spécifiquement mentionné dans l'appel d'offres, uniquement si l'inclusion de plusieurs ministères ou agences est justifiée.**

# CHAPITRE 2 : DONNÉES DÉPERSONNALISÉES, ANONYMISÉES OU AGRÉGÉES ET RISQUE DE REPERSONNALISATION

M. Therrien a noté que les ensembles de données dépersonnalisées doivent être protégés contre différents types de risques de repersonnalisation. Il a souligné que le cadre d'évaluation du commissariat met en garde contre le risque de repersonnalisation et le besoin d'adopter des moyens techniques pour protéger les renseignements dépersonnalisés. Il a aussi fait remarquer qu'il faut tenir compte de la nature, de la portée, du contexte et des objectifs du traitement dans chaque cas où des données dépersonnalisées sont publiées[28].

28 Lettre du commissariat du 14 mars 2022. Le commissaire nomme trois types de risque : « [L]'individualisation (c.-à-d. qu'il doit être impossible d'isoler un individu d'un ensemble de données), la corrélation (c.-à-d. qu'il doit être impossible de relier deux ensembles de données concernant le même individu) et l'inférence (c.-à-d. qu'il doit être impossible d'inférer de nouveaux renseignements sur une personne concernée à partir d'un ensemble de données). »

M. Lyon a noté ce qui suit à l'égard du risque de réidentification :

> Je ne suis pas un expert en matière de désindentification des données, mais des études approfondies menées par divers acteurs, dont l'Imperial College de Londres et l'Université de Louvain, montrent que 99,8 % des Américains pourraient être réidentifiés dans un ensemble de données utilisant 15 attributs démographiques. Il existe un potentiel de réidentification, et il faut donc s'assurer que les données sont réellement sécurisées et ne sont utilisées qu'à des fins pertinentes.

Toutefois, M. Lyon a dit que même s'il semble difficile d'arriver à un anonymat parfait en pratique, il est possible de faire preuve de prudence à toutes les étapes, c'est-à-dire durant la collecte, le regroupement des données et l'analyse de celles-ci.

M. El Emam, a indiqué que les termes anonymisation, dépersonnalisation ou agrégation sont souvent utilisés de façon interchangeable, mais ne veulent pas dire la même chose. Il est plus précis de parler de risque de repersonnalisation, l'objectif étant d'assurer que ce risque soit très faible.

M. El Emam a affirmé que l'acceptation d'un risque de repersonnalisation très faible n'est pas controversée puisque ceux qui transforment les données s'appuient sur des précédents qui ont très bien fonctionné dans le passé. Si la norme de repersonnalisation devait être « zéro », cela voudrait dire que toutes les données seraient considérées comme des renseignements personnels. À son avis, 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.

M. El Emam a expliqué que de nombreux types de transformation permettent de réduire le risque de repersonnalisation et qu'une panoplie de technologies permettent de renforcer la protection des renseignements personnels en vue d'un partage responsable des données individuelles. Par exemple, les dates peuvent être généralisées (en utilisant des intervalles plus grands), la granularité des lieux géographiques peut être réduite (en utilisant des zones géographiques plus grandes), du bruit peut être ajouté aux valeurs données ou des données synthétiques peuvent être créées (données factices qui conservent les modèles et les propriétés statistiques des données réelles sans correspondance directe avec les données originales). Il est aussi possible de crypter les données et d'effectuer des analyses sur ces données-là ou encore de partager des statistiques sommaires plutôt que des données individuelles.

Dr Khan a toutefois fait remarquer à l'égard des données synthétiques qu'elles conviennent dans un environnement très stable, ce qui n'est pas le cas pendant une pandémie, alors que les conditions changent constamment.

M. El Emam a rajouté que le risque de repersonnalisation est géré grâce à une combinaison de transformations de données et de mesures de contrôles additionnelles. Il a convenu que le risque de repersonnalisation n'est pas nul. Le risque résiduel est géré en mettant en place des contrôles de sécurité, des contrôles de confidentialité et des contrôles contractuels. Il a nommé des pratiques exemplaires pour une réutilisation et un partage responsable des données : la transparence (informer les personnes des fins auxquelles les données sont utilisées et donner une option de refus); la surveillance de l'éthique (procéder à un examen indépendant des finalités du traitement des données) et les attaques de repersonnalisation sur les données pour tester ce risque de façon empirique.

M. El Emam a insisté que si les données sont dépersonnalisées à l'aide de bonnes pratiques, les risques de repersonnalisation peuvent être très faibles.

## CHAPITRE 3 : UTILISATION DES DONNÉES POUR DES FINS COMMERCIALES LÉGITIMES ET DES FINS SOCIALEMENT BÉNÉFIQUES ET RÔLE DU CONSENTEMENT

M. Therrien a dit que dès le début de la pandémie, le commissariat a reconnu que les données peuvent servir dans l'intérêt public, par exemple pour protéger la santé publique. Comme indiqué plus haut, selon lui, « 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 ».

Sur le rôle du consentement, M. Therrien a reconnu que les organisations des secteurs public et privé réutilisent constamment des données à de nouvelles fins, ce qui suscite des préoccupations légitimes chez les consommateurs, surtout lorsque leurs données personnelles sont utilisées à leur insu et à des fins autres que celles auxquelles ils s'attendaient. Toutefois, il note que ça ne signifie pas que ces pratiques ne devraient être autorisées qu'avec le consentement des consommateurs. À son avis, comme le cas de l'ASPC l'a illustré, ce ne serait ni réaliste ni raisonnable.

Selon M. Therrien :

> Dans l'ère numérique actuelle, la protection des renseignements personnels ne peut pas reposer uniquement sur le consentement...le consentement peut servir à légitimer des usages qui, objectivement, sont complètement déraisonnables et contraires à nos

> droits et valeurs. Et le refus de donner son consentement peut parfois desservir l'intérêt public[29].

M. Therrien a dit :

> [J]e 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.

M. El Emam a abondé dans le même sens. Selon lui, il peut être peu pratique d'obtenir un consentement à priori dans des cas comme celui de l'ASPC. 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[30].

Teresa Scassa, titulaire de la Chaire de recherche en droit et politiques de l'information et professeur de droit à l'Université d'Ottawa, a indiqué qu'il faut faciliter l'utilisation de données à des fins bénéfiques pour la société, mais qu'on peut quand même s'interroger sur la validité du consentement obtenu, la conformité des pratiques de collections et le type de données recueillies. Selon M^me^ Scassa, les enjeux liés à la protection de la vie privée sont cruciaux, mais la possibilité pour les gouvernements de compter sur les meilleures données possibles pour prendre des décisions stratégiques importantes est également primordiale et il est souvent impossible pour le gouvernement de recueillir ces données lui-même.

Comme M. Therrien, M^me^ Scassa a reconnu qu'il y a tellement de données qui sont recueillies qu'il devient impossible d'obtenir le consentement de chacun pour toutes les utilisations que l'on veut en faire. C'est pourquoi des mécanismes ont été mis en place pour compenser l'impossibilité d'obtenir le consentement dans certaines circonstances. Le problème, selon M^me^ Scassa, c'est que les entreprises et les gouvernements essaient de déterminer du mieux qu'ils peuvent comment utiliser les données à des fins socialement bénéfiques d'une manière appropriée, alors qu'il n'existe pas de cadre adapté à ce type d'activité.

M^me^ Scassa a noté que l'ancien projet de loi C-11, Loi édictant la Loi sur la protection de la vie privée des consommateurs et la Loi sur le Tribunal de la protection des

29 *Ibid*.

30 ETHI, *Témoignages*, Khaled El Emam.

renseignements personnels et des données et apportant des modifications corrélatives et connexes à d'autres lois (projet de loi C-11 (43-2)), contenait « justement une définition de renseignement personnel dépersonnalisé ». Ce projet de loi visait à modifier la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE). La Loi sur la protection de la vie privée des consommateurs (LPVPC) prévoyait des exemptions permettant aux organisations de dépersonnaliser les renseignements personnels en leur possession et de les utiliser ou les divulguer dans certaines circonstances, à l'insu et sans le consentement des individus[31].

M^me^ Scassa a expliqué que l'article 39 de la LPVPC aurait permis de communiquer des renseignements personnels dépersonnalisés à des acteurs gouvernementaux, à des fins socialement bénéfiques, à l'insu et sans le consentement des personnes dont les renseignements ont été dépersonnalisés. Selon elle, une telle disposition se serait appliquée au cas concernant l'ASPC.

M^me^ Scassa s'est toutefois dite préoccupée par le libellé de l'article 39 de la LPVPC. Selon elle, certaines questions doivent se poser au sujet de la portée d'une telle disposition, par exemple au sujet de la définition de « fins socialement bénéfiques »; du degré de transparence qui devrait être exigé de la part des organisations qui communiquent des renseignements dépersonnalisés; de l'imposition potentielle de nouvelles obligations pour le secteur public que pourrait accompagner la communication d'informations par les organisations du secteur privé au gouvernement à des fins socialement bénéfiques; et de la possibilité d'un examen ou une approbation préalable des plans d'acquisition ou d'utilisation des données.

## Observations et recommandations du Comité

Le Comité est d'avis que si les entreprises peuvent utiliser des renseignements pour des fins commerciales légitimes ou des fins socialement bénéfiques, sans leur consentement, les Canadiens devraient être en mesure de savoir exactement en quoi consistent ces fins. Il recommande donc:

31 Voir par exemple les articles 20, 21, 22,39, 74 et 75 de la Loi sur la protection de la vie privée des consommateurs dans le projet de loi C-11 (43-2). À noter que le projet de loi contient une définition du terme « dépersonnaliser » à l'article 2. Certains articles de la loi font par la suite référence aux renseignements dépersonnalisés. Pour plus d'information sur le projet de loi C-1 (43-2), consulter le *Résumé législatif du projet de loi C-11 : Loi édictant la Loi sur la protection de la vie privée des consommateurs et la Loi sur le Tribunal de la protection des renseignements personnels et des données et apportant des modifications corrélatives et connexes à d'autres lois* préparé par la Bibliothèque du Parlement.

**Recommandation 7**

**Que le gouvernement du Canada modifie la *Loi sur la protection des renseignements personnels* et la *Loi sur la protection des renseignements personnels et les documents électroniques* afin de définir ce qui constitue un « intérêt commercial légitime » et un « bien public » dans la collecte, le stockage, l'utilisation, le transfert et la vente de données privées, telles les données sur la mobilité, et que le Commissariat à la protection de la vie privée du Canada soit habilité à enquêter sur les violations des lignes directrices éthiques définissant ces critères.**

# CHAPITRE 4 : UNE LÉGISLATION ADAPTÉE À L'ÈRE NUMÉRIQUE

M. Geist a noté que la façon par laquelle les données ont été agrégées et dépersonnalisées dans le cas impliquant l'ASPC est une approche typique de la manière dont les organisations s'acquittent de leurs obligations en matière de protection de la vie privée en les dépersonnalisant et les plaçant à l'extérieur du champ d'application de la loi. L'utilisation de ces données en pleine pandémie peut très bien être bénéfique. Il ne semble pas y avoir de violation de la loi, puisque les données étaient agrégées et dépersonnalisées. Selon lui, le problème fondamental que le cas concernant l'ASPC met en lumière : l'inadaptation de nos lois à leurs fins et le besoin de les réformer. Le Comité est d'accord avec M. Geist : les lois doivent être modernisées.

## Besoin de réforme

La LPRP a été adoptée en 1983 et n'a fait l'objet d'aucune réforme substantielle depuis. La LPRPDE a été adoptée en 2000. Elle n'a également fait l'objet d'aucune réforme substantielle depuis.

En 2016, le Comité a fait un examen de la LPRP[32]. En 2018, le Comité a fait un examen de la LPRPDE[33]. Il a aussi publié d'autres rapports qui contiennent de nombreuses recommandations visant à améliorer la LPRPDE[34].

32 ETHI, *Protéger la vie privée des Canadiens : Examen de la Loi sur la protection des renseignements personnels*, décembre 2016.

33 ETHI, *Vers la protection de la vie privée dès la conception : Examen de la Loi sur la protection des renseignements personnels et les documents électroniques*, février 2018.

34 ETHI, *Aborder les vulnérabilités de la vie privée numérique et les menaces potentielles au processus électoral démocratique canadien*, juin 2018; ETHI, *Démocratie menacée : Risques et solutions à l'ère de la désinformation et du monopole des données*, décembre 2018; ETHI, *Protection des renseignements personnels et services gouvernementaux numériques*, juin 2019.

En novembre 2020, le gouvernement a déposé l'ancien projet de loi C-11 (43-2), qui visait à modifier la LPRPDE. Il est mort au *Feuilleton*. En 2021, le gouvernement du Canada a publié un document de discussion dans le cadre d'une consultation publique concernant la modernisation de la LPRP[35]. Aucun projet de loi n'a été déposé pour modifier la LPRP à ce jour.

## Application des lois aux données dépersonnalisées

M. Therrien a expliqué ce qui suit à l'égard du consentement implicite et des données dépersonnalisées :

> 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

M. Therrien a noté qu'il faut se demander « si c'est une bonne politique législative que de ne pas appliquer les lois sur la protection des renseignements personnels aux données dépersonnalisées » considérant 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 ». Il a réitéré :

> 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*.

M^me^ Scassa a affirmé que la LPRP et la LPRPDE ont besoin d'être modernisées afin de prescrire des règles et des principes appropriés pour régir l'utilisation des données dans un environnement numérique transformé et en pleine mutation. Selon elle, le fait que les deux lois ne s'appliquent qu'aux données concernant des personnes identifiables,

35 Ministère de la Justice, *Respect, responsabilité, adaptabilité : Consultation publique concernant la modernisation de la Loi sur la protection des renseignements personnels* (document de consultation du ministère de la Justice à l'égard de la LPRP).

crée une zone grise pour les données dépersonnalisées. À son avis, le commissaire devrait être en mesure de surveiller l'utilisation de telles données, ou à tout le moins veiller à ce qu'il n'y ait pas de repersonnalisation[36].

M. El Emam a noté l'absence de directives réglementaires ou de codes de pratique clairs et pancanadiens pour la création de renseignements non identifiables. Selon lui, de tels codes et une plus grande clarté dans la loi réduiraient l'incertitude, fourniraient une orientation claire sur ce que sont les approches raisonnables et acceptables, et permettraient aux organisations d'être évaluées pour qu'elles démontrent leur conformité. Selon lui, les codes de pratique, des normes en matière de dépersonnalisation et des lignes directrices applicables aideraient à assurer l'adoption des bonnes pratiques à chaque fois[37].

M^me^ Scassa a indiqué si la loi s'applique aux données dépersonnalisées, alors elle devrait prévoir l'établissement ou l'examen des normes de dépersonnalisation qui devraient s'appliquer. M^me^ Cavoukian était également d'accord que les lois fédérales en matière de protection des renseignements personnels devraient s'appliquer aux données dépersonnalisées.

M. Therrien a dit appuyer les propositions mises de l'avant par le gouvernement dans le projet de loi C -11 (43-2) et dans le document de consultation du ministère de la Justice portant sur la modernisation de la LPRP. Ils proposent « d'inclure dans la loi une définition de la dépersonnalisation, d'assouplir la loi pour permettre l'utilisation et une divulgation dans certaines circonstances, et d'introduire une infraction pour la repersonnalisation de renseignements dépersonnalisés[38] ».

M. Therrien a noté que le Québec a mis à jour ses lois sur la protection de la vie privée en y incluant les termes « dépersonnalisé » et « anonymisé » et en prévoyant des sanctions si l'on procède ou tente de procéder à l'identification d'une personne physique

---

36 David Young a fait parvenir au Comité un bulletin de conformité qu'il a écrit en mai 2021. Le bulletin suggère que le projet de loi C-11 (43-2) bénéficierait de l'ajout d'un modèle complet pour les renseignements qui ne sont pas considérés personnels. Il suggère notamment l'ajout de disposition créant des catégories limitées de renseignements non personnels qui serait également sujet à la loi étant donné leur nature personnelle originale : tels les renseignements dépersonnalisés.

37 Le projet de loi C-11 (43-2) prévoyait la possibilité de créer des codes de pratiques, approuvés par le commissaire à la protection de la vie privée (articles 76 à 81 de la Loi sur la protection de la vie privée des consommateurs). M. El Emam offert comme exemple le travail mené par le *Canadian Anonymization Network* (dont Telus est un membre fondateur) et aux normes publiées par le Bureau du Commissaire à l'information et la protection de la vie privée de l'Ontario en 2016 : De-Identification Guidelines for Structured Data [DISPONIBLE EN ANGLAIS SEULEMENT].

38 Lettre du commissariat du 14 mars 2022.

à partir de renseignements dépersonnalisés. La loi québécoise permet d'utiliser des renseignements dépersonnalisés sans obtenir le consentement de la personne concernée lorsque cette utilisation est nécessaire à des fins d'étude, de recherche ou de production de statistiques[39].

M. Therrien a également mentionné que l'Ontario a modifié sa *Loi de 2004 sur la protection des renseignements personnels sur la santé* afin d'interdire de façon générale toute utilisation ou la tentative d'utilisation de renseignements anonymisés, seuls ou avec d'autres renseignements, pour identifier un particulier, avec certaines exceptions[40]. M^me^ Scassa a noté que l'Ontario a modifié sa *Loi sur l'accès à l'information et la protection de la vie privée*, qui s'applique au secteur public, afin de définir les renseignements dépersonnalisés aux fins d'utilisation par le gouvernement, d'exiger l'élaboration de normes à l'égard des données dépersonnalisées et de prévoir des sanctions en cas de repersonnalisation[41].

Au niveau international, M. Therrien a affirmé que le RGPD fait clairement la distinction entre les données « pseudonymisées » et les données « anonymisées »; le règlement continue de s'appliquer aux premières et ne s'applique plus aux secondes. Au Japon, la loi sur la protection des renseignements personnels définit des règles spécifiques pour les renseignements traités de « façon pseudonyme » ou de « manière anonyme ». En Australie, des règles spécifiques concernant les renseignements dépersonnalisés et une définition qui ressemble à celle que l'on retrouve dans la législation québécoise et ontarienne se trouvent dans la *Privacy Act, 1988*. En Corée du Sud, la législation permet une plus grande latitude pour le traitement de renseignements pseudonymes; ils peuvent être traités sans consentement à des fins statistiques, de recherche scientifique et d'archivage dans l'intérêt public. La loi sud-coréenne contient aussi une infraction pour la repersonnalisation[42].

Dans un mémoire soumis au Comité, Bell Canada a indiqué qu'elle n'a pas fourni de données sur la mobilité à l'ASPC, mais que l'utilisation appropriée de données dépersonnalisées peut servir l'intérêt public tout en protégeant la vie privée des Canadiens. Selon Bell, l'analytique des données offre une occasion énorme de tirer une valeur économique et sociale des données et de nombreuses techniques de dépersonnalisation existantes empêchent la repersonnalisation. L'entreprise est d'avis

39 *Ibid.*

40 *Ibid*.

41 Voir aussi les propos du commissaire à la protection de la vie privée à l'égard de la loi ontarienne : Lettre du commissariat du 14 mars 2022.

42 *Ibid.*

que les renseignements dépersonnalisés devraient tomber à l'extérieur du champ d'application des lois en matière de protection des renseignements personnels[43].

## Observations et recommandations du Comité

Le Comité est d'avis que compte tenu du fait que le risque de repersonnalisation n'est jamais nul, les lois fédérales en matière de protection des renseignements personnels devraient s'appliquer aux données dépersonnalisées. Il recommande :

**Recommandation 8**

**Que le gouvernement du Canada modifie les lois fédérales en matière de protection des renseignements personnels afin de rendre ces lois applicables à la collecte, à l'utilisation et à la communication de données dépersonnalisées et agrégées.**

**Recommandation 9**

**Que le gouvernement du Canada inclut dans les lois fédérales en matière de protection des renseignements personnels, une norme de dépersonnalisation des données ou la possibilité pour le commissaire à la protection de la vie privée de certifier un code de pratique à cet égard.**

## Flux de données entre le secteur public et privé

M. Therrien a constaté que les secteurs public et privé interagissent de plus en plus au chapitre de la gestion des données – ce qui n'est pas une mauvaise chose – mais cette relation doit être correctement réglementée selon des critères établis et faire l'objet d'enquête lorsqu'il le faut.

M^me^ Scassa a dit que la situation de l'ASPC illustre la facilité avec laquelle les données passent du secteur privé au secteur public au Canada. Le cadre juridique actuel régit séparément l'utilisation de données personnelles par ces deux secteurs. À son avis, il

43 Bell Canada a refusé une invitation à comparaître devant le Comité. SaskTel a refusé une invitation de comparaître devant le Comité. Dans une lettre au Comité datée du 10 février 2022, SaskTel a indiqué qu'elle n'était pas en mesure de répondre à des questions à l'égard des pratiques de Telus et BlueDot et n'avait pas l'intention de participer au processus d'appel d'offres de l'Agence de la santé publique du Canada (ASPC). Rogers Communications a refusé une invitation de comparaître devant le Comité. Dans une lettre au Comité datée du 4 février 2022, Rogers explique qu'elle n'a fourni aucunes données à l'ASPC, qu'elle ne va pas participer à l'appel d'offres de l'ASPC, et qu'elle ne divulgue pas de renseignements sur ses clients, dépersonnalisés ou non, à moins d'obtenir une ordonnance d'un tribunal ou d'une autre autorité légale qui l'y oblige.

faudrait des lois mieux adaptées pour tenir compte de la circulation des données d'un secteur à l'autre. Selon elle, ces flux de données n'ont pas été assez pris en compte dans la conception de nos lois.

M^me^ Scassa a toutefois tenté de rassurer le Comité en notant que le commissaire a déjà indiqué qu'une institution fédérale ne peut pas utiliser à des fins licites, des données qui ont été recueillies de manière illicite, citant le cas de Clearview AI en exemple[44].

M. Geist a aussi noté qu'il faut réfléchir à l'interaction que le gouvernement fédéral peut avoir avec les participants du secteur privé pour obtenir des données. La loi devrait donc établir des précautions et des mesures de sauvegardes efficaces à cet égard.

## Norme internationale à suivre

Plusieurs témoins ont reconnu que le RGPD est un modèle à suivre en matière de protection des données[45]. M^me^ Snively a par exemple mentionné que le RGPD inclut le principe de la protection de la vie privée dès la conception. En revanche, M^me^ Scassa a mis en garde contre simplement prendre ce qui a été fait en Europe et le reproduire dans le contexte canadien.

M. Geist a dit :

> Nous avons également, comme je l'ai mentionné d'entrée de jeu, le Règlement européen sur la protection des données, qui est le modèle que de nombreux intervenants approuvent et s'efforcent déjà de respecter. Il vise à régler certains de ces problèmes au niveau de la transparence algorithmique en imposant des sanctions plus sévères et en relevant quelques-uns des problèmes plus nouveaux tels que le droit à l'oubli et d'autres, ce qui fait partie de ce qui est largement considéré, à mon avis, comme étant une loi sur la protection des renseignements personnels modernisée, ce que le Canada n'a plus.

Cependant, M. Geist a reconnu que les règles pourraient être adaptées à la situation canadienne.

---

44 Commissariat à la protection de la vie privée du Canada, *Rapport spécial au Parlement sur l'enquête réalisée par le Commissariat à la protection de la vie privée du Canada sur l'utilisation par la GRC de la technologie de Clearview AI et version préliminaire d'un document d'orientation conjoint à l'intention des services de police qui envisagent d'avoir recours à la technologie de reconnaissance faciale*, 10 juin 2021.

45 Voir par exemple : ETHI, *Témoignages*, 7 février 2022, Khaled El Emam; ETHI, *Témoignages*, 10 février 2022, Ann Cavoukian et Theresa Scassa; ETHI, *Témoignages*, 14 février 2022, David Murakami Wood; ETHI, *Témoignages*, 28 février 2022, Michael Geist.

# Modernisation des lois

## Modification de la *Loi sur la protection des renseignements personnels*

Comme indiqué précédemment, M. Therrien a suggéré 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 ». Il a toutefois noté que « ce n'est malheureusement pas réaliste de s'attendre à ce que le Commissariat approuve toutes les utilisations ou divulgations de données au pays ».

M. Therrien a précisé que les vérifications proactives ne se veulent pas une épine au pied du gouvernement ou des entreprises qui veulent innover de manière responsable. Néanmoins, considérant la complexité des flux de données et des modèles commerciaux, il est d'avis que le commissariat est mieux placé pour regarder sous le capot à un certain nombre d'endroits où il pense qu'il pourrait y avoir des risques, afin de rassurer les Canadiens que la loi est respectée ou pour intervenir et sanctionner les entreprises qui ne la respectent pas.

M. Therrien a indiqué que le principe de transparence devrait faire partie de la LPRP. Il a souligné que le RGPD contient plusieurs obligations explicites en matière de transparence, tant au moment de la collecte, mais aussi en cas de changement important dans la finalité du traitement. Le RGPD exige que « toute information et communication relatives au traitement de données à caractère personnel soient facilement accessibles, faciles à comprendre, et formulées en termes clairs et simples[46] ».

Christopher Parsons a recommandé plusieurs modifications à la LPRP. D'abord le gouvernement devrait être tenu de confirmer que les organisations desquelles il reçoit des renseignements ont obtenu le consentement valable des personnes auxquelles ces renseignements se rapportent avant les divulguer. Il a suggéré que le champ d'application de la LPRP devrait s'étendre aux renseignements anonymes ou agrégés et que le gouvernement soit tenu de faire des évaluations de l'équité dans les analyses, du point de vue de la vie privée, de la façon dont les organismes gouvernementaux pourraient utiliser les données agrégées ou anonymisées qu'il obtient. Il a aussi recommandé que le gouvernement soit obligé d'obtenir l'approbation du commissaire à

46 Lettre du commissariat du 14 mars 2022.

la protection de la vie privée avant le lancement d'un programme ayant recours à de tels renseignements[47].

M. Parsons a suggéré l'inclusion de critères de nécessité et de proportionnalité, qui obligerait les institutions fédérales à démontrer que des données identifiables ou anonymisées sont nécessaires afin de compléter une activité précise et que la sensibilité des données est proportionnelle à l'activité en question. Selon lui, la LPRP devrait interdire l'utilisation des données pour d'autres fins que celles prévues lorsqu'elles ont été recueillies ou reçues, sans obtenir à nouveau le consentement valable des individus concernés[48]. M. Geist a aussi suggéré d'inclure un critère de nécessité dans la LPRP.

M. Parsons recommande aussi d'inclure une limite de temps à l'égard de la rétention des données agrégées ou anonymisées (en fonction du degré de dépersonnalisation et de confidentialité des données sous-jacentes) et une interdiction de repersonnalisation des données[49].

M. Parsons a recommandé que la LPRP donne le pouvoir au commissaire d'évaluer la proportionnalité de tout programme d'anonymisation d'ensemble de données. Il a aussi suggéré d'établir un site central qui permettrait aux Canadiens de voir si leurs données personnelles ont été recueillies ou transmises à des institutions fédérales[50].

M. Geist a recommandé d'inclure dans le mandat de la LPRP, comme c'est le cas sous la LPRPDE, un mandat relatif à l'éducation du public et la recherche. Il suggère aussi d'inclure un régime d'atteinte aux mesures de sécurité, comme celui qui se trouve sous la LPRPDE et d'imposer dans la loi une obligation de mener des évaluations des incidences sur la vie privée lorsque de nouveaux programmes sont lancés. À l'égard de la conservation des données comme celles auxquelles l'ASPC a eu accès, M. Geist note que toutes les lois modernes prévoient une limite, soit que les renseignements ne soient conservés qu'aussi longtemps qu'ils sont nécessaires.

47 Mémoire de Christopher Parsons.

48 *Ibid.* M. Parsons note dans son mémoire qu'à l'heure actuelle l'article 4 de la *Loi sur la protection des renseignements personnels* justifie presque tout traitement des données par le gouvernement fédéral, pourvu que cela soit lié à un programme ou une activité de l'institution fédérale.

49 *Ibid*.

50 *Ibid*.

## Modification de la *Loi sur la protection des renseignements personnels et les documents électroniques*

M. Therrien a expliqué ce qui suit à l'égard ce que l'on devrait trouver dans les lois relatives à la protection des renseignements personnels :

> 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.

Selon M. Therrien, le cadre législatif doit laisser une marge de manœuvre et permettre d'innover au chapitre de l'utilisation des données à des fins commerciales légitimes ou pour le bien public. Toutefois, il doit protéger la vie privée en tant que droit de la personne et être appliqué par un organisme de réglementation qui est habilité à réaliser des audits ou des enquêtes afin d'assurer que, dans ces circonstances, les données sont effectivement utilisées correctement. Le cadre devrait inclure des pénalités conséquentes pour les acteurs ou les entreprises qui enfreignent la loi.

M. Parsons était d'avis que les *Lignes directrices pour l'obtention d'un consentement valable* devraient être intégrées dans la LPRPDE. Il a suggéré que :

> [C]haque fois que le gouvernement du Canada reçoit d'organisations privées des renseignements identifiables ou des renseignements agrégés et anonymes provenant de personnes, il devrait être tenu de démontrer que ces renseignements ont été recueillis par ces organisations après que les personnes aient consenti de manière significative à leur collecte et à leur communication.

M. Parsons a recommandé d'obliger ces organisations à indiquer si elles ou leurs partenaires recueillent des informations, plutôt que de simplement évoquer la possibilité qu'elles puissent le faire. Il obligerait aussi les organisations à indiquer les autres parties auxquelles elles communiquent des renseignements et les usages qu'elles entendent en faire. Enfin, il inclurait dans la LPRPDE une obligation de fournir des rapports sur les mesures de transparence[51].

51 *Ibid.*

M^me^ Snively a noté que le RGPD comporte d'excellents éléments, dont l'intégration du principe de la protection de la vie privée dès la conception. Elle a toutefois noté que la LPRPDE actuelle contient aussi de bons éléments, notamment le fait qu'elle s'appuie largement sur des principes et qu'elle a permis à Telus d'être souples et agiles dans sa façon d'évaluer la protection de la vie privée.

À la question de créer un tribunal à la protection de la vie privée, M. Geist a noté qu'un tribunal devait être créé par le projet de loi C-11 (43-2). Il a indiqué qu'il y avait toutefois de l'opposition à l'égard de ce tribunal, dont de la part du commissaire. Il a dit ne pas être contre l'idée, mais seulement si le tribunal est un tribunal expert, ce qui n'était pas le cas dans l'ancien projet de loi. En matière d'application de la loi, M. Geist a noté que la loi devrait contenir de sévères pénalités et permettre au commissaire d'émettre des ordonnances.

## Observations et recommandations du Comité

Le Comité est d'avis que les lois fédérales en matière de protection des renseignements personnels doivent être améliorées le plus rapidement possible afin de s'adapter à la réalité actuelle où les données de millions d'utilisateurs sont quotidiennement recueillies, utilisées et communiquées à différentes fins; certaines louables, comme le cas en l'espèce; d'autres, plus problématiques.

Par conséquent, le Comité fait les recommandations suivantes :

**Recommandation 10**

**Que le gouvernement du Canada insère dans les lois fédérales en matière de protection des renseignements personnels, une interdiction de repersonnalisation de données dépersonnalisées et une pénalité conséquente.**

**Recommandation 11**

**Que le commissaire à la protection de la vie privée du Canada soit autorisé à vérifier de façon proactive les pratiques de tous les tiers fournisseurs de données mobiles pour s'assurer qu'ils respectent la *Loi sur la protection des renseignements personnels et les documents électroniques* lorsque les données recueillies sont utilisées par une institution fédérale.**

**Recommandation 12**

**Que le gouvernement du Canada modifie la *Loi sur la protection des renseignements personnels* et la *Loi sur la protection des renseignements personnels et les documents électroniques* afin de réglementer les activités des entreprises privées en matière de collecte, d'utilisation, de partage, de stockage et de destruction des données sur la mobilité des Canadiens, et que le gouvernement s'assure que les entreprises privées ont obtenu un consentement valable de leurs clients pour la collecte de ces données.**

**Recommandation 13**

**Que le gouvernement du Canada renforce les pouvoirs du Commissariat à la protection de la vie privée du Canada lui permettant de superviser le droit à la vie privée des Canadiens, avec le pouvoir d'enquêter et d'appliquer une *Loi sur la protection des renseignements personnels* et une *Loi sur la protection des renseignements personnels et les documents électroniques* renforcées, y inclus le pouvoir de rendre des ordonnances et la capacité d'imposer des pénalités.**

**Recommandation 14**

**Que le gouvernement du Canada modifie la *Loi sur la protection des renseignements personnels et les documents électroniques* afin d'obliger les fournisseurs de services qui recueillent des données à afficher un message offrant à l'utilisateur la possibilité de se retirer de la collecte de données, de continuer à utiliser le service sans accepter les conditions d'utilisation ou encore de refuser toutes les conditions et les témoins.**

**Recommandation 15**

**Que le gouvernement du Canada oblige les entreprises qui génèrent, gèrent, vendent ou utilisent des données à se conformer à un cadre additionnel à celui de l'autoréglementation.**

**Recommandation 16**

**Que le gouvernement du Canada ait l'obligation de faire ses propres vérifications sur la provenance des données ainsi que le consentement valable, les modalités de collecte, de transmission et de l'utilisation des données.**

**Recommandation 17**

**Que le gouvernement du Canada insère dans la *Loi sur la protection des renseignements personnels* un mandat d'éducation du public et de recherche similaire à celui que l'on**

**retrouve dans la *Loi sur la protection des renseignements personnels et les documents électroniques*.**

**Recommandation 18**

**Que le gouvernement du Canada modifie la *Loi sur la protection des renseignements personnels* afin d'y inclure des critères de nécessité et de proportionnalité pour l'utilisation, la collecte et la divulgation des renseignements personnels.**

**Recommandation 19**

**Que le gouvernement du Canada insère dans les lois fédérales en matière de protections des renseignements personnels la norme de la vie privée dès la conception.**

# CHAPITRE 5 : MÉGADONNÉES, SURVEILLANCE MASSIVE ET IMPACTS SOCIAUX POTENTIELS

## Mégadonnées et compréhension des utilisateurs

M. Therrien a noté que de manière générale, les gens ne sont pas au courant des nombreuses manières dont leurs données sont utilisées. Il espère que les utilisateurs de Telus 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 [*Les données au service du bien commun*]. Les Canadiens 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 pas à combien de fins elles peuvent être utilisées de nos jours.

M. Parsons a indiqué que peu d'utilisateurs réalisent qu'en acceptant de fournir des données sur la mobilité à un développeur d'application, ils permettent également que cette information soit vendue ou rendue disponible à d'autres entreprises. Dans ce contexte, l'utilisateur consent à la première utilisation, mais pas à la deuxième. Les clients peuvent lire les politiques de confidentialité, mais ces documents sont très difficiles à lire et à évaluer. Par exemple, la commissaire à l'information et la protection de la vie privée de l'Alberta a conclu dans une enquête impliquant Telus et Babylon

Health que la politique de confidentialité de Babylon Health était insuffisante pour un consentement éclairé[52].

M. French a fait des commentaires similaires quant à la complexité des conditions de services et politiques de confidentialité. Il a dit :

> Je pense que c'est une pratique générale, dans notre culture, de cliquer sur le bouton « j'accepte ». […] C'est tout simplement la culture dans laquelle nous vivons aujourd'hui. En effet, nous ne lisons généralement pas les conditions de service et les politiques de confidentialité, et nous ne sommes donc pas souvent conscients de ce que cela signifie. Comment le pourrions-nous? Trop souvent, ces conditions et politiques ne sont pas rédigées très clairement et elles ne sont pas écrites pour être lues ou comprises facilement.
>
> Je pense que c'est un gros problème. De nombreuses organisations affirment utiliser des renseignements personnels sur la santé, des données sur la mobilité et d'autres types de renseignements. Même après avoir regroupé et anonymisé ces données, par exemple, la question du consentement se profile toujours, de manière plus générale, à l'arrière-plan.

Mme Scassa a dit que l'utilisation de données sur la mobilité et la réaction qu'elle suscite mettent en lumière certains défis de notre société numérique et de données. Cette réaction confirme que les gens sont préoccupés par l'utilisation de leurs données et qu'ils ont du mal à saisir l'ampleur de la collecte de données, qui sont les acteurs engagés dans la collecte et le traitement des données et comment elles sont communiquées et utilisées par d'autres acteurs.

Mme Scassa a noté que les données sont souvent amassées et utilisées à des fins qui vont bien au-delà du maintien des relations avec le consommateur ou client. Elles carburent l'analyse, le profilage et l'intelligence artificielle. Certaines utilisations sont souhaitables et socialement bénéfiques; d'autres, nuisibles ou profondément abusives. Le défi consiste à faciliter les utilisations positives des données et mettre fin aux utilisations négatives.

Mme Scassa a rajouté qu'il faut souvent adhérer à toutes sortes de politiques de protection de la vie privée, alors que nous n'avons pas le temps, ni parfois les compétences nécessaires pour les comprendre.

52 Mémoire de Christopher Parsons; Commissaire à l'information et à la protection de la vie privée de l'Alberta, *Investigation Report P2021-R-02: Investigation into Babylon by Telus Health's compliance with Alberta's Personal Information Protection Act*, p. 67 [DISPONIBLE EN ANGLAIS SEULEMENT].

M. Murakami Wood est d'avis qu'à l'heure actuelle, le consentement éclairé est pratiquement dénué de sens. Il est impossible de comprendre ou de lire les politiques créées par les sociétés et les gouvernements. Les types particuliers d'opérations, comme la localisation, sont souvent cachés dans ces politiques. Le consentement n'est pas significatif, car il est souvent exigé pour obtenir un service : si vous ne donnez pas votre consentement, vous n'obtenez pas le service.

M. Lyon a aussi convenu qu'il devient de plus en plus difficile d'obtenir le consentement dans l'environnement de collecte et d'analyse des données dans lequel nous vivons actuellement. Selon lui, il faut assurer une éducation beaucoup plus approfondie du public afin que les personnes comprennent ce qu'elles font lorsqu'elles donnent soi-disant leur consentement et lorsqu'elles le donnent réellement.

M. Deneault a répondu ce qui suit concernant l'habileté des gens à exprimer clairement leur consentement à la collecte et l'utilisation de leurs données :

> La réponse est non, tout simplement. Des études ont été faites sur la difficulté qu'il y a à vraiment comprendre les contrats qu'on nous fait signer lorsque nous devenons des utilisateurs de ces logiciels qui collectent nos données dès que nous les utilisons. Nous connaissons tous l'adage: quand on nous donne quelque chose comme un logiciel, c'est parce que c'est nous, le produit. Il faut une formation de juriste, et encore, pour avoir un jugement éclairé sur ce à quoi on s'engage quand on utilise ces logiciels.

M. Deneault est même allé jusqu'à suggérer que la production de données massive par les géants de la technologie constitue un appauvrissement juridique du point de vue des États, parce que ces entreprises, qui détiennent un monopole technique, se trouvent à faire le droit par l'entremise de contrats d'adhésion.

M. Deneault a suggéré que la production de données massives est en soi un dispositif totalitaire, qui consiste à quadriller la réalité comportementale des sujets et à la rendre prévisible, voire contrôlable. Il estime que cette production devrait être empêchée à la source. Selon lui, les préoccupations éthiques qui existent à l'égard de l'utilisation des données résident dans le fait que le dispositif est totalitaire. Il a néanmoins reconnu qu'il y a des risques à ne pas utiliser des données massives, mais suggéré que le risque est de banaliser la surveillance.

M. Deneault, s'inspirant des propos de l'éthicien Hans Jonas, a soulevé les points suivants à l'égard des mégadonnées. Les techniques de production mise en œuvre aujourd'hui agissent sur la subjectivité humaine. Si on laisse de telles techniques se déployer à l'échelle sociale sans être capable de mesurer ni de contrôler leur incidence (vérifier ce qu'elles génèrent à l'échelle sociale et politique) on ne fait pas preuve

d'éthique. Enfin, il faut être aussi créatif en matière d'éthique que sont inventifs les techniciens qui créent ces engins.

M. French a soulevé des inquiétudes à l'égard de la dépendance de plus en plus grandes du secteur public envers des organismes privés pour faire son devoir et exercer ses responsabilités envers le public. Il a noté, par exemple, que la fragilité du système de santé publique couplée à la capacité incroyable de rassembler des données que possèdent les entreprises privées conduit logiquement à penser à aller chercher des données auprès d'elles.

Confrontés à des questions relatives à l'exploitation des données et au capitalisme de surveillance, Dr Khan a concédé que certaines utilisations des données sont préoccupantes et entraînent des répercussions sociales négatives, mais il a indiqué ne pas croire que le travail de BlueDot, qui selon lui est noble et vise le bien commun, tombe sous cette catégorie. Mme Snively a fait des commentaires similaires à l'égard des activités de Telus.

## Surveillance et limites de la collecte de données

### Définition de la surveillance

M. Lyon a noté qu'on associe souvent la surveillance à une activité policière, par exemple qui permet de garder un suspect sous observation ou pour surveiller des personnes soupçonnées de terrorisme. Or, la définition du terme surveillance est beaucoup plus large et inclut la surveillance en santé publique. Selon lui, la surveillance devrait être définie comme étant « l'attention ciblée, routinière et systématique portée aux renseignements personnels à des fins particulières, comme la gestion, la protection ou l'influence ».

M. DeMarsh a expliqué que dans le domaine de la santé publique le mot « surveillance » est couramment utilisé comme un terme fourre-tout pour les données sur les cas de maladies infectieuses ou d'autres maladies. C'est un terme général bien compris dans le domaine de la collecte de données de santé publique.

### Impacts sociaux potentiels

M. Murakami Wood a exposé au Comité le risque que présente la collecte de grands ensembles de données : le fait que ceux-ci cachent des formes existantes de préjugés et d'idées préconçues. Selon lui il est très important de pouvoir comprendre non

seulement les données en tant que faits, mais aussi dans leur contexte social. Il a partagé un scénario fictif pour illustrer ce point :

> Supposons que, dans les « data for good » de Telus — et ceci n'est qu'un scénario fictif, soit dit en passant — on ait découvert que les habitants d'une certaine banlieue de Toronto parcouraient de plus longues distances plus souvent que les autres habitants de Toronto. Vous pourriez facilement supposer, à partir de ces données, que ces personnes propagent le virus ou désobéissent aux consignes du gouvernement en matière de déplacements. En réalité, si vous examinez cette banlieue particulière, vous constatez qu'il s'agit d'un quartier à faible revenu, dans lequel vivent principalement des personnes noires et des minorités ethniques. Vous avez dans cette zone des gens qui doivent se déplacer pour se rendre à des emplois dans le secteur de l'entreposage ou travailler dans l'économie des petits boulots, et la raison pour laquelle ils sont mobiles et se déplacent plus souvent est précisément parce qu'ils sont défavorisés. Par conséquent, le fait de stigmatiser ces personnes ou de les rendre responsables de la propagation du virus serait une mauvaise lecture des faits sociaux sur le terrain.

Christopher Parsons a aussi noté que même les données agrégées ou anonymisées peuvent avoir des effets au niveau de la population quand cette information est utilisée pour développer des politiques publiques comme l'allocation de ressources et de services. Par exemple, certaines communautés pourraient être moins représentées dans les données sur la mobilité si tous les membres d'une famille n'ont pas d'appareil mobile. Ainsi, il faut considérer l'impact sur les communautés et non pas juste sur la violation de la vie privée d'un individu[53].

M. French a fait des commentaires similaires. Il n'est pas contre la surveillance en santé publique, mais s'intéresse à évaluer si elle aide les gens ou si elle leur nuit. Comme les données sur la mobilité peuvent être utilisées pour formuler des recommandations ou cerner des problèmes comme le non-respect des consignes de confinement ou d'un couvre-feu, M. French note que s'il s'en suit une intensification du maintien de l'ordre ou de l'application de la loi, cela pourrait peser lourdement sur des groupes aux prises avec d'autres problèmes. Dans un mémoire soumis au Comité, il explique davantage comment il est possible que certains groupes soient exposés à des risques ou des

53 Mémoire de Christopher Parsons.

préjudices accrus en raison du suivi de la mobilité pour la santé publique, se penchant sur des questions d'équité[54].

M. Lyon a aussi reconnu que la surveillance de santé publique est une tâche importante, mais souligne que cela n'enlève rien au fait qu'elle comporte des risques à chaque étape : collecte, analyse, interprétation et utilisation. Chaque étape présente des difficultés et peut inclure des préjudices au niveau individuel ou au niveau du groupe. Selon M. Lyon, la surveillance peut causer toutes sortes de torts, mais aussi procurer des avantages à la société.

M. Murakami Wood a toutefois précisé que la surveillance et l'utilisation d'ensembles de données ne sont pas en soi une forme de violation de fait des droits de la personne ou d'autres droit. Elle peut être bonne, dans la mesure où elle est à la base de l'élaboration de politiques fondées sur des preuves. Il a offert l'exemple du débat relatif au recensement long ou malgré certaines réserves à l'égard de la vie privée, la majorité des universitaires plaidait en sa faveur, car il fournissait des données importantes permettant l'élaboration de politiques efficaces.

## Limites de la surveillance

M^me^ Cavoukian a noté que pendant une crise ou une situation d'urgence, comme c'était le cas lors du 11 septembre 2001, des mesures d'urgence peuvent être adoptées pour mettre de côté des dispositions sur la protection de la vie privée. Le problème, selon elle, c'est qu'une fois la situation d'urgence terminée, les mesures d'urgence restent souvent en place. La transparence disparaît et la surveillance ne cesse de croître. Il faut donc s'assurer qu'une fois la pandémie terminée, les mesures prises pendant la situation d'urgence soient suspendues.

M^me^ Cavoukian soulève aussi le fait que plusieurs technologies sont mises en place sans tenir compte de l'effet qu'elles peuvent avoir sur les autres, donnant l'exemple des systèmes de caméras qui capturent des photos des voisins. Selon elle, il faut mettre en

54 Martin French, *Mémoire au comité ETHI : Étude sur la collecte et l'utilisation des données sur la mobilité par le gouvernement du Canada*, 25 mars 2022. M. French fait trois recommandations à l'égard de l'Agence de la Santé publique du Canada: elle devrait faire davantage de travail de sensibilisation et d'éducation du public autour des initiatives de suivi de la mobilité et de surveillance des maladies; elle devrait empêcher l'accès par les autorités chargées de l'application de la loi aux données de suivi sur la mobilité ou autres données de surveillance, afin d'éviter entre autres la criminalisation des maladies; et elle devrait développer de robustes formes d'engagement communautaire, par exemple à l'aide de conseils consultatifs communautaires indépendants et axés sur la surveillance dont le mandat consisterait s'assurer que l'avis de divers membres de la communauté à l'égard d'initiatives de suivi de la mobilité et de surveillance des maladies soit entendu.

place des mesures qui réduisent la collecte de données, la surveillance, et qui maximisent les choix relatifs à la vie privée que les gens peuvent faire.

M^me^ Cavoukian a aussi noté qu'aujourd'hui elle n'a plus besoin d'expliquer aux gens pourquoi la vie privée est importante puisqu'ils sont déjà inquiets à son sujet. Elle note un déclin de la confiance du public envers les institutions, et une crainte généralisée quant à la possibilité d'atteintes à la vie privée. Cette réalité fait en sorte que :

> Il s'ensuit une surveillance qui s'intensifie pour prendre des proportions colossales. Il arrive souvent que des gens me disent que l'on est aussi bien de renoncer à notre vie privée, que ce n'est tout simplement plus possible. Non, il ne faut pas baisser les bras. La protection de la vie privée est le fondement même de notre liberté. Si nous voulons vivre dans une société libre et ouverte, il faut que notre vie privée soit protégée. Je continue donc à lutter pour cette cause même si la confiance s'étiole. Travaillons ensemble pour rétablir cette confiance. Réclamons de nos gouvernements qu'ils nous indiquent franchement ce qu'ils font avec notre information ou, tout au moins, qu'ils nous avisent en pareil cas. En camouflant le tout pour que personne ne soit au courant, on ne fait malheureusement qu'alimenter la méfiance.

Le Comité est d'accord. Il n'est pas temps de renoncer à la vie privée.

## Observations et recommandations du Comité

Le Chapitre 5 met en évidence les nombreux défis que vivre dans une société hautement numérique peut engendrer. Il confirme que de nombreuses personnes ne comprennent pas la fréquence à laquelle leurs données personnelles sont recueillies, utilisées et partagées, ni l'impact que peuvent avoir les différentes formes de surveillance. Le Comité fait donc les recommandations suivantes :

**Recommandation 20**

**Que le gouvernement du Canada augmente ses investissements dans les initiatives de littératie numérique, y compris les initiatives visant à informer les Canadiens des risques associés à la collecte et à l'utilisation des données massives.**

**Recommandation 21**

**Que le gouvernement du Canada augmente son travail de sensibilisation et d'éducation du public entourant ses initiatives de suivi de la mobilité et de surveillance des maladies.**

**Recommandation 22**

**Que le gouvernement du Canada élabore des lignes directrices claires concernant l'utilisation de données sur la mobilité par les institutions fédérales et qu'il consulte dans ce processus le Commissariat à la protection de la vie privée, les parties prenantes et les groupes communautaires qui pourraient être touchés de façon disproportionnée par une telle initiative.**

## CONCLUSION

Le cas concernant l'ASPC a mis en lumière les défis que représente la société numérique dans laquelle nous vivons. En raison de cette réalité, le Comité suggère que lorsque le gouvernement cherche à exploiter le potentiel des mégadonnées, comme les données sur la mobilité, il devrait le faire de la manière la plus transparente possible, en redoublant d'efforts pour expliquer aux citoyens quel genre de données sont recueillies, pourquoi elles sont nécessaires, comment elles vont être utilisées et comment se retirer de l'initiative s'ils le souhaitent.

Les témoignages ont aussi clairement illustré que le cadre réglementaire actuel au Canada n'est pas adéquat pour bien encadrer l'utilisation des données, en particulier celles qui sont dépersonnalisées ou agrégées. Le Comité constate, comme il l'a fait dans plusieurs rapports antérieurs que les lois fédérales en matière de protection des renseignements personnels doivent absolument être modernisées. Le Comité est convaincu que, si elles sont mises en œuvre, les recommandations formulées dans ce rapport permettront de renforcer la protection de la vie privée des Canadiens.

Le Comité invite aussi le gouvernement du Canada à consulter les recommandations de ses rapports antérieurs en plus de celles qui se trouvent dans le présent rapport.

# ANNEXE A
# LISTE DES TÉMOINS

Le tableau ci-dessous présente les témoins qui ont comparu devant le Comité lors des réunions se rapportant au présent rapport. Les transcriptions de toutes les séances publiques reliées à ce rapport sont affichées sur la page Web du Comité sur cette étude.

| Organismes et individus | Date | Réunion |
|---|---|---|
| **Agence de la santé publique du Canada** | 2022/02/03 | 4 |
| Christopher Allison, vice-président par intérim<br>Direction générale surveillance et données organisationnelles | | |
| D^re^ Theresa Tam, administratrice en chef de la santé publique | | |
| Kathy Thompson, première vice-présidente | | |
| **Ministère de la Santé** | 2022/02/03 | 4 |
| L'hon. Jean-Yves Duclos, C.P., député, ministre de la santé | | |
| **À titre personnel** | 2022/02/07 | 5 |
| Khaled El Emam, chaire de recherche du canada en intelligence artificielle médicale | | |
| **Commissariat à la protection de la vie privée du Canada** | 2022/02/07 | 5 |
| Daniel Therrien, commissaire à la protection de la vie privée du canada | | |
| Martyn Turcotte, directeur<br>Direction de l'analyse des technologies | | |

| Organismes et individus | Date | Réunion |
|---|---|---|
| **À titre personnel** | 2022/02/10 | 6 |
| Ann Cavoukian, directrice exécutive<br>Global Privacy and Security by Design | | |
| Martin French, professeur agrégé<br>Département de sociologie et anthropologie, Université Concordia | | |
| Teresa Scassa, titulaire de la chaire de recherche en droit et politiques de l'information<br>Faculté de droit, Section Common Law, Université d'Ottawa | | |
| Daniel Weinstock, professeur titulaire<br>Département de philosophie, Université McGill | | |
| **À titre personnel** | 2022/02/14 | 7 |
| Alain Deneault, professeur de philosophie | | |
| David Lyon, professeur émérite<br>Queen's University | | |
| David Murakami Wood, directeur<br>Surveillance Studies Centre et professeur agrégé, Département de sociologie, Queen's University | | |
| Christopher Parsons, associé de recherche principal<br>Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto | | |
| **BlueDot** | 2022/02/17 | 8 |
| Alex Demarsh, directeur<br>Science des données | | |
| Dr Kamran Khan, président-directeur général et fondateur professeur en médecine et en santé publique, University of Toronto | | |
| **Société Telus Communications** | 2022/02/17 | 8 |
| Pamela Snively, vice-présidente<br>Chef des donnés et du Bureau des relations de confiance | | |
| **À titre personnel** | 2022/02/28 | 9 |
| Jean-Pierre Charbonneau, ex-parlementaire du québec et conférencier sur l'éthique | | |
| Michael Geist, professeur de droit<br>Titulaire de la chaire de recherche du Canada en droit d'Internet et du commerce électronique | | |

# ANNEXE B
# LISTE DES MÉMOIRES

Ce qui suit est une liste alphabétique des organisations et des personnes qui ont présenté au Comité des mémoires reliés au présent rapport. Pour obtenir de plus amples renseignements, veuillez consulter la page Web du Comité sur cette étude.

**Bell Canada**

**French, Martin**

**Parsons, Christopher**

# DEMANDE DE RÉPONSE DU GOUVERNEMENT

Conformément à l'article 109 du Règlement, le Comité demande au gouvernement de déposer une réponse globale au présent rapport.

Un exemplaire des *procès-verbaux* pertinents (réunions nos 3 à 10, 13, 14 et 16) est déposé.

Respectueusement soumis,

Le président,
Pat Kelly

**Opinion dissidente du Parti libéral du Canada**

Le 13 janvier 2022, le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes (le " Comité ") a adopté à l'unanimité une motion visant à étudier la question de la collecte et de l'utilisation des données sur la mobilité par le gouvernement du Canada. La motion se lit comme suit :

> *Que, à la lumière des rapports récents des médias, le Comité entreprenne immédiatement une étude, conformément à l'article 108(3)(h)(vi) et (vii) du Règlement, 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, à leur insu ou sans leur consentement, et : (a) invite l'administratrice en chef de la santé publique du Canada à comparaître pendant une heure, y compris une déclaration d'ouverture de cinq minutes; (b) invite le ministre de la Santé à comparaître pendant une heure, y compris une déclaration d'ouverture de cinq minutes; (c) demande aux membres du Comité de fournir au greffier, une journée après l'adoption de cette motion, leurs listes préliminaires de témoins pour cette étude .*

Les membres libéraux du Comité reconnaissent l'importance de la vie privée des Canadiens et la responsabilité du gouvernement de protéger cette vie privée. Bien que les membres libéraux applaudissent les efforts du Comité pour s'attaquer au problème en question, nous constatons que :

- La motion est fondée sur des rapports inexacts sur la portée de la collecte et de l'utilisation des données sur la mobilité par l'Agence de la santé publique du Canada. Des témoins ont confirmé que si des données sur la mobilité ont été recueillies, elles ne concernaient pas 33 millions de personnes, comme l'ont rapporté et répété les membres du Comité. Les membres libéraux du Comité notent également que le texte de la motion est basé sur une fausse prémisse - que les Canadiens n'ont pas été informés de cette collecte de données dépersonnalisées et agrégées alors qu'en fait, le gouvernement a annoncé en mars 2020 cette collecte. Le travail effectué avec la collecte de données sur la mobilité a été rendu public sur le site Web COVIDTrends comme un moyen de fournir aux Canadiens des informations locales sur le COVID-19 dans leurs communautés avec des explications sur la façon dont ces données sont utilisées, et les protections de la vie privée actuellement en place.

- Le rapport, bien qu'il mette en lumière d'importantes questions relatives à la protection de la vie privée et à la responsabilité du gouvernement en matière d'ouverture et de transparence, comprend des recommandations générales qui vont au-delà de la portée de l'étude proposée par la motion susmentionnée. L'étude entreprise par le Comité était en fait une étude de cas d'un contrat spécifique engageant des entrepreneurs pour collecter, dépersonnaliser et agréger des données sur la mobilité dans le but de mieux informer les décisions de politique de santé publique pendant la pandémie de COVID-19. L'appel d'offres comprenait des dispositions qui imposaient la protection de la vie privée des Canadiens. Des témoins ont confirmé que, pour mieux protéger la vie privée, l'Agence de la santé publique du Canada a également utilisé une approche à barrières multiples depuis la source des données, tout au long du pipeline de

données et avant leur réception. En fait, les témoins ont confirmé que même si le risque de réidentification des données n'est jamais nul, dans ce contrat, il n'y a pas eu d'atteinte à la vie privée des Canadiens et des normes strictes de protection de la vie privée ont été suivies.

- Le rapport identifie plus de 20 recommandations qui vont au-delà de la portée de cette étude de cas. Les membres libéraux du Comité notent que de nombreuses recommandations demandent au gouvernement de faire ce qu'il fait déjà. Par exemple, le Comité a entendu des témoins dire que le gouvernement procède déjà à des consultations importantes et continues avec le commissaire à la protection de la vie privée et des experts en la matière lorsqu'il s'agit de la collecte de données. Un autre exemple est que le commissaire à la protection de la vie privée a déjà le pouvoir d'enquêter sur les plaintes et les éventuelles atteintes à la vie privée.

- Les membres libéraux du Comité notent également que plusieurs recommandations de ce rapport exigent que la législation sur la protection de la vie privée soit modifiée de diverses façons. Nous convenons que la législation sur la protection de la vie privée, notamment la Loi sur la protection des renseignements personnels et les documents électroniques (LPRDE), doit être modernisée. Toutefois, nous sommes d'avis que cette modernisation doit être fondée sur un examen complet de la législation fédérale sur la protection de la vie privée qui définit et saisit clairement la portée, l'utilisation et la communication des données dépersonnalisées et agrégées ; cet examen devrait inclure l'établissement d'une norme pour la dépersonnalisation des données. En l'absence d'un examen complet, il pourrait en résulter un ensemble de modifications disparates qui ne permettraient pas de relever les défis actuels.

- Les membres libéraux du Comité notent que le ministre de l'Innovation, des Sciences et de l'Industrie s'est engagé à faire de la réforme de la protection de la vie privée numérique une priorité absolue, notamment la réforme de la Loi sur la protection des renseignements personnels et les documents électroniques (LPRDE), et qu'il tiendra compte de ces considérations.

- Nous notons également que le ministre de la Justice et procureur général du Canada s'est également engagé à réformer la Loi sur la protection des renseignements personnels (LPRP) et qu'il tiendra également compte de ces considérations. En particulier, il a été mandaté pour s'appuyer sur les consultations publiques précédentes et les engagements techniques entre experts et pour poursuivre l'examen de fond de la LPRP, y compris l'engagement avec les partenaires autochtones pour élaborer des propositions spécifiques de modifications.

- Les membres libéraux du Comité croient que, lorsqu'il s'agit de la protection de la vie privée des Canadiens, il est toujours possible de faire mieux et que le gouvernement devrait continuer à examiner les politiques et les lois et identifier les lacunes dans l'espace numérique en constante évolution et ses implications sur la vie privée des Canadiens.

Les membres libéraux du Comité remercient les analystes et le greffier de la Chambre des communes pour leur travail acharné sur cette importante étude de cas, ainsi que les témoins qui ont comparu devant nous et ont contribué à la rédaction du présent rapport.