À l'intention du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique : *Étude sur la collecte et l'utilisation des données sur la mobilité par le gouvernement du Canada*

Christopher Parsons
Associé de recherche principal

Citizen Lab
Munk School of Global Affairs & Public Policy
Université de Toronto

Introduction

1. Je suis associé de recherche principal au Citizen Lab de la Munk School of Global Affairs & Public Policy, à l'Université de Toronto. Dans mes travaux, je m'intéresse aux recoupements entre le droit, les politiques et la technologie, et mes recherches portent sur les questions de sécurité nationale, de sécurité des données et de confidentialité des données. Je propose les réflexions qui suivent à titre professionnel, mais celles-ci ne traduisent pas nécessairement le point de vue du Citizen Lab.

Contexte

2. Je tiens tout d'abord à remercier les employés de l'ASPC et d'autres organismes qui luttent contre la propagation de la COVID-19 et à saluer leur travail. Mes réflexions ne visent en rien à discréditer leurs efforts. Elles visent plutôt à circonscrire les domaines de gouvernance des données où il y a lieu d'améliorer l'usage que fait le gouvernement des données sur la mobilité et, plus généralement, des renseignements personnels et anonymisés, ainsi que la gestion de ces renseignements par des sociétés privées.

3. Selon ma définition, les données sur la mobilité sont des données de géolocalisation extraites de réseaux d'appareils cellulaires comme ceux qu'exploite Telus, ainsi que les données de géolocalisation obtenues par les courtiers en données. Ces courtiers obtiennent souvent des renseignements en les achetant à des distributeurs d'applications ou en insérant des codes de traçage dans les applications de téléphones intelligents, le plus souvent à l'insu des propriétaires de ces appareils[1]. Quant aux données sur la mobilité utilisées par l'ASPC, elles ont été agrégées et anonymisées par TELUS et BlueDot avant que l'Agence n'en prenne possession.

Un cadre de communications chaotique

4. Dès le début de la pandémie de COVID-19, des organismes gouvernementaux, des organisations sans but lucratif, des groupes universitaires et des entreprises privées se sont attelés à trouver des moyens d'atténuer la propagation du virus. Dans les premiers jours de la pandémie, la communication d'informations provenant de tous les ordres de gouvernement était désordonnée. Entre autres causes de confusion, il y avait la mesure dans

[1] https://themarkup.org/privacy/2021/09/30/theres-a-multibillion-dollar-market-for-your-phones-location-data.

laquelle les gouvernements utilisaient les données sur la mobilité et à quelles fins.

5. Par exemple, et cela concerne cette étude, le premier ministre s'est prononcé le 24 mars 2020 sur la question de savoir si le gouvernement chercherait à obtenir des informations auprès des fournisseurs de télécommunications. Il a alors déclaré : « Pour autant que je sache, ce n'est pas quelque chose que nous envisageons actuellement[2]. » Il a cependant laissé planer la possibilité que ce soit le cas plus tard. Le même jour, la Dre Tam a précisé que l'idée d'utiliser des données sur la mobilité ne devrait pas être écartée, mais elle n'a pas laissé entendre que cela se faisait effectivement[3]. La veille, le 23 mars 2020, le maire John Tory déclarait que la municipalité de Toronto avait accès à des données sur la mobilité provenant des réseaux de télécommunications, mais cette déclaration a aussitôt été démentie : « La municipalité de Toronto ne recueille pas de données de géolocalisation sur les appareils cellulaires et on ne lui en communique pas. La municipalité de Toronto n'utilisera pas de données de géolocalisation des appareils cellulaires[4]. »

6. Une série d'articles ont été publiés à la fin d'avril au sujet de l'utilisation des données sur la mobilité pour limiter la propagation de la COVID-19. À l'époque, ni les journalistes ni les experts n'ont prétendu savoir si le gouvernement du Canada obtenait des données sur la mobilité auprès d'entreprises de télécommunications ou de BlueDot[5].

7. Pour illustrer la difficulté à se faire une idée de l'usage des données sur la mobilité par le gouvernement du Canada, songeons, par exemple, à ce qu'a déclaré le premier ministre à ce sujet comparativement à ce qu'ont révélé des sources non gouvernementales. Dans sa déclaration du 23 mars 2020, le premier ministre ne dit pas que des données de géolocalisation ont été fournies par BlueDot[6]; pour saisir la nature exacte de l'entente, il faut trouver et lire un communiqué de presse de l'Université de Toronto[7]. Au passage, précisons

---

[2] Voir : https://www.cbc.ca/news/politics/cellphone-tracking-trudeau-covid-1.5508236 [TRADUCTION].
[3] Voir : https://www.cbc.ca/news/politics/cellphone-tracking-trudeau-covid-1.5508236.
[4] Voir : https://www.cbc.ca/news/politics/cellphone-tracking-trudeau-covid-1.5508236 [TRADUCTION].
[5] Voir, p. ex. : https://ablawg.ca/2020/04/16/covid-19-and-cellphone-surveillance/; https://uwaterloo.ca/math/news/q-and-experts-privacy-vs-tracking-covid-19; https://theccf.ca/hed-police-are-using-phone-data-to-track-covid-patients-can-they-do-that/.
[6] Voir : Le Plan canadien de mobilisation des sciences pour lutter contre la COVID-19 | Premier ministre du Canada (pm.gc.ca). « Un soutien à BlueDot, qui est une entreprise numérique de santé de Toronto. Elle utilise une technologie d'alerte précoce mondiale, première du genre, pour les maladies infectieuses. L'entreprise a été l'une des premières au monde à détecter la propagation de la COVID-19. 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. »
[7] Voir : https://www.utoronto.ca/news/u-t-infectious-disease-expert-s-ai-firm-now-part-canada-s-covid-19-arsenal. « ... BlueDot fournira au gouvernement fédéral de l'information et du renseignement pour l'aider à lutter contre le virus – entre autres, en utilisant des données de géolocalisation anonymes prélevées sur des centaines de

que la politique de protection de la vie privée de BlueDot n'indique pas que l'entreprise participe à la collecte de données sur la mobilité[8].

8. Toujours pour illustrer combien il est difficile pour les Canadiens de savoir comment les données sur la mobilité ont été utilisées, reportons-nous aux renseignements fournis par le ministre Duclos à votre comité le 3 février 2022. Celui-ci a déclaré que l'ASPC s'était associée, en mars 2020, au Centre de recherches sur les communications d'ISDE pour utiliser les données fournies par TELUS. Il a également déclaré que les Canadiens pouvaient savoir quelles données sur la mobilité étaient utilisées en consultant le site de TendancesCOVID.

9. Outre les commentaires du commissaire Therrien, qui a expliqué au comité que, pour être renseigné sur l'utilisation des données sur la mobilité, il fallait connaître l'existence du site TendancesCOVID et se rendre jusqu'au bas de la page, il faut savoir que ces renseignements n'ont été mis à la disposition des Canadiens qu'à partir de décembre 2020. C'est-à-dire des mois après que TELUS et BlueDot eurent commencé à fournir des données sur la mobilité au gouvernement du Canada. On peut le confirmer en utilisant le service d'archivage des sites Web par la technologie Wayback Machine. Au 30 novembre 2020, le site n'affichait pas d'informations concernant les données sur la mobilité[9]; ces informations ne sont apparues dans les archives de Wayback Machine que dans une capture d'écran du 6 décembre 2020 montrant que le site avait été mis à jour le 3 décembre 2020[10]. Au 9 février 2022, le site Web ne précisait pas d'où viennent les données sur la mobilité et n'indiquait pas non plus comment les intéressés pouvaient refuser que l'on recueille leurs données s'ils le souhaitaient[11].

10. Je soulève ces questions non pas pour laisser entendre que le gouvernement a menti aux Canadiens, mais pour expliquer que le contexte des communications était chaotique. Je suis absolument d'accord avec le commissaire Therrien pour dire qu'il est tout à fait improbable que la plupart des Canadiens, ni même une infime minorité d'entre eux, savaient que le gouvernement se procurait des données sur la mobilité ou que ces données servaient à étayer les décisions stratégiques relatives à la COVID-19. Cette opacité a soulevé des questions concernant la transparence et le consentement associés à la collecte de ces

---

millions d'appareils cellulaires pour vérifier l'efficacité des mesures prises par la Santé publique. BlueDot est en train de produire des données métriques qui permettront au gouvernement de savoir où la distanciation sociale est efficace, si les gens suivent les recommandations de la Santé publique et où il convient de déployer de précieuses ressources. » [TRADUCTION]

[8] Voir : https://bluedot.global/privacy/.

[9] Voir : TendancesCOVID - Infobase santé publique | Agence de la santé publique du Canada (archive.org).

[10] Voir : TendancesCOVID - Infobase santé publique | Agence de la santé publique du Canada (archive.org).

[11] Voir : TendancesCOVID : Données sur la COVID-19 dans votre région | Agence de la santé publique du Canada (archive.org).

données par des entreprises privées et leur transmission au gouvernement du Canada.

11. J'ai quatre recommandations à formuler concernant TendancesCOVID. Premièrement, **je recommande** une mise à jour du site Web pour y préciser clairement que certaines personnes connaissent les sources exactes des données sur la mobilité utilisées par le gouvernement.

12. Deuxièmement, **je recommande** une mise à jour du site Web de TendancesCOVID pour y inclure un hyperlien vers la page de désinscription du programme des données au service du bien commun de TELUS[12], pour que les gens puissent s'exclure du partage de données entre TELUS et le gouvernement du Canada s'ils le souhaitent.

13. Troisièmement, **je recommande** de contraindre TELUS à intégrer sur tous les portails pour les clients (de TELUS, Koodo, etc.) un mécanisme d'exclusion qui soit visible pour que les gens sachent qu'ils ont le choix. Cela pourrait faire partie de la refonte de la LPRPDE proposée par le comité.

14. Quatrièmement, **je recommande** une mise à jour du site Web de TendancesCOVID pour permettre aux gens de s'exclure de la collecte de données de BlueDot, quoiqu'on ne sache pas pour l'instant avec certitude si BlueDot recueille des données sur la mobilité ni comment s'exclure de cette collecte.

L'utilisation des réseaux de télécommunications et des services d'analyse de données pour surveiller la situation sanitaire

15. En septembre 2021, on dénombrait 34 millions d'abonnements à des services sans fil au Canada[13]. La plupart des Canadiens s'attendent raisonnablement à ce que des fournisseurs de services de télécommunications comme TELUS recueillent des données sur la géolocalisation des appareils mobiles pour entretenir ou exploiter leur réseau (p. ex. pour la planification ou l'entretien). Mais la divulgation de données sur la géolocalisation des abonnés à des tiers, en dehors des besoins de développement et d'entretien du réseau — même si les données sont ostensiblement agrégées et anonymisées et sont autorisées dans la politique de confidentialité ou dans le contrat —, transforme de fait la nature des données techniques que TELUS recueille en les faisant passer du statut de données d'entretien du service à celui de base de données générales.

16. Les gens n'ont pas l'impression qu'on empiète sur leur vie privée lorsque des données de

[12] Voir : Opt-Out (telus.com).

[13] Voir : CWTA | Statistiques.

géolocalisation sont recueillies à des fins de réparation ou d'entretien du réseau, mais ce n'est plus le cas lorsque l'utilisation de ces données change, et notamment quand cela se produit à leur insu et sans leur consentement éclairé. Helen Nissenbaum, spécialiste des questions liées à la protection de la vie privée, estime que ce genre de situation est une violation des normes de protection des renseignements personnels, puisque l'utilisation des données à d'autres fins peut avoir techniquement pour effet de porter atteinte à la vie privée[14].

17. Je ne doute pas un instant que les employés de TELUS et le gouvernement du Canada aient eu à cœur ce qu'ils estimaient être les intérêts des Canadiens lorsqu'ils ont partagé des données sur la mobilité sous forme agrégée et anonymisée. Cela dit, même agrégées et anonymisées, ces données peuvent avoir des effets à l'échelle de la population lorsque les informations recueillies servent à orienter des décisions stratégiques. Certains groupes peuvent être contraints de se déplacer plus souvent durant la pandémie pour effectuer un travail essentiel, tandis que d'autres peuvent être moins représentés dans ces données si les membres d'un même ménage n'ont pas tous un appareil mobile, et c'est à partir de ces données que les gouvernements pourront être amenés à modifier la répartition de leurs ressources policières ou de services. Tout cela pour dire que même des données agrégées et anonymisées peuvent avoir des répercussions sur les collectivités. Il ne suffit pas de simplement se demander s'il y a violation de la vie privée individuelle — quoique cela s'est peut-être produit —; il est impératif de s'interroger sur les effets collectifs de la façon dont ces données sont recueillies et utilisées pour prendre des décisions stratégiques ou attribuer des ressources[15].

18. Concernant BlueDot, on a moins d'informations sur l'origine de leurs données sur la mobilité. D'après les renseignements accessibles au public, celles-ci semblent provenir « de données de géolocalisation anonymes tirées de centaines de millions d'appareils mobiles dans le but d'évaluer l'efficacité des mesures de santé publique[16] ». On aurait besoin de plus d'informations pour savoir exactement comment ces données de géolocalisation sont recueillies. Si elles proviennent du courtage de données — qui fonctionne largement à l'insu des gens dont les données sont recueillies et qui, par principe et régulièrement, les désanonymise[17] —, il serait troublant de constater que le gouvernement du Canada participe

[14] Voir « Privacy as Contextual Integrity » dans : https://digitalcommons.law.uw.edu/cgi/viewcontent.cgi?article=4450&context=wlr.
[15] Nous explicitons cette argumentation dans le rapport du Citizen Lab intitulé *Pandemic Privacy*, voir : https://citizenlab.ca/wp-content/uploads/2021/09/092721_pandemic-privacy_v3.pdf.
[16] Voir : https://www.utoronto.ca/news/u-t-infectious-disease-expert-s-ai-firm-now-part-canada-s-covid-19-arsenal [TRADUCTION].
[17] Voir « Estimating the success of re-identifications in incomplete datasets using generative models » dans : https://www.nature.com/articles/s41467-019-10933-3/.

à cette façon de faire, qui est vraisemblablement contraire à l'éthique, bien qu'apparemment légale.

19. J'aimerais faire deux recommandations. Premièrement, **je recommande** au comité de proposer une révision de la *Loi sur la protection des renseignements personnels* qui comprendrait des dispositions prévoyant que les entreprises privées qui fournissent des données anonymisées, agrégées ou identifiables à des organismes gouvernementaux soient tenues de prouver, avant de divulguer ces renseignements, qu'elles ont obtenu le consentement éclairé des gens que ces renseignements concernent.

20. Deuxièmement, **je recommande** au comité de proposer une révision de la *Loi sur la protection des renseignements personnels* pour couvrir les données anonymes et agrégées qui sont recueillies ou obtenues par des organismes gouvernementaux. Puisque nous entrons dans l'ère du Big Data — et comme la Dre Tam a indiqué que ce genre de données pouvait intéresser l'ASPC —, des données agrégées et anonymisées peuvent servir à orienter des politiques touchant les particuliers comme les collectivités, mais ces particuliers et ces collectivités ne se désintéressent pas de ces données sous prétexte qu'elles sont anonymisées. Cette proposition devrait clarifier l'obligation du gouvernement du Canada d'inclure 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'ils obtiennent, mais aussi prévoir l'approbation du commissaire à la protection de la vie privée avant toute mise en œuvre d'un programme associé à ce genre de données.

Un consentement éclairé à la collecte privée et à l'utilisation publique de données sur la mobilité

21. Beaucoup d'entreprises recueillent des données sur la mobilité à des fins commerciales. Il faut parfois consentir à la collecte d'informations, par exemple quand on doit autoriser une application à accéder à des données de géolocalisation. Peu d'utilisateurs se rendent compte que ce type de consentement peut permettre à l'exploitant d'avoir accès à leurs données de géolocalisation et de vendre ou de communiquer ces données à d'autres entreprises par le biais d'un code implanté dans l'application. Dans ce cas, l'utilisateur donne son consentement éclairé à l'exploitant de l'application pour l'autoriser à recueillir et utiliser des données de géolocalisation pour fournir un service. On ne peut pas en dire autant des tierces parties qui recueillent ou obtiennent aussi ces mêmes données.

22. Dans le même ordre d'idées, les abonnés à des services de télécommunications doivent prendre acte du fait qu'ils partagent des données de géolocalisation avec les fournisseurs de

services de télécommunications pour obtenir un service, mais ils sont moins susceptibles d'être conscients (ou de comprendre) que ces sociétés pourraient utiliser ces données à des fins commerciales autres que la fourniture de services de télécommunications.

23. Le commissaire à la protection de la vie privée fournit des directives aux entreprises concernant le consentement éclairé et ce qu'il suppose. Plus précisément, ces directives leur enjoignent de souligner les principaux aspects de la collecte, de l'utilisation et de la divulgation des données; de permettre aux clients de contrôler le degré de détail de la collecte, de l'utilisation et de la divulgation des leurs renseignements personnels; de fournir aux clients des choix clairs entre « oui » et « non »; de faire preuve d'innovation et de créativité, par exemple en fournissant des avis ponctuels ou en employant des outils interactifs, ou encore en élaborant des interfaces mobiles sur mesure; de tenir compte du point de vue des clients; de faire du consentement un processus dynamique et systématique; et de rendre des comptes en étant prêtes à faire la preuve qu'elles se conforment aux règles. Le Commissariat a notamment fait savoir que le consentement explicite est obligatoire lorsque des données sont utilisées ou divulguées alors que l'utilisateur n'a aucune raison de s'y attendre, y compris dans le cas de « la communication de certains renseignements à un tiers » ou « le suivi de géolocalisation »[18]. Les clients de TELUS ne sont pas invités à donner leur consentement éclairé pour autoriser l'utilisation de leurs renseignements personnels à d'autres fins que la fourniture de services de télécommunications. Même chose chez les courtiers en données qui obtiennent des données sur la mobilité à l'insu des utilisateurs. Rappelons que la commissaire à la protection de la vie privée de l'Alberta a conclu, au terme d'une enquête analogue sur l'entreprise Babylon Health de TELUS, qu'on ne donne pas son consentement explicite simplement en acceptant une politique de confidentialité[19].

24. **Je recommande** que le gouvernement du Canada, lorsqu'il obtient des données identifiables ou des données agrégées et anonymisées tirées des renseignements personnels fournis à des entreprises privées, soit tenu de faire la preuve que ces renseignements ont été recueillis et divulgués par ces entreprises avec le consentement éclairé des intéressés.

Les lacunes de la *Loi sur la protection des renseignements personnels*

25. Le commissaire à la protection de la vie privée et d'autres experts estiment qu'il faut absolument mettre à jour la *Loi sur la protection des renseignements personnels*. La LPRPDE exige d'obtenir le consentement des intéressés avant la collecte, l'utilisation et la divulgation de renseignements, alors que la *Loi sur la protection des renseignements personnels* autorise

[18] Voir : Lignes directrices pour l'obtention d'un consentement valable - Commissariat à la protection de la vie privée du Canada.
[19] Voir : https://www.oipc.ab.ca/media/1165666/P2021-IR-02.pdf, p. 218-221.

et justifie la plupart des usages que fait le gouvernement fédéral de ces renseignements au motif que la collecte, l'utilisation et la divulgation de renseignements personnels ont un lien direct avec les programmes opérationnels d'un organisme gouvernemental ou sont conformes aux fins de ces programmes. Comme mes collègues et moi-même l'avons déjà écrit, le principe du « lien direct avec des activités opérationnelles » est appliqué de façons contrastées. Le Conseil du Trésor et le Commissariat à la protection de la vie privée ont déjà défini la notion de « lien direct avec des activités opérationnelles » en prévoyant qu'il fallait déterminer si la collecte, l'utilisation ou la divulgation était « nécessaire », et, plus récemment, la Cour d'appel fédérale a statué que la *Loi sur la protection des renseignements personnels* n'impose pas d'obligation de nécessité aux organismes du gouvernement[20]. « Le consentement est donc un facteur important lorsque des organismes gouvernementaux souhaitent intervenir en dehors de leur mandat ou réorienter l'usage des données recueillies au départ à d'autres fins[21]. »

26. Les dispositions actuelles de la *Loi sur la protection des renseignements personnels* autorisent le gouvernement à recueillir des volumes importants de données à l'insu ou sans le consentement des intéressés. Comme l'a rappelé le ministre Duclos, le gouvernement estime que les données anonymisées et agrégées échappent au champ d'application de la *Loi sur la protection des renseignements personnels*. Il s'ensuit, aujourd'hui, que le gouvernement affirme être libre de recueillir ce genre de renseignements et de les réutiliser à d'autres fins que celles prévues au départ. Dans le cadre de la présente étude, l'ASPC n'a pas exprimé le désir, le besoin ou l'intention de désanonymiser ultérieurement les ensembles de données (peut-être en combinaison avec d'autres ensembles de données que l'ASPC a en sa possession). Il n'empêche que cette politique pourrait changer du jour au lendemain compte tenu des dispositions actuelles de la *Loi sur la protection des renseignements personnels*.

27. La commande qui a attiré l'attention du public sur l'utilisation que fait le gouvernement des données sur la mobilité souligne la nécessité de réviser la *Loi sur la protection des renseignements personnels*. La description du contrat prévoit que l'ASPC obtienne des données de géolocalisation auprès d'exploitants d'antennes-relais de téléphonie mobile pour analyser les données sur la mobilité des populations du Canada à des fins très larges, notamment pour « connaître la situation et […] éclairer les politiques, les messages de santé publique, l'évaluation des mesures de santé publique et d'autres aspects liés à la réponse, à la programmation, à la planification et à la préparation en matière de santé publique[22] ». Le

---

[20] Canada (Syndicat des agents correctionnels du Canada) c. Canada (Procureur général), 2019 FCA 212, par. 40.
[21] Voir : https://citizenlab.ca/wp-content/uploads/2021/09/092721_pandemic-privacy_v3.pdf, p. 34 [TRADUCTION].
[22] Données et services de localisation basés sur les opérateurs pour l'analyse de la mobilité en matière de santé publique (1000236419) - Achatsetventes.gc.ca.

libellé du contrat lui-même n'est pas du tout restrictif, pourtant, en vertu de la *Loi sur la protection des renseignements personnels*, l'ASPC pourrait étendre encore l'utilisation des renseignements en restant dans les limites de la réglementation, du moment qu'elle ne déborde pas de son mandat.

28. Certaines des limitations actuelles de la *Loi sur la protection des renseignements personnels* pourraient être corrigées par une révision du texte législatif. **Je recommande** donc une révision de la loi et l'inclusion de dispositions concernant la nécessité et la proportionnalité, afin de contraindre les organismes gouvernementaux à faire la preuve qu'ils ont besoin de données identifiables ou anonymisées pour remplir un mandat précis, et d'exiger que le degré de confidentialité des données soit proportionnel au mandat en question.

29. **Je recommande** également que le gouvernement révise la *Loi sur la protection des renseignements personnels* pour interdire aux organismes gouvernementaux de réutiliser des données en leur possession, à moins d'obtenir, s'il y a lieu, le consentement éclairé des intéressés à cet égard.

30. Concernant les ensembles de données anonymisées ou agrégées, **je recommande** une révision de la *Loi sur la protection des renseignements personnels* pour contraindre les organismes gouvernementaux à s'assurer que les intéressés ont donné leur consentement éclairé avant que leurs renseignements soient inclus dans des ensembles de données anonymisées; pour que des limites de conservation soient appliquées à ces ensembles (en fonction du degré de désanonymisation et de confidentialité des données sous-jacentes); que les tentatives de désanonymisation soient strictement interdites; et pour que le commissaire à la protection de la vie privée ait le pouvoir d'évaluer la proportionnalité des programmes de bases de données anonymisées.

31. **Je recommande** également une révision de la *Loi sur la protection des renseignements personnels* pour faire en sorte que le gouvernement soit tenu de créer un site central où les intéressés pourront évaluer la mesure dans laquelle leurs propres renseignements sont recueillis ou obtenus par des organismes gouvernementaux et savoir à quelles fins ils sont utilisés. Ce site devrait également indiquer clairement les organismes gouvernementaux qui obtiennent des renseignements personnalisés ou des données anonymisées ou agrégées tirées de renseignements personnalisés, et fournir des explications précises sur les programmes aux fins desquels les renseignements sont recueillis et utilisés.

32. Enfin, **je recommande** au comité d'inscrire dans le cadre de son étude le projet de réviser la *Loi sur la protection des renseignements personnels*, déjà envisagé en 2016 à l'occasion de

son examen de la *Loi sur la protection des renseignements personnels*[23].

Échecs en matière de consentement et de transparence

33. Les données agrégées et anonymisées qui sont l'objet d'étude du comité viennent d'entreprises privées qui les recueillent directement ou indirectement auprès de leurs clients. Il est généralement difficile pour les intéressés de comprendre comment ces renseignements sont recueillis à leur sujet, comment ils sont utilisés par l'entreprise qui les recueille ou comment ces entreprises partagent leurs renseignements avec des tiers. Les clients peuvent lire les politiques de confidentialité, mais ces documents sont, comme on le sait, très difficiles à comprendre et à évaluer. Le Citizen Lab a réalisé de nombreux projets dans le cadre desquels nous avons fait enquête sur des politiques de confidentialité et les avons analysées, et nous nous sommes régulièrement retrouvés devant la question de savoir si des renseignements sont effectivement recueillis, utilisés ou divulgués lorsque des entreprises emploient des termes au conditionnel lorsqu'ils décrivent ce genre d'activités[24]. Il est rare que des entreprises révèlent l'identité des tiers avec lesquels elles partagent des informations.

34. La façon dont les entreprises gèrent les informations qu'elles ont en leur possession est souvent controversée. Ces entreprises expliquent que leur gouvernance suppose la publication de « rapports sur les mesures de transparence ». Cela a tout d'abord servi à révéler le nombre de fois que des organismes d'application de la loi ou du renseignement ont demandé des informations à ces entreprises, à préciser les autorisations légales justifiant ces demandes, à indiquer le volume d'informations fournies, et à donner le nombre d'abonnés au sujet desquels des informations ont été divulguées. Depuis, ces statistiques ont été complétées par de l'information sur les retraits de droits d'auteur, et les entreprises sont de plus en plus invitées à fournir également de l'information sur le traitement qu'elles réservent aux discours haineux[25].

35. Les rapports sur les mesures de transparence pourraient également servir à préciser, sous forme statistique et narrative, à quelle fréquence des renseignements personnels — sous forme identifiable ou non — sont communiqués à des tiers à des fins commerciales ou non. Il s'agirait d'expliquer clairement aux utilisateurs de services, et à la population en général, comment fonctionne l'économie des données et la mesure dans laquelle des renseignements

---

[23] Voir : Protéger la vie privée des Canadiens : examen de la Loi sur la protection des renseignements personnels (ourcommons.ca).
[24] Voir, p. ex. : https://citizenlab.ca/wp-content/uploads/2018/02/approaching_access.pdf; https://citizenlab.ca/2020/05/we-chat-they-watch/.
[25] Pour plus de détails, voir : https://www.newamerica.org/oti/reports/transparency-report-tracking-tool/.

personnels sont communiqués à des tiers. Je précise que cela ne corrigerait pas complètement les asymétries d'information entre les utilisateurs et les entreprises privées qui recueillent leurs renseignements personnels ou les communiquent à d'autres parties, mais les Canadiens sauraient un peu mieux et plus précisément comment leurs données sont utilisées.

36. **Je recommande** donc au comité de proposer une révision de la LPRPDE qui comprendrait des dispositions imposant aux entreprises privées d'obtenir le consentement éclairé de leurs clients avant de communiquer des renseignements identifiables, anonymisés ou agrégés à des tiers.

37. **Je recommande** au comité de proposer une révision de la LPRPDE qui comprendrait des dispositions imposant aux entreprises privées de préciser si elles ou leurs partenaires recueillent des informations, au lieu d'indiquer simplement qu'elles « pourraient » le faire ou que ce serait une « possibilité », et d'indiquer clairement les autres parties auxquelles elles communiquent des informations, ainsi que l'usage que ces autres parties entendent en faire.

38. **Je recommande** également au comité de proposer une révision de la LPRPDE qui comprendrait des dispositions imposant aux entreprises privées de fournir des rapports sur les mesures de transparence. Ces rapports devraient s'inspirer des modèles facultatifs fournis par ISDE[26] et comprendre plus exhaustivement de l'information sur les retraits de droits d'auteur, le traitement des discours haineux et les modes de transmission de données personnalisées ou anonymes à des tiers.

Renseignements organisationnels

39. Les opinions exprimées ici sont miennes et s'appuient sur des travaux de recherche que mes collègues et moi-même avons effectués sur mon lieu de travail, le Citizen Lab. Le Citizen Lab est un laboratoire interdisciplinaire de la Munk School of Global Affairs and Public Policy, à l'Université de Toronto, qui se concentre sur la recherche, le développement et les politiques stratégiques de haut niveau, ainsi que l'engagement juridique au croisement des technologies de l'information et des communications, des droits de la personne et de la sécurité mondiale.

40. Nous avons recours à des « méthodes mixtes », dans nos travaux de recherche, en conjuguant des pratiques issues des sciences politiques, du droit, de l'informatique et d'études sectorielles. Nos travaux consistent notamment : à faire enquête sur l'espionnage

[26] Voir : Lignes directrices concernant la production de rapports sur les mesures de transparence - Gestion du spectre et télécommunications.

numérique exercé contre la société civile; à documenter les technologies et pratiques de filtrage d'Internet et autres qui ont une incidence sur la liberté d'expression en ligne; à analyser les mécanismes de protection de la vie privée, de sécurité et de contrôle dans les applications populaires; et à examiner les mécanismes de transparence et de responsabilisation en jeu dans les relations entre les entreprises privées et les organismes d'État concernant les renseignements personnels et d'autres activités de surveillance.