CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

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

ETHI • NUMÉRO 133 • 1re SESSION • 42e LÉGISLATURE

TÉMOIGNAGES

Le jeudi 31 janvier 2019

Président

M. Bob Zimmer

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

Le jeudi 31 janvier 2019

● (1530)

[*Traduction*]

Le président (M. Bob Zimmer (Prince George—Peace River—Northern Rockies, PCC)): Bienvenue, tout le monde.

Selon l'avis de convocation, il s'agit de la 133e réunion du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique. L'étude porte sur la protection des données personnelles dans les services gouvernementaux numériques.

Aujourd'hui, nous accueillons une personne qui a comparu à plusieurs reprises dans le passé, Daniel Therrien, commissaire à la protection de la vie privée du Canada. Nous recevons également Gregory Smolynec, sous-commissaire, Secteur des politiques et de la promotion, et Lara Ives, directrice exécutive, Direction des politiques, de la recherche et des affaires parlementaires.

Avant de céder la parole à M. Therrien, je veux laisser M. Kent intervenir rapidement.

L'hon. Peter Kent (Thornhill, PCC): Merci, monsieur le président.

Chers collègues, j'espère que j'obtiendrai le consentement unanime à ce sujet. À la lumière de la récente annonce de la ministre des Institutions démocratiques selon laquelle un nouveau groupe de travail sera mis sur pied pour surveiller la publicité, les messages et les renseignements divulgués au cours des prochaines élections, je suggère de prévoir au moins une réunion pour convoquer des représentants de quelques-unes des sept organisations qui assureront une surveillance pour veiller à ce que les reportages et les publicités soient acceptables.

Le président: Monsieur Angus.

M. Charlie Angus (Timmins—Baie James, NPD): Si je comprends bien, je pense que ce serait avantageux pour nous. Comme avec les recommandations unanimes des parties pour protéger le système électoral, notre comité a formulé des recommandations. Je pense qu'il vaudrait la peine de faire valoir notre point de vue à ce sujet.

Je pense que c'est probablement plus adapté à un plan qui porte sur la cybersécurité et les cybermenaces, étant donné que les menaces visant les élections sont beaucoup plus subtiles. Les manipulations peuvent être plus difficiles à repérer.

Il serait bien de savoir si ces représentants ont examiné nos travaux et de les interroger. Je serais très favorable à ce que l'on procède ainsi.

Le président: Monsieur Saini.

M. Raj Saini (Kitchener-Centre, Lib.): Je n'y vois pas d'inconvénient, mais je préférerais une motion officielle pour que je puisse savoir exactement ce que vous voulez et quelles sont les organisations.

L'hon. Peter Kent: D'accord.

M. Raj Saini: Nous l'envisagerons.

L'hon. Peter Kent: Ce n'est pas nécessaire. J'en fais la proposition. Passons au vote. Si vous jugez bon de rejeter la motion, alors nous procéderons à un vote en bonne et due forme.

M. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Pouvez-vous répéter le libellé exact?

L'hon. Peter Kent: À la lumière de l'annonce faite par la ministre hier selon laquelle un nouveau groupe de travail composé de représentants soit créé...

Le président: C'est le groupe de travail sur la sécurité, je crois.

L'hon. Peter Kent: ... le groupe de travail sur la sécurité, qui comprend le Conseil privé, le SCRS —, les sept organisations qui ont été nommées... Nous les inviterions à expliquer comment elles perçoivent leur nouvelle fonction, et nous pourrions leur accorder quelques semaines pour y réfléchir. Je suppose qu'elles ont été mises au courant avant que la ministre en fasse l'annonce hier, mais on les inviterait à discuter de leur mission et de la façon dont ils la réaliseront.

La ministre n'a pas été en mesure de dire hier quand les Canadiens seront prévenus de violations éventuelles ou quel est l'objectif du groupe de travail, mais je pense que ce serait utile, plus particulièrement compte tenu des travaux que nous avons menés dans ce dossier au cours de la dernière année.

Le président: Raj est le prochain intervenant, et ensuite Charlie?

M. Charlie Angus: J'ai un libellé pour une motion.

Le président: D'accord. On vous écoute, monsieur Angus.

M. Charlie Angus: « Que le Comité invite le groupe de travail sur la sécurité composé de sept organisations » — nous pourrions les nommer — « pour expliquer au Comité son rôle afin de protéger l'intégrité du système électoral canadien pour les élections de 2019 ».

Le président: Par souci de clarté, fournissez-vous le libellé pour M. Kent?

M. Charlie Angus: Oui. Il expliquait ce qu'il voulait, mais je pense que nous voulons seulement que le groupe de travail sur la sécurité nous décrive son rôle et son plan pour protéger l'intégrité du système électoral du Canada.

L'hon. Peter Kent: Monsieur le président, je peux maintenant vous donner la liste car l'application a téléchargé. C'est le greffier du Bureau du Conseil privé, la conseillère à la sécurité nationale et au renseignement, la sous-ministre de la Justice, le sous-ministre de la Sécurité publique et le sous-ministre d'Affaires mondiales Canada. C'est un groupe de personnes estimées.

Le président: Madame Fortier.

● (1535)

Mme Mona Fortier (Ottawa—Vanier, Lib.): J'aimerais qu'on ajourne le débat sur la motion et qu'on laisse le commissaire faire sa déclaration.

Le président: Nous allons d'abord entendre le témoignage de M. Therrien, puis nous reviendrons à la motion plus tard. Est-ce que cela vous va?

L'hon. Peter Kent: Les libéraux veulent demander conseil.

Le président: Est-ce juste, monsieur Angus?

M. Charlie Angus: Je veux seulement clarifier les règles. Je ne crois pas que demander l'ajournement du débat clarifie quoi que ce soit. Je suppose que Peter sera d'accord pour reporter le débat.

Le président: Nous allons passer au vote.

M. Nathaniel Erskine-Smith: Supposons que nous allons revenir à la question...

Le président: Nous nous prononçons sur l'ajournement du débat.

(La motion est adoptée.)

Le président: J'imagine que nous...

L'hon. Peter Kent: Tant que nous passons au vote d'ici la fin de la réunion...

Le président: D'accord. Entendu.

Monsieur Therrien, on vous écoute.

[*Français*]

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

Messieurs les membres du Comité, je vous remercie de m'avoir invité à vous donner mon point de vue dans le cadre de votre étude sur les répercussions sur la protection de la vie privée et les obstacles juridiques éventuels liés à la mise en œuvre de services gouvernementaux numériques au Canada.

La Feuille de route de la Stratégie de données pour la fonction publique fédérale, qui a été publiée en novembre 2018 et qui nous a été communiquée à la fin de l'année dernière, constitue un bon point de départ pour cette étude, puisqu'elle définit l'approche du gouvernement.

Dans ce document, le gouvernement indique ce qui suit:

> Les données ont le pouvoir de permettre au gouvernement de prendre de meilleures décisions, de concevoir de meilleurs programmes et d'offrir des services plus efficaces. Mais pour que cela se produise [...] nous devons renouveler notre approche.
>
> Aujourd'hui, chaque ministère et organisme produit et détient un vaste éventail de données diversifiées et en constante expansion [...] Ces données sont souvent recueillies d'une manière, fondée sur des pratiques et des principes informels, qui rend difficile leur communication à d'autres ministères ou aux Canadiens. Leur utilisation est inégale dans l'ensemble du gouvernement et leur valeur est sous-optimisée dans le processus décisionnel et dans les opérations quotidiennes.

Nous appuyons, bien sûr, l'utilisation de la technologie pour améliorer la prise de décision du gouvernement et la prestation des services, mais, comme il est indiqué dans votre mandat, cela doit être effectué tout en protégeant la vie privée des Canadiens. À cet égard, il est important de se rappeler que la protection de la vie privée est un droit fondamental de la personne qui est également une condition préalable à l'exercice d'autres droits fondamentaux, comme la liberté, l'égalité et la démocratie.

La Feuille de route du gouvernement souligne la difficulté de communiquer les données dans tous les ministères et attribue cette situation aux pratiques et principes informels ou, parfois, à des obstacles juridiques. Je comprends qu'il existe en fait, au sein du gouvernement, un exercice servant à cerner ces obstacles juridiques en vue d'éliminer ceux qui seraient jugés incompatibles avec la nouvelle approche qui, selon le gouvernement, est nécessaire pour tirer parti des données.

Je dirais que ce qui est un obstacle juridique pour certains peut être considéré par d'autres comme une garantie de protection de la vie privée. La terminologie que le gouvernement ou d'autres intervenants utilisent dans ce débat n'est pas neutre. Plusieurs des obstacles présumés se trouvent aux articles 4 à 8 de la Loi sur la protection des renseignements personnels actuelle. Ces règles devraient-elles être réexaminées en vue d'améliorer les services gouvernementaux à l'ère du numérique? Certainement. Certaines de ces règles devraient-elles être modifiées? Probablement.

Cependant, je vous demanderais de vous rappeler lors de votre étude que, bien que des rajustements puissent être souhaitables, toute nouvelle mesure législative conçue pour faciliter les services gouvernementaux numériques doit respecter la vie privée en tant que droit de la personne. Je pourrai préciser ce point au cours de la période des questions, si vous le voulez. Autrement dit, les modalités peuvent changer, mais la fondation doit être solide et respecter le droit à la vie privée. Cette fondation doit reposer sur une loi renforcée sur la protection des renseignements personnels. Comme vous le savez, nous avons fait des recommandations en ce sens en 2016. J'ajouterais ici une nouvelle recommandation, soit celle d'adopter, dans le secteur public, le concept de protection de la vie privée dès la conception.

● (1540)

[*Traduction*]

J'ai examiné avec intérêt le témoignage qui vous a été présenté par des représentants de l'Estonie au lancement de votre étude. On parle souvent du modèle estonien en raison de son architecture technologique, mais j'ai remarqué que les représentants ont plutôt mis l'accent sur l'importance des facteurs liés à l'attitude, y compris le besoin de surmonter les cloisonnements administratifs de l'État afin de réutiliser des renseignements personnels à des fins autres que celles pour lesquelles ils ont été recueillis.

Cela pourrait être considéré comme une validation de l'opinion selon laquelle notre Loi sur la protection des renseignements personnels doit être réexaminée et les « obstacles juridiques » doivent être éliminés. J'aimerais toutefois souligner qu'en Estonie, l'élimination des cloisonnements n'a pas entraîné une gestion horizontale tout azimut des données personnelles à l'échelle du gouvernement. Dans le modèle estonien, la réutilisation — ou la communication des renseignements personnels — semble plutôt fondée sur des lois généralement conformes aux principes de vie privée reconnus à l'échelle mondiale et au Règlement général sur la protection des données. Je vous encourage toutefois à faire un suivi sur les conditions juridiques qui sont en place en Estonie concernant la réutilisation.

En ce qui concerne les aspects technologiques du modèle estonien, nous comprenons qu'il n'existe pas de base de données centralisée. L'accès est plutôt accordé grâce à la capacité de relier des serveurs individuels au moyen de voies d'accès cryptées avec accès ou réutilisation autorisés à des fins légitimes déterminées. Ce système qui limite l'accès à des fins précises par les organismes gouvernementaux est susceptible de réduire le profilage.

Nous comprenons également que des mesures de protection de la vie privée et de sécurité sont prises au moyen du cryptage et de l'utilisation de la chaîne de blocs. Cela est conforme à l'une de nos recommandations de 2016 concernant la refonte de la Loi sur la protection des renseignements personnels, à savoir de créer une obligation juridique pour les institutions gouvernementales de protéger les renseignements personnels.

Je constate que l'autorité chargée de la protection des données occupe une place importante dans le modèle estonien, ce qui comprend un rôle proactif explicite, ainsi que le pouvoir de rendre des ordonnances contraignantes, de demander l'ouverture de poursuites criminelles et d'imposer des amendes lorsque des données sont traitées de façon non conforme à la loi. De même, la place qu'occupe le Commissariat à la protection de la vie privée pour ce qui est de son rôle proactif et de surveillance devrait être tout aussi importante, conformément à nos recommandations concernant la réforme de la Loi sur la protection des renseignements personnels.

J'aimerais conclure avec des questions que je veux que vous preniez en considération lorsque vous examinerez plus attentivement le modèle estonien ou discuterez de son application dans le contexte canadien.

Premièrement, nous avons entendu des représentants dire que le succès du système repose sur la confiance, laquelle requiert des protections solides. Toutefois, aucun système n'est entièrement sécuritaire. Quelles mesures d'atténuation sont en place dans le modèle estonien lorsque, et non pas si, il y a une atteinte à la sécurité?

Deuxièmement, la feuille de route de la stratégie de données du Canada suppose que la valeur d'un modèle comme celui de l'Estonie réside dans l'analyse des données détenues par l'ensemble du gouvernement. Étant donné la décentralisation des ensembles de données et le régime législatif qui limite la réutilisation à des fins précises, nous ne voyons pas bien comment cela pourrait être réalisé. Vous pourriez peut-être considérer cet enjeu.

Enfin, je suggère d'obtenir des éclaircissements de la part des fonctionnaires estoniens au sujet des conditions juridiques régissant la réutilisation des données, car c'est une mesure de protection importante pour veiller à ce qu'il n'y ait aucun profilage global et d'échange de données horizontales sans frontières, comme je l'appelle.

Merci de votre attention. Je me ferai un plaisir de répondre à vos questions.

Le président: Merci encore une fois, monsieur Therrien.

Pour les sept premières minutes, nous entendrons Nate et David.

Allez-y.

M. Nathaniel Erskine-Smith: Merci beaucoup.

Ma première question porte sur le modèle estonien et sur les voies légales.

Lorsque Michael Geist a comparu devant nous, il a dit que la mise en place de mesures technologiques semble être une excellente idée, mais que nous ne pourrions pas avoir confiance dans ces mesures et que nous devons revoir la Loi sur la protection des renseignements personnels. Je crois que vous êtes du même avis.

Pour revoir la Loi sur la protection des renseignements personnels et assurer la clarté de l'échange de renseignements, je crois savoir qu'en Estonie, ils ont un modèle « une fois suffit », mais il faut des autorisations législatives précises pour pouvoir réutiliser les renseignements. Donc, votre argument selon lequel la loi en Estonie doit être clarifiée est important.

En ce qui concerne la Loi sur la protection des renseignements personnels, vous croyez que nous devrions clarifier les voies légales pour l'échange de renseignements au Canada également.

M. Daniel Therrien: Oui. Nous avons des règles de longue date, bien entendu, pour régir les conditions en vertu desquelles les données peuvent être communiquées entre les ministères. Ce sont essentiellement les articles 4 à 8 de la Loi sur la protection des renseignements personnels de la fonction publique.

Votre mandat traite des obstacles juridiques. La feuille de route de la stratégie de données énonce les obstacles juridiques éventuels. Je présume que lorsque le gouvernement parle d'obstacles, il fait référence à l'examen pour déterminer si les articles 4 à 8 sont encore appropriés. J'en conviens, mais je dis aussi que ce sont des règles importantes, et bien que certaines modalités ou certains ajustements peuvent être envisagés, ne perdons pas de vue l'objectif principal, à savoir qu'il faut respecter la vie privée.

● (1545)

M. Nathaniel Erskine-Smith: Le gouvernement a-t-il communiqué avec vous pour discuter d'un projet d'identification numérique?

M. Daniel Therrien: Nous avons eu des discussions très générales avec le gouvernement à la fin de l'année dernière à propos de la feuille de route de la stratégie de données. Nous avons été invités récemment à présenter nos points de vue sur les stratégies que les ministères doivent ou peuvent adopter conformément à la feuille de route. Ce processus n'a pas été entamé, mais j'accueille favorablement cette invitation du gouvernement.

M. Nathaniel Erskine-Smith: En ce qui concerne l'identification numérique plus précisément, je crois savoir que des conversations sont en cours au fédéral pour réaliser un projet conjointement avec les provinces. Vous a-t-on consulté à ce sujet?

M. Daniel Therrien: Ces discussions sont en cours depuis un certain nombre d'années. Mme Ives a peut-être quelque chose à ajouter à ce sujet.

Mme Lara Ives (directrice exécutive, Direction des politiques, de la recherche et des affaires parlementaires, Commissariat à la protection de la vie privée du Canada): Oui. J'ajouterais qu'il y a eu diverses versions au fil des ans. Je pense que la plus récente était en 2012. Nous avons passé en revue les évaluations des facteurs relatifs à la vie privée plutôt qu'un projet d'identification numérique: des moyens d'accès aux services gouvernementaux en ligne. L'une d'elles est publiée par le gouvernement du Canada et l'autre utilise les justificatifs bancaires, mais cela ne coïncide pas tout à fait avec l'identification numérique.

M. Nathaniel Erskine-Smith: J'ai une dernière question, puis je vais céder la parole à David.

Y a-t-il des exemples qui démontrent que le gouvernement actuel ou les gouvernements précédents ont mis en ligne des services pour offrir de meilleurs services numériques en s'adressant directement à vous et en vous disant, « Réglons les problèmes liés à la protection des renseignements personnels »? Avons-nous un exemple canadien d'un service qui a fait tout ce qu'il fallait? Prenez votre temps.

Des voix: Oh, oh!

M. Daniel Therrien: Dans un esprit d'optimisme et de positivisme, je dirais qu'il est intéressant d'examiner le modèle estonien de ce point de vue. Il renferme de nombreux aspects positifs. Ce sont les détails qui posent problème, de toute évidence, mais le modèle n'est pas si mal.

M. Nathaniel Erskine-Smith: Très bien. Merci beaucoup.

David.

M. David de Burgh Graham (Laurentides—Labelle, Lib.): Merci.

Je pense qu'il est plus facile de partager des données que du temps, mais nous allons faire ce que nous pouvons.

[*Français*]

J'aimerais comprendre comment on peut définir les paramètres de l'autorisation donnée par une personne. Mardi, j'ai donné comme exemple les lecteurs automatiques de plaques d'immatriculation des véhicules. Lorsqu'une auto passe, le lecteur enregistre le numéro de la plaque. C'est le gouvernement qui fait cela. Ce sont des données que nous fournissons sans que ce soit vraiment volontaire, étant donné que nous n'avons pas d'autre choix que de les fournir.

Si, partout au pays, les ministères ou les services de police utilisent ces données sans vraiment avoir obtenu l'autorisation des gens pour le faire, comment peut-on déterminer si ceux-ci ont donné leur consentement? Où tire-t-on la ligne?

M. Daniel Therrien: Je vais considérer que votre question repose sur le principe voulant qu'il s'agisse d'informations du domaine public. Les plaques d'immatriculation sont publiques, dans un sens, puisque les voitures circulent sur les voies publiques. Des gens — le gouvernement, mais aussi des compagnies — se prévalent de la nature publique de l'environnement pour recueillir des données et les utiliser ensuite de façon à ce qu'elles ne soient pas considérées comme des renseignements personnels. Dans ce cas, les règles concernant l'utilisation et la divulgation de ces renseignements sont plus permissives.

M. David de Burgh Graham: À chaque étape du déplacement, on peut lire le numéro de la plaque et savoir à quel individu elle appartient, quelle est son adresse et quel est son historique. Même si on ne recueille pas chaque fois ces données, on peut suivre l'individu d'un bout à l'autre du pays et savoir quels sont ses déplacements.

Ce n'est pas le but des plaques d'immatriculation, mais, en déterminant que c'est du domaine public, a-t-on l'autorisation d'utiliser les données de cette façon? Les États-Unis le font déjà.

● (1550)

M. Daniel Therrien: Il faut être prudent avant de considérer des renseignements comme étant publics. En effet, comme vous venez de le dire, il est quand même possible d'identifier l'individu qui est associé au véhicule, son comportement, et ainsi de suite. Donc, même si les renseignements sont soi-disant publics, il faut se demander si ce sont néanmoins des renseignements personnels et quelle est l'autorité du ministère en question pour colliger les renseignements. Cela se fait ministère par ministère. Même si ces renseignements sont du domaine public, le fait de les recueillir doit être lié à un mandat du ministère en question. C'est une condition très importante prévue dans la loi actuelle. Elle pourrait être renforcée, selon certaines recommandations que nous avons faites en vue de modifier la LPRP.

Bref, il faut être prudent à l'égard des données qui sont du domaine public. En outre, il est important de s'assurer que chaque ministère qui collige et utilise de tels renseignements a bel et bien un mandat pour le faire.

M. David de Burgh Graham: Merci.

[*Traduction*]

Me reste-t-il du temps?

Le président: Vous n'avez plus de temps.

[*Français*]

M. David de Burgh Graham: Merci.

[*Traduction*]

Le président: Nous allons maintenant entendre M. Kent pour les sept prochaines minutes.

L'hon. Peter Kent: Merci, monsieur le président.

Je suis ravi de vous revoir, monsieur le commissaire, ainsi que vos partenaires qui sont ici aujourd'hui.

En raison des importantes différences entre le modèle estonien et le Canada à l'heure actuelle... L'identité numérique en Estonie couvre littéralement la vie entière des gens, pas seulement les données relatives à leur santé et leurs renseignements fiscaux, mais aussi leur éducation... Elle couvre pratiquement tous les aspects de leur vie quotidienne.

J'ai lu votre déclaration, et vous semblez considérer la première étape d'un gouvernement numérique, si on en vient à cela au Canada, comme étant le début au niveau fédéral. Est-il pratique d'essayer de se lancer dans des secteurs où il y a un écart marqué et aucun chevauchement entre les administrations provinciales et municipales?

M. Daniel Therrien: Bien entendu, une très grande différence entre l'Estonie et le Canada est que c'est un État unitaire tandis que nous sommes un État fédéral. Cela crée diverses difficultés au Canada pour mettre sur pied un système. Ce sont des problèmes d'ordre technologique, mais les administrations et les lois sont différentes aussi. À mon avis, il n'est pas inconcevable d'avoir un système qui communiquerait les renseignements entre les gouvernements fédéral et provinciaux, mais en raison de la complexité de l'État fédéral canadien, il est probablement plus pratique de commencer à un niveau.

L'hon. Peter Kent: Avez-vous lu la transcription des témoignages de M. Cavoukian et de M. Geist, qui ont comparu devant le Comité cette semaine?

M. Daniel Therrien: Oui.

L'hon. Peter Kent: Pourriez-vous nous faire part de vos observations générales? M. Cavoukian avait des préoccupations très importantes.

M. Daniel Therrien: Je vais vous les présenter à ma façon.

Je pense que le modèle estonien est intéressant, car le risque des services gouvernementaux numérisés basés sur un identificateur numérique commun serait que le gouvernement, que ce soit le gouvernement fédéral ou les gouvernements en général, aurait un seul profil par personne. Il est alors très difficile d'assurer la protection des renseignements personnels.

L'un des avantages évidents du modèle estonien est que les données ne sont pas centralisées. Elles sont encore entre les mains d'un grand nombre d'institutions, et il y a une voie technologique avec des autorités judiciaires pertinentes qui autorisent que les renseignements soient réutilisés d'un ministère à un autre. La décentralisation du modèle estonien, à première vue, semble être un aspect positif qui réduit ce qui serait un risque autrement.

Vous avez mentionné des préoccupations qui ont été exprimées.

L'hon. Peter Kent: Oui.

M. Daniel Therrien: Pouvez-vous être plus précis?

L'hon. Peter Kent: Je n'ai pas la transcription devant moi, mais essentiellement, après avoir lu bon nombre des remarques formulées par M. Cavoukian, la cybersécurité est vulnérable lorsque des renseignements numériques sont transférés de dépôts de données à une entité qui demande d'y avoir accès. Les garanties de sécurité absolue n'existent pas encore.

● (1555)

M. Daniel Therrien: Il ne fait aucun doute que les systèmes technologiques sont vulnérables aux atteintes à la sécurité. Je ne suis pas certain s'il existera un jour un système exempt de ce risque. D'un point de vue juridique, je pense que s'il y a des services numériques, il est important qu'il y ait une obligation légale du gouvernement d'appliquer de robustes mesures de protection technologiques. Sur le plan technologique, en Estonie, comme vous le savez, il y a des chaînes de blocs et du cryptage. Ce sont des systèmes de pointe. Garantissent-ils qu'il n'y aura aucune atteinte à la sécurité? Non.

L'hon. Peter Kent: Dans votre exposé, vous avez parlé de confiance et de consentement. Encore une fois, l'une des principales différences entre l'Estonie et le Canada, c'est que l'Estonie a une population très docile depuis l'effondrement de l'Union soviétique et une nouvelle démocratie très énergique au sein de laquelle on est déterminé à créer un gouvernement numérique à partir de zéro.

Lorsqu'on tient compte du scepticisme naturel des Canadiens et du cynisme générationnel à l'égard de l'environnement numérique, ainsi que de Cambridge Analytica, de Facebook, d'Aggregate IQ, de tous les scandales et maintenant de la controverse liée à Sidewalk Labs et des préoccupations des gens liées à l'exposition, à la vie privée, au contenu personnel, à la question de savoir qui possède quelles données et comment elles sont accessibles, pensez-vous qu'étant donné tous ces facteurs, il sera difficile d'obtenir le consentement des Canadiens pour ce type de gouvernement numérique dans un délai raisonnable? Je parle peut-être d'une décennie — de notre vivant.

M. Daniel Therrien: Je crois que les hauts fonctionnaires estoniens ont mentionné que même en Estonie, les systèmes n'ont pas été mis en oeuvre du jour au lendemain. Il faut suivre plusieurs étapes.

Je crois qu'il est essentiel d'avoir des mesures de protection sur le plan technologique. Les mesures de protection sur le plan juridique sont également essentielles. Je dirais probablement qu'une mise en oeuvre graduelle, dans laquelle le gouvernement a l'occasion de démontrer que le système mérite qu'on lui fasse confiance, pourrait rassurer davantage la population. Il ne fait aucun doute qu'actuellement, les Canadiens craignent que leur vie privée ne soit pas respectée.

L'hon. Peter Kent: Merci.

Le président: Merci, monsieur Kent.

La parole est maintenant à M. Angus. Il a sept minutes.

M. Charlie Angus: Merci, monsieur le président.

Monsieur Therrien, nous sommes toujours heureux de vous accueillir au Comité.

J'aimerais revenir sur votre dernière déclaration au sujet de la confiance et sur la question de savoir si on devrait s'attendre à ce que les Canadiens fassent confiance à un tel système.

Au fil des ans, dans le cadre de mes travaux liés à ce dossier, j'ai observé que nous avions des fuites de données chaque année. Certaines d'entre elles sont des fuites de données extrêmement importantes, par exemple les renseignements liés aux prêts contractés par un quart de million d'étudiants ou plus, et récemment, les renseignements personnels de 80 000 personnes ont été compromis par l'entremise de l'ARC.

Vos travaux laissent-ils croire que le nombre de fuites change à mesure que la technologie évolue? Est-ce une norme...? D'une année à l'autre, observons-nous certaines fuites assez importantes, mais également des fuites plus petites? Observez-vous un grand changement au sein des ministères?

M. Daniel Therrien: Je ne dirais pas que nous voyons de grandes améliorations à cet égard. Il ne fait aucun doute qu'inspirer cette confiance représente un énorme défi.

J'aimerais utiliser un exemple qui est représentatif sur de nombreux plans, selon moi. Comme vous le savez, le gouvernement a mis en oeuvre un système de paie appelé Phénix qui a fait l'objet de critiques à plusieurs niveaux. Au Commissariat à la protection de la vie privée du Canada, nous avons mené une enquête sur les mesures de sécurité et de protection de la vie privée qui avaient été mises en oeuvre, ou qui ne l'avaient pas été, dans le système Phénix. L'une des conclusions très préoccupantes auxquelles nous sommes parvenus au cours de notre enquête, c'est que des hauts fonctionnaires du gouvernement ont délibérément décidé de ne pas surveiller étroitement l'accès aux renseignements personnels dans le système, car cela aurait été coûteux, cela aurait entraîné des retards dans le système, etc.

Pour répondre directement à votre question, je ne vois pas beaucoup d'amélioration. Je dirais qu'il est essentiel, avant de mettre en oeuvre ces systèmes à plus grande échelle — pour revenir aux attitudes —, que les hauts fonctionnaires du gouvernement adoptent une attitude qui consiste à veiller à ce que des mesures de sécurité soient déployées avant la mise en oeuvre des systèmes.

● (1600)

M. Charlie Angus: Je vous remercie beaucoup de cette réponse, car elle m'amène à ma préoccupation.

Je suis ici depuis 15 ans. Je vois mes collègues de l'autre côté et ils rayonnent de l'espoir des nouveaux croyants qui pensent que nous avons finalement atteint le salut et que le gouvernement fonctionnera. Mais moi, au fil des ans, je suis devenu sceptique et agnostique.

Des députés: Oh, oh!

M. Charlie Angus: Lorsqu'il s'agit des activités du gouvernement, je suis comme saint Thomas. J'ai fait partie d'un comité après l'autre où nous étions certains que les plus gros joueurs étaient les meilleurs, que le gouvernement avait toujours... Chaque fois qu'on cherchait à attribuer des contrats, on tenait à choisir les plus gros fournisseurs possible. Mais les plus gros n'étaient pas les meilleurs. Les plus gros étaient beaucoup plus dispendieux. Mais les contrats, ainsi que les sous-ministres, favorisaient toujours les plus gros... et qui avait obtenu les contrats et qui ne les avait pas obtenus.

Ensuite, nous avons eu Phénix. Je présume que je demanderais aux citoyens de ma circonscription s'ils font confiance à Phénix. Ne croyez-vous pas qu'il faudrait mettre en oeuvre un ensemble extrêmement complexe de mesures de sécurité pour pouvoir rassurer les Canadiens sur le fait que tous leurs renseignements financiers, tous leurs renseignements personnels et tous les renseignements les concernant sont en sécurité, même s'ils se retrouvent dans un ministère ou un gouvernement qui subit, tous les ans, des fuites graves dans presque tous les grands ministères?

M. Daniel Therrien: C'est complexe, mais je dirais que c'est humainement faisable. Cela indique probablement qu'il est nécessaire de mettre en oeuvre ce système de façon graduelle, car les systèmes ne peuvent pas être modifiés du jour au lendemain, et il faut donc y aller graduellement, selon moi. Manifestement, je commencerais par... On n'a pas le choix, il faut numériser les services gouvernementaux pour toutes sortes de raisons, notamment pour améliorer les services à la population. On ne peut pas refuser de le faire parce que c'est une tâche colossale ou trop complexe, mais lorsqu'on mettra cette politique en oeuvre, on ne devrait pas négliger les mesures de sécurité sur le plan politique, juridique et technologique.

M. Charlie Angus: Merci.

Les gens auxquels je parle préféreraient certainement que des personnes répondent au téléphone lorsqu'ils ont des questions plutôt que d'obtenir leurs données numériques plus rapidement. Mais des solutions numériques seront toujours adoptées plutôt que des solutions qui favoriseraient l'embauche de gens pour répondre au téléphone.

J'aimerais savoir s'il s'agit d'un processus unidirectionnel ou bidirectionnel. Si je veux trouver mes renseignements personnels liés à l'ARC et que j'ai une carte numérique, je peux les trouver. L'un de mes collègues libéraux a laissé entendre que ce serait une excellente façon pour le gouvernement de communiquer avec les citoyens.

Pour moi, c'est très inquiétant. Si je suis obligé de tout faire en ligne et si je dois fournir tous mes renseignements en ligne, je crois qu'il est nécessaire de préciser que c'est dans le but de me fournir les services que je souhaite obtenir, mais pas nécessairement pour que le gouvernement soit en mesure de communiquer avec moi.

Comprenez-vous que si nous avons une communication bidirectionnelle, cela change la nature du processus, car le risque que les droits relatifs à la protection de la vie privée des citoyens soient bafoués augmente considérablement?

M. Daniel Therrien: La situation que vous décrivez est exactement la raison pour laquelle je soutiens qu'il est essentiel d'examiner très attentivement le cadre juridique dans lequel des données seront échangées d'un ministère à l'autre ou dans lequel un ministère sera en mesure de réutiliser des données recueillies par un autre ministère, comme c'est le cas en Estonie.

Cela commence avec un cadre juridique approprié qui limite les circonstances dans lesquelles un ministère peut communiquer avec un citoyen parce qu'un autre ministère lui a offert un service. C'est extrêmement important. Nous avons déjà des règlements à cet égard dans les articles 4 à 8 de la Loi sur la protection des renseignements personnels. Oui, ces articles peuvent faire l'objet d'un examen, mais c'est aussi un bon endroit pour commencer. C'est une partie importante du fondement. Ensuite, je crois que la technologie suit les principes qui ont été adoptés avec les mesures de sécurité nécessaires pour veiller à ce que, sur le plan technologique, les banques de données ne puissent pas communiquer entre elles, à moins qu'une loi les autorise à le faire.

Cela commence avec un cadre bien défini et bien conçu. On peut appeler cela un échange ou la réutilisation de renseignements.

● (1605)

M. Charlie Angus: Merci beaucoup.

Le président: Merci, monsieur Angus.

Nous entendrons maintenant M. Saini. Il a sept minutes.

M. Raj Saini: Bonjour, monsieur Therrien. Nous sommes toujours heureux de vous accueillir. Je crois que vous êtes le témoin qui comparaît le plus souvent devant notre comité, et c'est très bien.

Le 23 novembre, vous avez présenté un mémoire à ISDE. Je l'ai lu. C'était très intéressant. Vous avez notamment écrit ceci: « Il n'est pas exagéré d'affirmer que la numérisation de tant d'aspects de nos vies est en train de redéfinir l'humanité. » J'irais encore plus loin en disant qu'une fois que cette marche vers la technologie est amorcée, il est très difficile de l'arrêter. Elle finira par réussir.

Je sais que nous utilisons le modèle de l'Estonie, mais si vous examinez la situation actuelle de ce pays, vous constaterez qu'il y a 1,3 million d'habitants sur 4 millions d'hectares, dont la moitié est recouverte de forêts. Il s'ensuit que la connectivité à large bande ne cause pas vraiment de grandes difficultés là-bas. Lorsque nous examinons la situation actuelle du Canada et la plus récente enquête des Nations unies sur les pays dominants dans la mise en oeuvre du gouvernement électronique, nous constatons que le Canada se trouve au 23^{e} rang et que le reste du monde finira par s'engager dans cette voie.

Dans les notes que j'ai lues, vous indiquez que la protection de la vie privée vous préoccupe beaucoup. Nous devons établir un point de départ et un objectif. La majorité des pays, surtout les pays avancés, numérisent de plus en plus leur gouvernement. Laissons de côté l'exemple de l'Estonie pour l'instant. Où commençons-nous?

J'aborderai la question sous deux angles différents. Tout d'abord, l'Estonie a deux paliers de gouvernement. Dans certains cas, nous avons quatre paliers de gouvernement. Comment protégeons-nous la vie privée? Comme M. Angus l'a dit, les gens veulent que leurs données soient protégées, mais différents paliers de gouvernement jouent différents rôles. Les données ne sont pas toutes confiées à un seul palier de gouvernement. Par exemple, le gouvernement provincial s'occupe de la santé. Le gouvernement fédéral s'occupe de l'ARC. Comment protégeons-nous les renseignements personnels des Canadiens d'un palier de gouvernement à un autre? Comment favorisons-nous l'interopérabilité du système entre les différents ministères d'un même palier de gouvernement?

M. Daniel Therrien: Je crois qu'il serait bon de commencer par définir les circonstances précises dans lesquelles le gouvernement croit qu'il ne peut pas fournir des services efficaces en raison de ce qu'on appelle souvent le cloisonnement entre les ministères, ce qui nuit à l'échange de renseignements. Quels sont les problèmes d'ordre pratique? À part un gouvernement plus efficace, que souhaitent obtenir les citoyens? Quels types de services ne peuvent pas être fournis de façon efficace et rapide en raison d'obstacles juridiques et bureaucratiques? Je crois que ce serait un bon début.

M. Raj Saini: De plus, selon l'hypothèse utilisée en Estonie, la population ou les citoyens sont propriétaires des données. Il leur revient de déterminer comment ces données sont distribuées et qui a le droit de les consulter.

Si nous allons à l'étape suivante, si nous commençons par le secteur public — manifestement, le secteur privé participera dans une certaine mesure, qu'il s'agisse de renseignements bancaires ou d'autres types de renseignements. Si le secteur privé a un type de technologie et que le secteur public a un autre type de technologie... L'un des exemples qui ont été utilisés est celui de la technologie des chaînes de blocs.

Une entité est régie par la LPRPDE et une autre entité est régie par la Loi sur la protection des renseignements personnels. Comment peut-on intégrer ces deux entités? Quel serait le point de contact où on pourrait permettre au secteur public et au secteur privé de protéger les renseignements personnels, tout en leur permettant de continuer à exercer leur compétence respective?

M. Daniel Therrien: Je ne suis pas technologue — même si, après avoir occupé ce poste pendant quelques années, j'ai maintenant acquis un peu plus de connaissances technologiques —, mais je crois que nous sommes revenus à une approche graduelle. Les systèmes seront interopérables — pas du jour au lendemain, mais graduellement. La technologie nous permettra d'y arriver. Je commencerais par déterminer ce que le gouvernement souhaite accomplir et par cerner les obstacles à la prestation de services efficaces. Ensuite, je déterminerais la technologie nécessaire pour y arriver.

● (1610)

M. Raj Saini: La numérisation du gouvernement ira manifestement de l'avant. Que les progrès soient rapides ou lents, elle ira de l'avant. Quel rôle devrait jouer le Commissariat à la protection de la vie privée et à quel moment devrait-il s'intégrer au processus, afin d'ouvrir la voie et de veiller à ce que le système n'ait pas été mis au point? Ensuite, votre Commissariat pourrait intervenir et indiquer les choses qui posent problème.

À votre avis, à quel moment votre Commissariat devrait-il intervenir? Vous parlez de technologie. Vous parlez de protection de la vie privée. Vous parlez, dans certains cas, de transférabilité. Vous parlez de différents paliers de gouvernement. Vous parlez d'interopérabilité au sein du gouvernement. À votre avis, où votre Commissariat devrait-il s'intégrer, afin de veiller à ce que cela devienne une approche efficace?

M. Daniel Therrien: J'utiliserai le mot « proactivité », car je l'ai déjà utilisé devant votre comité lorsque j'ai parlé de la réforme de la Loi sur la protection des renseignements personnels.

Nous avons communiqué avec des hauts fonctionnaires actuellement en poste pour leur demander de conseiller les ministères pendant qu'ils élaborent leurs stratégies. Je crois que cela fait partie de ce processus. Si des lois sont modifiées, nous devrions être consultés au sujet de l'élaboration de ces lois. Une fois les lois adoptées, nous devrions obtenir les pouvoirs plus accrus que nous avons demandés, afin de veiller à ce que des principes juridiques en matière de protection de la vie privée soient mis en oeuvre. Ce sera un long processus.

Ma réponse, c'est qu'avec nos ressources limitées, nous sommes prêts et disposés à jouer un rôle aussi proactif que possible. Nous ne déterminerons pas les objectifs. Le gouvernement déterminera les objectifs, mais nous sommes disposés, dans la mesure de nos moyens, à fournir des conseils aussitôt que possible, et une fois les systèmes adoptés, nous pourrons jouer un rôle de surveillance tout en ayant les pouvoirs juridiques nécessaires pour assumer ce rôle.

M. Raj Saini: J'aimerais poser une dernière question.

Vous parlez de différents intervenants. À votre avis, serait-il préférable de commencer par réunir des intervenants du gouvernement, du secteur privé, du secteur public et du secteur de la technologie pour qu'ils déterminent la voie à suivre, afin que tout le monde soit sur la même longueur d'onde? De cette façon, le processus suivrait les étapes appropriées, mais de façon proactive et intermittente, de façon à veiller, si des changements répétitifs doivent être apportés, à ce qu'ils ne soient pas apportés à la fin du processus de développement d'un système, mais au début, lorsque ce développement suit les étapes appropriées.

M. Daniel Therrien: Je crois qu'il y a lieu d'avoir ce type de discussion générale sur les principes, qu'ils soient juridiques, bureaucratiques, opérationnels ou technologiques. Toutefois, en ce qui concerne leur mise en oeuvre, je crois que cela sera fait de façon graduelle.

M. Raj Saini: Merci.

Le président: La parole est maintenant à M. Gourde. Il a cinq minutes.

[*Français*]

M. Jacques Gourde (Lévis—Lotbinière, PCC): Merci, monsieur le président.

Monsieur Therrien, je vous remercie d'être ici.

Pensez-vous qu'il existe une étude économique sur la numérisation future des données au Canada, afin que les Canadiens aient un aperçu de la question? Cela représente-t-il des millions, des milliards?

M. Daniel Therrien: Je n'ai pas entendu le début de votre question. Me demandez-vous quel est le coût de la numérisation?

M. Jacques Gourde: Existe-t-il une étude qui établit le coût d'un environnement numérique qui soit sain dans l'avenir? On sait que le registre des armes à feu a coûté presque 2 milliards de dollars, et ce, juste pour entrer les données sur les armes d'épaule. Imaginez combien cela pourrait coûter pour faire l'entrée des données numériques pour l'ensemble du Canada.

M. Daniel Therrien: À ma connaissance, il n'y a pas de telle étude, et ce serait toute une entreprise d'en faire une.

L'une des raisons pour lesquelles je suis d'accord pour que le gouvernement numérise les services, c'est que cela permettrait d'améliorer les soins de santé, par exemple. Il peut y avoir des investissements dans la technologie, entre autres, mais il y aurait un rendement des investissements, puisque les soins de santé seraient d'une plus grande efficacité.

À ma connaissance, il n'y a pas de telle étude. Premièrement, il est difficile d'envisager l'avenir sans numérisation. Deuxièmement, même si les coûts sont importants, il y aura sûrement un rendement des investissements.

M. Jacques Gourde: Les services de nos ministères sont déjà numérisés, mais cela se fait en vase clos. Ils donnent déjà des services aux Canadiens, mais chacun de son côté.

● (1615)

M. Daniel Therrien: Oui.

M. Jacques Gourde: Il y a des choses qu'on pourrait sans doute garder. Quelle approche devrait-on avoir? On pourrait donner beaucoup plus de services aux Canadiens, mais sans jeter le bébé avec l'eau du bain ou tout recommencer à zéro.

M. Daniel Therrien: Je suis d'accord avec vous. C'est pour cela que je parle d'une approche par étapes, où les systèmes qui fonctionnent seraient maintenus. Le gouvernement devrait cerner là où cela fonctionne moins bien et faire des améliorations. Cela ne veut pas dire de tout remettre en question et de repartir à zéro, sur le plan technologique du moins.

M. Jacques Gourde: Dans un monde idéal de numérisation, quelles données confidentielles ou plus sensibles des Canadiens seraient moins bien protégées dans ce nouveau monde?

M. Daniel Therrien: Le gouvernement possède toutes sortes de renseignements extrêmement sensibles. Je viens de parler du domaine de la santé. Les renseignements médicaux font partie des renseignements très importants. L'identification peut dépendre de la biométrie; ce sont des renseignements très sensibles. Le gouvernement ne peut faire autrement que de colliger et d'utiliser des renseignements sensibles qui sont au coeur de la vie privée et de l'intimité. Le lot d'informations que le gouvernement va détenir contiendra nécessairement des renseignements sensibles, par exemple des renseignements financiers. Par conséquent, il faut que les protections soient très élevées.

M. Jacques Gourde: Merci, monsieur Therrien.

Monsieur le président, je veux juste faire une petite remarque. Quand il y a des conciliabules en arrière de la salle, c'est fatigant pour ceux qui posent des questions. Il faudrait peut-être demander à ceux qui ont besoin de discuter de sortir de la salle. S'il faut qu'il y ait de telles discussions, alors arrêtons la réunion complètement. Personnellement, cela me dérange.

[*Traduction*]

Le président: Oui. Je crois que c'est mieux maintenant. Je demanderais à tous les gens dans la salle d'aller parler dans le corridor s'ils souhaitent avoir une conversation assez forte pour que nous l'entendions à la table.

Merci.

Allez-y, monsieur Gourde.

[*Français*]

M. Jacques Gourde: J'ai terminé. Merci.

[*Traduction*]

Le président: D'accord. Merci.

La parole est maintenant à M. Baylis. Il a cinq minutes.

M. Frank Baylis (Pierrefonds—Dollard, Lib.): Je suis heureux de vous revoir, monsieur Therrien, car vous êtes très réservé et nous n'obtenons pas beaucoup de renseignements.

J'aimerais tout d'abord réfuter quelques affirmations. L'une d'entre elles, c'est que les Canadiens craignent la technologie ou la numérisation. J'aimerais invoquer la statistique selon laquelle 85 % des citoyens remplissent leur formulaire d'impôt en ligne. Ils ne sont pas obligés de le faire, car ils ont le droit de le faire sur papier. Toutefois, ils choisissent de le faire en ligne pour toutes sortes de raisons liées à l'efficacité.

Avez-vous des preuves, à part celles qui ont été fournies, que les Canadiens sont contre la technologie ou contre la numérisation?

M. Daniel Therrien: Je ne pense pas avoir dit que les Canadiens sont préoccupés par l'utilisation de la technologie.

[*Français*]

Je n'ai pas dit non plus qu'ils se méfiaient de la technologie.

Les sondages démontrent constamment que les Canadiens sont préoccupés du non-respect de leur vie privée, que ce soit par le secteur public ou le secteur privé, et du fait qu'ils n'ont pas le contrôle de leurs informations. Cela ne veut pas dire qu'ils n'utilisent pas la technologie ou qu'ils s'en méfient. C'est plutôt qu'ils croient que leur vie privée n'est pas suffisamment protégée par le secteur public et le secteur privé.

Il faut numériser les services, mais en utilisant différents moyens, qu'ils soient légaux, technologiques ou autres, pour bien assurer la sécurité des informations.

M. Frank Baylis: Vous faites une distinction assez importante.

[*Traduction*]

Même si la numérisation peut permettre une mauvaise utilisation des données, il reste que le vol d'identité et ce genre de chose existaient bien avant la venue des ordinateurs et la numérisation. Les gens ne s'opposent pas à la numérisation; ils sont simplement préoccupés par la protection de leurs renseignements personnels et ils veulent s'assurer que, si nous nous engageons dans cette voie, nous fassions tout ce que nous pouvons pour protéger leur vie privée. Est-ce ce que...?

M. Daniel Therrien: Oui, le vol d'information existait auparavant, mais il est clair qu'avec la numérisation les conséquences d'une atteinte à la protection des données sont beaucoup plus grandes.

● (1620)

M. Frank Baylis: Oui, effectivement. C'est vrai.

Mme Cavoukian, qui est une spécialiste du domaine, a témoigné lors de la dernière réunion. Elle a fait valoir que la sécurité et la vie privée ne sont pas incompatibles. Nous n'avons pas à choisir l'un ou l'autre. En fait, nous devons cesser de penser cela. Si nous faisons les choses correctement, il est possible de mieux protéger la vie privée grâce à de meilleurs moyens d'assurer la sécurité. Il faudrait cesser de dire « Eh bien, si nous améliorons la sécurité, ce sera au détriment de telle ou telle chose. »

Qu'avez-vous à dire à ce sujet?

M. Daniel Therrien: Je suis d'accord. Ce n'est pas un jeu à somme nulle en ce qui concerne la vie privée et la sécurité, ou la vie privée et l'innovation ou bien la vie privée et l'amélioration de la prestation des services. Nous pouvons faire tout cela, pourvu que les systèmes, y compris les systèmes juridiques, soient bien conçus. Cela m'amène à mentionner l'important concept qu'est la protection de la vie privée dès la conception, qui devrait exister en droit et qui devrait aussi être appliqué sur le terrain par la bureaucratie, les ministères, dans le cadre de la prestation des services.

M. Frank Baylis: D'une certaine façon, nous sommes dans une situation où on a fait des comparaisons avec le Far West, par exemple. Lorsqu'il y a quelque chose de nouveau, les gens évaluent les possibilités et adoptent cette nouveauté. Ensuite, on légifère et lentement les choses se structurent en fonction des lois. Actuellement, la législation n'est pas suffisante, surtout dans le monde numérique, alors nous avons du rattrapage à faire, si je puis dire. Ainsi, j'aimerais que vous souligniez, comme certaines personnes l'affirment, que nous ne pouvons pas retourner en arrière ou même rester immobiles. Nous devons aller de l'avant, mais nous pouvons le faire de la façon qu'a proposé Mme Cavoukian, c'est-à-dire en assurant la protection de la vie privée dès la conception. C'est un concept plutôt nouveau qui nous permet de commencer à penser à la protection des renseignements personnels lors de l'étape de la conception.

Qu'en pensez-vous?

M. Daniel Therrien: Je suis d'accord. Je suis tout à fait en faveur du concept de la protection de la vie privée dès la conception. Je dirais qu'il est vrai que la numérisation aura forcément lieu, mais la protection de la vie privée dès la conception signifie que la façon dont nous procédons doit faire l'objet d'une sérieuse et rigoureuse réflexion.

Il faut notamment tenir compte du rôle du secteur privé dans la prestation de services gouvernementaux. Vous avez parlé du Far West. Vous êtes bien placé pour savoir qu'il existe d'importants problèmes en ce qui a trait à la façon dont certaines entreprises gèrent les renseignements personnels des gens. L'amélioration des services gouvernementaux se fait grâce à la technologie appartenant au secteur privé et qui est utilisée pour la prestation de services. C'est très bien, mais en ce qui a trait à la prestation des services, par l'entremise du secteur privé — par exemple, à l'aide des Alexa de ce monde — le gouvernement doit faire très attention à la façon dont cela se fera, et ce, pour de nombreuses raisons. Il doit notamment savoir à qui appartient l'information transmise par Alexa, ou qui gère cette information, lorsqu'un citoyen demande des services gouvernementaux. Qu'arrive-t-il à cette information? Est-ce qu'elle est gérée par le gouvernement ou le secteur privé? Est-ce qu'elle est monétisée? Ce sont là des questions très importantes et fondamentales.

M. Frank Baylis: Je vous remercie.

Le président: Merci, monsieur Baylis.

Monsieur Kent, vous disposez de cinq minutes.

L'hon. Peter Kent: Merci.

Monsieur le commissaire, le Comité a déposé trois rapports auprès du gouvernement au cours de la dernière année environ. Dans chacun de ces rapports, il recommande d'élargir vos pouvoirs, de vous conférer le pouvoir de rendre des ordonnances et d'accroître la sévérité des sanctions dans les cas de violation. Il recommande également, en ce qui concerne la loi, que le gouvernement tienne compte du RGPD et qu'il actualise et renforce la réglementation canadienne sur la protection des renseignements personnels, qui est à peine acceptable actuellement.

Recommanderiez-vous que votre commissariat participe directement à la conception du gouvernement numérique? Autrement dit, pensez-vous qu'il est essentiel que le commissaire à la protection de la vie privée soit un partenaire clé dans tout projet lié au gouvernement numérique, dès les premières étapes ou certainement les étapes ultérieures?

● (1625)

M. Daniel Therrien: Nous pouvons constituer une valeur ajoutée, c'est certain, et nous avons offert nos services au gouvernement. Parfois, il a accepté notre offre. Est-ce nécessaire? Ce n'est peut-être pas à moi de répondre à cette question, mais je peux dire que je crois de façon générale que nous constituons une valeur ajoutée et que les systèmes conçus en fonction de nos recommandations risquent de mieux assurer la protection des renseignements personnels.

Lorsque ce n'est pas une question de choix, lorsqu'une loi précise, par exemple, les conditions dans lesquelles les données sont échangées entre les ministères, il est nécessaire qu'un organisme de réglementation solide veille au respect de ces conditions. Cet organisme est le commissariat.

L'hon. Peter Kent: Si le gouvernement numérique est la propriété du gouvernement et qu'il survient une atteinte grave et importante à la protection des données, qui cause des torts et qui a des conséquences sur la protection des renseignements personnels de citoyens canadiens ou de quiconque, pensez-vous que ce serait le commissaire à la protection de la vie privée qui imposerait des sanctions aux responsables de cette atteinte à la protection des données? Comment cela fonctionnerait-il si le gouvernement est celui qui gère le système?

M. Daniel Therrien: Vous soulevez la question...

L'hon. Peter Kent: Je parle de la responsabilité.

M. Daniel Therrien: D'accord. Le gouvernement doit être tenu responsable de la façon dont il gère les renseignements des citoyens. Le commissariat est bien placé pour veiller à ce que, dans une situation en particulier, le gouvernement soit tenu responsable et qu'il remédie à une atteinte à la protection des données.

Est-ce qu'une sanction pécuniaire doit être imposée? Je n'en suis pas certain en ce qui concerne le secteur public, mais quelqu'un doit repérer les infractions à la loi et veiller à ce que des mesures soient prises à cet égard. Nous sommes très bien placés pour faire cela.

L'hon. Peter Kent: En Estonie, il y a des dépôts de données. Comme vous l'avez dit, il y a de nombreux silos liés au système central et il y a la carte d'identité avec puce. Il est presque certain que diverses entités vont se livrer concurrence pour bénéficier des gains financiers qu'on peut retirer de la participation au gouvernement numérique. Neil Parmenter, le président de l'Association des banquiers canadiens, dans un discours qu'il a prononcé le mois dernier et auquel j'ai assisté, a pris soin de souligner que les banques canadiennes sont dignes de confiance. Elles utilisent l'authentification à double facteur. M. Parmenter a fait valoir l'intérêt des banques à jouer un rôle central au sein du gouvernement numérique. Que pensez-vous de cela?

M. Daniel Therrien: Il est vrai que les banques offrent des services qui, contrairement à d'autres, sont bien sécurisés. Je n'ai pas de problème en principe avec le fait que des banques ou d'autres organismes réputés, des organismes privés, soient responsables, par exemple, de la gestion de l'identificateur commun. C'est un des éléments du système. Le type d'information qu'ils obtiennent lorsque le gouvernement fournit des services aux citoyens constitue à mon sens une autre question, mais pour ce qui est de la gestion d'un identificateur commun sécurisé, j'estime que les banques sont sans doute bien placées pour effectuer cette tâche.

L'hon. Peter Kent: Merci.

Le président: Merci, monsieur Kent.

La parole est maintenant à M. Picard.

[*Français*]

M. Michel Picard (Montarville, Lib.): Bonjour, monsieur Therrien.

Je vais vous soumettre une prémisse, au sujet de laquelle j'aimerais connaître votre point de vue.

Je ne critique pas du tout le travail que nous avons fait. Je pense depuis longtemps que le Comité fait un travail respectable et excellent. Cependant, je vais vous proposer une autre façon de voir les choses.

Depuis environ six ou huit mois, nous étudions la protection des données personnelles, mais j'ai l'impression que nous pédalons dans le beurre et que nous travaillons pour rien, parce que nous n'avons pas été foutus de définir le problème à régler, c'est-à-dire de définir ce qui constitue une donnée personnelle. Je m'explique.

On panique à l'idée qu'on puisse lire une plaque d'immatriculation, sous prétexte que c'est de nature privée. Or, tout ce que cette plaque permet de faire, c'est identifier le véhicule sur lequel elle est installée, et non la personne qui est au volant. De la même manière, une adresse IP ne révèle pas l'identité de la personne qui tape au clavier de l'ordinateur, mais seulement l'endroit où se trouve ce dernier.

Les gens communiquent allégrement bien des données personnelles. Par exemple, rappelez-vous que, dans les premiers clubs vidéo, nous donnions sans hésiter notre numéro de permis de conduire pour avoir le droit de louer un film.

La raison pour laquelle j'ai l'impression qu'on ne veut pas toucher au problème de la définition d'une donnée personnelle, c'est que la plupart des témoins que nous avons entendus depuis presque un an nous ont répondu que la meilleure façon de protéger nos données personnelles n'était pas le recours à des moyens technologiques, mais la transparence: une entreprise comprend qu'un individu est prêt à lui donner à peu près n'importe quel renseignement personnel, mais elle s'engage en contrepartie à lui dire ce qu'elle en fera. Cela signifie donc que le spectre des données que vous êtes en mesure de fournir à quiconque n'est pas défini. Par conséquent, si nous ne sommes pas capables de définir le problème que nous voulons gérer, il sera difficile de définir les mesures que nous voulons prendre. Pourquoi ne pas simplement arrêter tout cela et interdire toute transaction de données? Si quelqu'un voulait faire une telle transaction, il devrait alors communiquer avec vous pour savoir comment gérer l'information transmise. C'est la première partie de ma question.

● (1630)

M. Daniel Therrien: En droit, je regrette de devoir vous dire que vous avez tort quand vous suggérez que les adresses IP ne sont pas des renseignements personnels. La Cour suprême en a décidé autrement dans un jugement, il y a quelques années. L'adresse IP pouvant être reliée à un individu, il s'agit d'un renseignement personnel qui doit être protégé à ce titre.

En ce qui a trait à la plaque d'immatriculation, la question ne se pose pas tout à fait de la même façon. Il n'y a quand même pas 800 personnes qui conduisent mon véhicule; il y a seulement mon épouse et moi. Il s'agit peut-être de renseignements personnels aussi.

Les renseignements personnels sont donc définis. Ce n'est pas sorcier: il s'agit de tout renseignement, y compris un numéro, qui se rapporte à une personne identifiable. Nous pourrions en discuter, mais je ne suis pas enclin à adhérer à votre prémisse.

Est-ce que la transparence fait partie de la solution pour protéger la vie privée? Oui, elle fait partie de la solution, mais elle n'est pas toute la solution, loin de là. On peut être transparent, mais quand même porter atteinte à la réputation d'un individu. Cela dit, la transparence fait partie de la solution.

Il s'agit effectivement d'une question complexe, et si nous avons de la difficulté à progresser, c'est parce qu'elle est complexe sur différents plans, notamment conceptuel et technologique. C'est pour cela que, plus récemment, j'ai mis l'accent sur la vie privée comme étant un droit de la personne. Commençons donc par les principes de base.

Quand je dis que la vie privée est un droit fondamental, il s'agit d'un concept qui devrait être reconnu non seulement par la loi, mais aussi par les instances gouvernementales qui, jour après jour, mettent en place des systèmes de collecte de données et d'administration de programmes publics, technologiques ou autres. Cela nous ramène à l'importance de la protection de la vie privée dès l'étape de la conception, un concept que nous devrions toujours garder à l'esprit. Si nous avons le choix entre offrir un service d'une façon qui met en danger la vie privée et offrir ce même service d'une autre façon tout aussi efficace, mais qui, elle, respecte la vie privée, le concept de protection de la vie privée dès l'étape de la conception nous dit que nous devrions choisir la deuxième option.

Toutes ces questions de vie privée peuvent sembler nébuleuses, mais, en droit, ce qui constitue un renseignement personnel est assez clair. Il faut nous rappeler quels éléments de la vie privée nous voulons protéger pour nous assurer de ce respect dans les activités du gouvernement et dans les lois.

● (1635)

[*Traduction*]

Le président: Je vous remercie, monsieur Picard.

La parole est à M. Angus pour les dernières minutes. On m'a demandé d'accorder un peu de temps à deux autres membres qui n'ont pas eu l'occasion de poser une question. C'est ce que je vais faire lorsque M. Angus aura terminé. Ensuite, nous allons passer à la motion qui a été présentée tout à l'heure.

La parole est à M. Angus pour trois minutes.

M. Charlie Angus: Merci, monsieur le président.

Je vous remercie, monsieur Therrien.

Plus tôt au cours de la présente session parlementaire, nous avons entamé une étude sur une atteinte à la protection des données qui concerne Cambridge Analytica et Facebook. Depuis, j'ai parfois l'impression que nous sommes devenus le comité parlementaire spécialiste de Facebook. Nous avons parcouru la moitié de la planète pour essayer d'obtenir des réponses de la part de cette entreprise et nous nous faisons encore berner, et je crois que nous allons inviter la moitié de la planète à venir nous rencontrer encore une fois à Ottawa lorsque le temps sera plus clément afin d'obtenir peut-être davantage de réponses de la part de Facebook. Il me semble que toutes les semaines de nouvelles questions surgissent et qu'il semble y avoir continuellement une absence de reddition de comptes.

J'aimerais vous demander précisément si vous vous êtes ou non penchés là-dessus. Il y a eu cet article qui a fait grand bruit dans le *New York Times* à propos des privilèges accordés à certains utilisateurs de Facebook leur permettant de lire des messages personnels et privés de certains autres utilisateurs de Facebook. On mentionnait que la RBC en faisait partie. Nous avons entendu des représentants de la RBC. Ils ont affirmé qu'ils n'ont jamais bénéficié de tels privilèges, qu'ils n'ont jamais fait cela. La revue *The Tyee* affirme que Facebook lui a déclaré que la RBC est en mesure de lire, d'écrire et de supprimer des messages privés dans les comptes d'utilisateurs de Facebook qui utilisent l'application de la banque.

Vous êtes-vous penchés là-dessus? Croyez-vous que cette situation mérite d'être examinée? Devrions-nous croire la RBC sur parole? Devrions-nous, en tant que comité, considérer cela comme un autre dossier à étudier en ce qui concerne Facebook?

M. Daniel Therrien: Je dirais oui pour répondre brièvement, pour deux raisons.

Lorsque le comité parlementaire britannique a publié les documents de Six4Three, on y a vu le nom de la Banque royale, et nous nous sommes demandé si nous devions examiner cela dans le cadre de notre enquête sur Facebook et AIQ. Nous avons à ce moment-là reçu des plaintes de la part de personnes qui se demandaient si la Banque royale se trouvait à enfreindre la LPRPDE d'une certaine façon étant donné qu'elle recevait de l'information de cette manière. Cette question fait donc l'objet d'une enquête distincte.

M. Charlie Angus: Soyons clairs, vous dites que vous avez reçu des plaintes à propos d'infractions commises par la RBC...

M. Daniel Therrien: Des plaintes au sujet du fait que la RBC recevait présumément des renseignements de Facebook et qu'elle enfreignait semble-t-il la LPRPDE.

M. Charlie Angus: D'accord. D'après ce que vous savez de ces privilèges accordés à certains clients de Facebook, pouvez-vous me dire s'il était possible de lire des messages privés d'utilisateurs de Facebook grâce à ces privilèges?

M. Daniel Therrien: Je ne peux pas faire de commentaires à ce sujet, car nous sommes en train de mener une enquête. Nous allons le déterminer, c'est certain.

M. Charlie Angus: Vous êtes en train d'effectuer une enquête. D'accord, c'est très bien.

Je vous remercie beaucoup.

Le président: Je vous remercie, monsieur Angus.

La parole est maintenant à Mme Vandenbeld pour deux minutes et demie, et ensuite...

Mme Mona Fortier: Elle va prendre tout le temps de parole.

Le président: D'accord.

Allez-y.

Mme Anita Vandenbeld (Ottawa-Ouest—Nepean, Lib.): Je vous remercie, monsieur le président, de m'accorder la dernière question. Le témoignage du commissaire est très important et très intéressant.

J'aimerais revenir sur l'idée de la propriété et du consentement dans le contexte du gouvernement. Si Air Canada me demande mon adresse courriel et mon numéro de téléphone cellulaire pour que je puisse recevoir des messages m'informant que mon vol est retardé, par exemple, j'ai le choix de donner ou non cette information. Toutefois, en ce qui concerne le gouvernement, vous n'avez pas toujours le choix. Vous devez fournir l'information, notamment à des fins fiscales. L'idée de consentement n'a automatiquement plus la même signification lorsque l'on doit fournir des renseignements.

Cela dit, comment envisagez-vous le consentement et même la propriété des données? Si je vais dans le site d'Air Canada, je peux supprimer mon profil. J'ai le choix. Mais en ce qui a trait au gouvernement, s'il s'agit d'un casier judiciaire, on ne peut pas décider de le supprimer ou de le modifier. L'information n'appartient plus réellement à la personne.

Qu'en est-il de la propriété et du consentement lorsqu'il s'agit du gouvernement?

● (1640)

M. Daniel Therrien: Vous avez tout à fait raison de dire qu'il n'est pas toujours nécessaire de donner son consentement à un gouvernement pour qu'il recueille des renseignements sur nous. La situation est différente. La Loi sur la protection des renseignements personnels contient déjà des dispositions à cet égard.

Une des dispositions stipule que le gouvernement devrait recueillir des renseignements, dans la mesure du possible, directement auprès de la personne concernée, avec ou sans le consentement, par exemple, dans une situation d'application de la loi. Le principe est que le gouvernement doit recueillir l'information directement auprès de la personne, mais des questions se posent quant aux renseignements qui se trouvent dans les médias sociaux ou qui sont potentiellement publics. C'est difficile à gérer dans le cadre de la loi actuelle. Quoi qu'il en soit, le premier principe est que le gouvernement doit recueillir l'information auprès de la personne concernée, avec ou sans le consentement. Dans le secteur privé, ce n'est pas tout à fait la même chose. Je conviens que le consentement n'est pas toujours nécessaire.

Mme Anita Vandenbeld: Cela étant dit, nous avons entendu dire que le gouvernement a recours notamment à l'analytique prédictive et qu'il pourrait le faire davantage dans le futur. Je crois qu'on a donné comme exemple l'ARC, qui peut même utiliser une certaine forme d'intelligence artificielle et l'analytique prédictive pour déterminer où le risque de fraude est le plus probable, afin qu'elle puisse cibler ce genre de situation.

Par contre, le concept de la protection de la vie privée dès la conception implique précisément que les données sont utilisées aux fins pour lesquelles elles sont recueillies. Si vous fournissez des renseignements à l'ARC à propos de vos impôts, et que l'ARC a le mandat d'enquêter sur les fraudes fiscales, vos renseignements pourraient ne pas nécessairement être utilisés aux fins pour lesquelles ils ont été recueillis, mais il pourrait s'agir d'une utilisation légitime de l'information par le gouvernement. Ce n'est qu'un exemple parmi d'autres.

Dans un monde où on a davantage recours à l'analytique prédictive et à l'intelligence artificielle, qu'en est-il du concept de la protection de la vie privée dès la conception?

M. Daniel Therrien: Dans le domaine fiscal, l'ARC obtient directement du contribuable certains renseignements. Il est possible que l'ARC utilise les médias sociaux et d'autres sources pour obtenir des renseignements et qu'elle recueille toute cette information pour alimenter un système d'intelligence artificielle. C'est quelque chose d'important. L'analytique est une nouvelle réalité et elle a de nombreux avantages.

Cependant, en ce qui concerne les systèmes d'intelligence artificielle, l'information qui alimente ces systèmes doit être fiable et avoir été obtenue légalement, ce qui entraîne certaines conséquences. Si l'ARC recueille des renseignements dans les médias sociaux, et présumons un instant qu'il s'agit d'information réellement publique, cela ne signifie pas que ces renseignements sont fiables.

Pour répondre à votre question, je dirais que, dans le contexte de l'intelligence artificielle, la protection de la vie privée dès la conception vise à faire en sorte que l'intelligence artificielle soit utilisée de façon à ce que l'information qui alimente le système ait premièrement été obtenue légalement, deuxièmement, soit fiable et, troisièmement, n'entraîne pas de discrimination pour des motifs interdits et soit fondée sur des facteurs d'analyse objectifs.

Mme Anita Vandenbeld: On a aussi proposé, pour de nombreuses utilisations, d'anonymiser les données avant de les examiner. Croyez-vous que c'est faisable?

M. Daniel Therrien: C'est préférable, mais ce n'est pas toujours possible. Je peux concevoir que l'intelligence artificielle utilise des renseignements personnels, mais il est préférable de commencer avec des renseignements anonymisés.

Mme Anita Vandenbeld: Je vous remercie.

Le président: Je vous remercie tous.

Je remercie le commissaire et son personnel d'avoir comparu devant nous aujourd'hui. Vos propos nous éclairent toujours. C'est un sujet qui semble prendre continuellement de l'ampleur. Je vous remercie donc pour votre présence aujourd'hui.

M. Daniel Therrien: Je vous en prie.

Le président: Nous allons continuer un peu pour traiter de la motion qui a été présentée avant le témoignage de M. Therrien.

La parole est d'abord à M. Kent, et ensuite, ce sera au tour de M. Angus.

L'hon. Peter Kent: Je vous remercie, monsieur le président.

Je crois comprendre que les libéraux aimeraient disposer de 48 heures pour examiner la demande, alors, au nom de la collégialité, j'accepte d'accorder 48 heures.

Cependant, j'aimerais présenter une motion visant à faire en sorte que la motion originale d'aujourd'hui figure comme premier point à l'ordre du jour de notre prochaine réunion.

Le président: Allez-y, monsieur Angus.

M. Charlie Angus: Je suis absolument outré par la collégialité dont fait preuve mon collègue, alors je vais devoir consulter mon voisin pour décider si nous allons faire de l'obstruction.

● (1645)

Le président: Il me semble que la discussion a été plutôt bruyante durant la réunion, alors, la prochaine fois, je vous demanderais d'être un peu plus calmes. Il semble que nous allons traiter de cela mardi prochain, alors je vous souhaite à tous une bonne fin de semaine.

Oui, monsieur Angus.

M. Charlie Angus: Il y a une autre chose. Nous étions censés discuter de ma motion aujourd'hui, qui porte sur la planification d'une étude parallèle. Nathaniel souhaite travailler le libellé de ma motion avant la séance publique.

Au nom de la collégialité, comme on a dit, on vous accorde cela une fois pendant les quatre ans et c'est tout, alors profitez-en.

M. Frank Baylis: Vous pouvez mettre cela sur Twitter.

M. Charlie Angus: Oui, sur Twitter. Je fais preuve de collégialité aujourd'hui.

Je vais vous proposer une formulation qui, je l'espère, sera acceptable pour tout le monde et que je vais soumettre à Peter.

Je vous remercie.

Le président: Je vous remercie tous. Bon week-end.

La séance est levée.