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 135 • 1re SESSION • 42e LÉGISLATURE

TÉMOIGNAGES

Le jeudi 7 février 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 7 février 2019

● (1530)

[*Traduction*]

Le président (M. Bob Zimmer (Prince George—Peace River—Northern Rockies, PCC)): Je déclare ouverte la réunion 135 du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique. Conformément au sous-alinéa 108(3)*h*)(vii) du Règlement, notre étude porte sur la protection des données personnelles dans les services gouvernementaux numériques.

Nous accueillons aujourd'hui des invités qui témoignent à titre personnel. Nous avons Jeffrey Roy, professeur à l'École d'administration publique de l'Université Dalhousie; David Eaves, conférencier en politiques publiques de digital HKS à la Harvard Kennedy School; et la dernière, mais non la moindre Amanda Clarke, professeure adjointe à l'Université Carleton.

Avant de débuter, je tiens à mentionner que la majorité d'entre vous a vu le communiqué au sujet du Grand Comité international qui a été diffusé aujourd'hui à midi. J'ai aussi parlé ce matin avec Damian Collins, mon homologue du Royaume-Uni. C'est une histoire à suivre à mesure que cela progresse. Nous communiquons avec des groupes pour leur demander de témoigner, et nous ajouterons des pays à la liste que nous avons déjà. Cela s'en vient. Si vous voulez d'autres renseignements, n'hésitez pas à le demander.

Mme Fortier a proposé un témoin. Je tiens à dire officiellement que vous pouvez proposer des témoins à tout moment. Nous avions une échéance parce que nous avions besoin d'un certain nombre de témoins au départ pour aller de l'avant. Si vous avez un témoin qui, selon vous, pourrait aider le Comité dans ses travaux, faites parvenir son nom au greffier ou à mon bureau, et nous l'ajouterons à la liste. Cela étant dit, je tiens à vous envoyer la liste des témoins — là où nous en sommes rendus actuellement — pour que vous sachiez l'endroit où se trouve votre témoin dans la liste.

Charlie a une question.

M. Charlie Angus (Timmins—Baie James, NPD): J'ai deux points. Premièrement, j'aimerais avoir une liste de témoins. Jusqu'à présent, nous n'avons pas suivi la procédure normale au Comité, c'est-à-dire de déterminer le nombre de réunions que nous aurons et d'ensuite passer en revue les témoins pour établir si nous avons besoin de tous les entendre. J'aimerais le faire.

Je ne souhaite pas prendre le temps consacré à nos brillants témoins, mais la semaine prochaine est une semaine de relâche, et j'aimerais souligner que, compte tenu de l'article du *Globe and Mail* sur les allégations concernant SNC-Lavalin et de ce qui est dit au sujet du lobbying qui a eu lieu, le Comité de l'éthique devra se pencher sur la question et en particulier déterminer le genre de lobbying qu'a fait SNC-Lavalin.

Je proposerai une motion aux fins de discussions, étant donné que les gens s'attendront à ce que nous examinions toutes les allégations d'activités de lobbying inacceptables qui peuvent avoir influé sur l'orientation d'une politique. Je la proposerai à la prochaine réunion.

Le président: Merci, monsieur Angus. Y a-t-il d'autres commentaires?

D'accord. Allons-y. Je remercie nos témoins de leur présence aujourd'hui. Vous avez 10 minutes.

Nous entendrons en premier Mme Clarke. Comme le dit l'expression, les femmes d'abord.

Mme Amanda Clarke (professeure adjointe et titulaire de la chaire d'excellence en recherches en affaires publiques, School of Public Policy and Administration, Carleton University, à titre personnel): Merci beaucoup.

Je m'appelle Amanda Clarke. Je suis professeure adjointe à l'École d'administration publique et de politique gouvernementale de l'Université Carleton ici à Ottawa où je suis titulaire de la chaire d'excellence en recherche sur les affaires publiques.

Je réalise des recherches et je conseille les gouvernements sur le gouvernement numérique depuis 10 ans. Mes travaux ont en fait débuté ici. À une certaine époque, j'étais analyste à la Bibliothèque du Parlement, et j'étais aux premières loges lorsque les parlementaires ont commencé à nous poser des questions sur des choses comme Twitter, Facebook et les données ouvertes. C'est très intéressant d'être de retour ici pour discuter encore une fois de certains de ces sujets.

J'ai poursuivi mes travaux dans ce domaine avec un doctorat à l'Oxford Internet Institute de l'Université d'Oxford, où j'ai réalisé une étude doctorale qui compare les réformes sur le gouvernement numérique au Canada et au Royaume-Uni. Les parties de cette étude ayant trait au Royaume-Uni se concentraient passablement sur le modèle d'un « gouvernement comme plateforme » qu'a mis en place le gouvernement du Royaume-Uni. Vous en avez parlé un peu et vous avez aussi parlé du Government Digital Service. Je serai ravie d'en discuter avec vous pendant les séries de questions.

Les parties de cette étude ayant trait au Canada ont récemment été publiées dans un livre qui décrit l'historique et la trajectoire du gouvernement numérique au Canada. Je mets l'accent en particulier sur les tensions entre certaines exigences du gouvernement numérique et la tradition du régime de gouvernement britannique au Canada.

Je mène actuellement un projet de recherche sur les technologies civiques et la gouvernance des données. Ces travaux visent à analyser le rôle que les intervenants privés jouent dans la prestation de services gouvernementaux numériques. Nous examinons les mécanismes de gouvernance disponibles pour veiller à une administration plus responsable et plus équitable des données personnelles et publiques.

Je suis vraiment reconnaissante d'avoir l'occasion de prendre la parole devant vous aujourd'hui. Je vous félicite d'avoir inscrit au programme parlementaire un enjeu que je considère comme vraiment important.

Je traiterai de trois sujets. Le premier sujet concerne les tensions et les complémentarités entre les services gouvernementaux numérisés et la protection des renseignements personnels et la sécurité. Deuxièmement, j'aimerais parler de la gouvernance des données et de la privatisation des services gouvernementaux numériques. Troisièmement, il sera question très brièvement de la gouvernance des données autochtones.

Pour ce qui est du premier thème, votre étude a vraiment comme objectif de promouvoir des services gouvernementaux numériques efficaces, tout en veillant à la protection des renseignements personnels des Canadiens et en traitant des enjeux connexes de sécurité. Je crois que vous avez raison de croire que ces objectifs sont peut-être en concurrence et d'essayer d'arriver à un équilibre entre ces priorités.

Au sujet de cet équilibre, le Comité et de précédents témoins ont cerné des manières dont les fonctionnaires fédéraux en particulier donnent l'impression de faire preuve de laxisme en ce qui concerne l'importance de la protection des renseignements personnels. Il y a eu des discussions au sujet de gens qui ont perdu des disques durs contenant des données sur les utilisateurs et qui cachent de l'information au commissaire à la protection de la vie privée concernant des atteintes à la protection des données, par exemple. Parallèlement, dans mes travaux de recherche auprès de fonctionnaires fédéraux, j'entends régulièrement...

● (1535)

Le président: Madame Clarke, nos interprètes ont de la difficulté à suivre votre rythme. Pouvez-vous parler un peu moins vite? Merci.

Mme Amanda Clarke: D'accord. C'est vrai que j'ai pris un café avant de m'en venir ici.

Des voix: Ha, ha!

Mme Amanda Clarke: Mes étudiants me reprochent la même chose. Je m'excuse.

M. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Cela nous arrive à tous. Ne vous en faites pas.

Mme Amanda Clarke: D'accord.

C'est bon. Je vais prendre le temps de respirer.

Le Comité semble avoir l'impression... Ce que je veux dire, c'est qu'il y a eu beaucoup de discussions qui sous-entendaient que les fonctionnaires fédéraux ne sont pas suffisamment conscients de l'importance de la protection des renseignements personnels. Parallèlement, dans mes travaux auprès de fonctionnaires fédéraux, j'entends souvent un autre son de cloche qui dépeint les fonctionnaires comme faisant preuve, dans certains cas, d'excès de zèle en ce qui concerne leurs préoccupations relatives à la protection des renseignements personnels et la question connexe de cybersécurité.

Bon nombre d'entre vous se demanderont peut-être comment les gouvernements peuvent faire preuve d'excès de zèle en ce qui a trait à la protection des renseignements personnels et à la sécurité et se diront que ces éléments devraient toujours être une priorité. Toutefois, si vous pensez ainsi, cela permet en gros à ces inquiétudes de prendre le dessus. Dans bon nombre de cas, cela peut directement restreindre la portée de l'innovation et des améliorations nécessaires aux services que les gouvernements offrent aux Canadiens. Cela peut aussi vraiment nuire à l'efficacité des activités quotidiennes du gouvernement, en particulier en ce qui a trait à l'analyse des politiques. Il arrive souvent que cette inquiétude excessive concernant la protection des renseignements personnels et la sécurité ne permette même pas de régler les véritables questions en la matière.

Il y a trois exemples concrets. Bon nombre de bureaux gouvernementaux n'ont pas d'accès sans fil à l'Internet. C'est en partie parce que des gestionnaires qui ont une trop grande aversion pour le risque ont décidé que le risque pour la sécurité et la protection des renseignements personnels était trop élevé. Dans le même ordre d'idées, de nombreux fonctionnaires ne peuvent pas télécharger les outils dont ils ont besoin pour faire leur travail, comme des gratuiciels en ligne qui leur permettraient de faire des analyses de données plus poussées ou même des analyses de données très simples. Il arrive souvent que des fonctionnaires ne puissent pas avoir accès à certains sites Web qui contiennent des renseignements très pertinents à leur travail d'élaboration de politiques, d'autant plus que ce sont des sites Web qu'utilisent régulièrement les intervenants et les utilisateurs des services.

Peut-être plus important encore, cela s'explique en partie en raison des inquiétudes relatives à la protection des renseignements personnels, mais les lois actuelles, les régimes de responsabilisation verticale et les stratégies ministérielles de gestion de l'information favorisent le cloisonnement des données dans la fonction publique. Cela nuit vraiment à notre capacité d'apporter des améliorations importantes à la prestation des services et d'avoir des analystes des politiques qui se penchent sur des données provenant de divers domaines. Il est de plus en plus important de réaliser des analyses des politiques transversales qui s'appuient sur des données provenant de nombreux ministères étant donné que nous reconnaissons que les défis actuels au chapitre des politiques ne sont pas propres à un seul ministère. Il y a une transversalité intrinsèque. Ces enjeux se fichent des frontières ministérielles.

Dans de telles circonstances, les fonctionnaires — les gens s'en plaignent chaque jour — ne peuvent pas vraiment avoir accès aux outils, aux données et aux gens dont ils ont besoin pour accomplir un bon travail. Cela crée des milieux de travail qui renforcent le stéréotype d'un gouvernement qui est déconnecté de la réalité et qui ne fait pas preuve d'innovation, ce qui ne contribue certainement pas au recrutement au sein de la fonction publique. Qui plus est, cela garantit que nous continuerons d'avoir des services gouvernementaux qui sont inférieurs à la norme et qui ne répondent pas aux attentes, ce qui ancre les taux de confiance déjà faibles des Canadiens à l'égard de l'État.

Je tiens à préciser que je ne propose pas au gouvernement de mettre de côté les préoccupations en matière de sécurité et de protection des renseignements personnels. Je suggère plutôt que votre comité préconise une approche qui tient compte des concessions et de la perte d'efficacité qui peuvent arriver lorsque nous accordons une trop grande priorité à la protection des renseignements personnels et à la sécurité sans adopter une approche plus équilibrée. Je recommande ici des cadres permissifs et flexibles. Quelle forme prendraient-ils dans les faits? Nous pouvons examiner certains travaux déjà en cours au gouvernement fédéral qui montrent qu'il y a des mesures vraiment prometteuses qui sont prises par des fonctionnaires pour trouver l'équilibre que cherche le Comité. En voici quelques-unes.

Premièrement, le gouvernement du Canada a récemment proposé des normes pour les services numériques qui accordent la priorité à la protection des renseignements personnels et à la sécurité, mais ces normes permettent de respecter ces principes tout en mettant en place des services qui répondent aux besoins des utilisateurs. Par ailleurs, le Canada s'est récemment révélé un chef de file dans l'élaboration de cadres très progressistes concernant l'utilisation responsable de l'intelligence artificielle au gouvernement. Ces travaux visent à trouver encore une fois un équilibre entre la nécessité de respecter les principes d'équité, de représentation démocratique, de transparence, de protection des renseignements personnels et de sécurité, tout en utilisant de manière très novatrice les données pour améliorer les services gouvernementaux et élaborer des solutions plus solides en matière de politiques.

Fait important, ces travaux sur l'utilisation responsable de l'intelligence artificielle ont été réalisés de manière ouverte. Cela s'est fait en collaboration avec des intervenants et des experts au moyen de Google Docs. Cela permet de donner aux travaux une certaine légitimité, mais cela permet aussi une grande transparence, et je crois que nous devrions nous en réjouir.

Enfin, j'aimerais parler du Service numérique canadien qui relève du Secrétariat du Conseil du Trésor. Cet organisme a été créé dans le budget de 2017. C'est un autre endroit où le gouvernement recrute une équipe de personnes talentueuses qui ont non seulement une grande expertise technologique, mais aussi un esprit très éclairé en matière de politiques en vue de trouver un équilibre entre la nécessité d'améliorer les services gouvernementaux et le respect des principes relatifs à la protection des renseignements personnels et à la sécurité. Je parle ici de ce que l'industrie a de meilleur à offrir en matière de protection des renseignements personnels et de sécurité, et je crois que cela permet vraiment de stimuler de grandes innovations au gouvernement.

● (1540)

Bref, je crois que nous avons un contexte très prometteur, et la chose à retenir pour le Comité est qu'il faut continuer de soutenir ce travail. Pour ce faire, il faut du financement pour embaucher plus de gens dans ces domaines. Cela signifie aussi qu'il faut donner à certains groupes qui mènent ces travaux les leviers législatifs, politiques et administratifs dont ils ont besoin pour le faire à l'échelle de la fonction publique. Même si ces travaux sont prometteurs, ce n'est que le début, et cela se trouve majoritairement au centre du gouvernement.

Comme il ne me reste que quelques minutes, je vais passer au deuxième point dont j'aimerais parler, soit les questions relatives à la gouvernance des données dans le contexte de la privatisation des services gouvernementaux numériques.

Le message que je souhaite vraiment vous transmettre, c'est qu'il est important pour le Comité de reconnaître que l'État ne s'occupe pas directement, voire aucunement, de la prestation d'un grand nombre de services gouvernementaux numériques. Les gens espéraient au départ qu'avec le gouvernement numérique les gouvernements rendraient publiques leurs données et que d'autres les utiliseraient pour innover.

Ce discours a été plutôt nuancé, et je crois que les gouvernements ont adopté une approche beaucoup plus réaliste en la matière. Néanmoins, il y a de nombreux services gouvernementaux fédéraux auxquels nous accédons par l'entremise de plateformes qui n'appartiennent pas au gouvernement. Je vous donne l'exemple du logiciel TurboTax que plus de 12 millions de Canadiens ont utilisé depuis 2012 pour produire des déclarations de revenus ou de l'application CANImmunize qui a été développée en partenariat avec des hôpitaux et qui a aussi été partiellement financée et entérinée par des gouvernements. Cette application mobile permet de faciliter le suivi de votre dossier de vaccination.

Il y a aussi un nombre incalculable d'interfaces numériques que nous utilisons pour avoir accès aux services gouvernementaux. Certaines sont offertes directement par le gouvernement. D'autres ne le sont pas, mais le gouvernement les approuve. Enfin, certaines interfaces sont exploitées de façon indépendante.

À mon avis, voici la question importante que nous devons nous poser. Lorsque ces interfaces numériques qui ne sont pas gérées par le gouvernement et qui appartiennent par conséquent à des intérêts privés deviennent la seule manière d'avoir accès aux services gouvernementaux ou la manière la plus facile, quel est le rôle du gouvernement et comment le gouvernement peut-il s'assurer que la collecte de données sur ces interfaces se fait conformément aux règles en matière de protection des renseignements personnels et respecte les principes d'une bonne gouvernance des données? Par exemple, lorsque des gouvernements sous-traitent la prestation de services numériques à des entreprises privées, les gouvernements doivent définir très rigoureusement les données qui peuvent être recueillies, l'utilisation et la monétisation qui peuvent en être faites et les entités qui profiteront de cette monétisation.

Nous devons aussi adopter une approche très réaliste à l'égard de la capacité des citoyens de donner leur consentement éclairé concernant certains de ces services privés. Dans un récent article de fond du *New York Times*, on estimait qu'il faudrait 76 jours de travail à une personne moyenne pour lire toutes les politiques sur la protection des renseignements personnels numériques qu'elles acceptent en une année. Selon moi, dans nos modèles de consentement pour certains de ces services privés, nous devrions aussi réfléchir un peu plus à cette question.

● (1545)

Le président: Merci, madame Clarke.

Mme Amanda Clarke: Puis-je mentionner le dernier point, parce que je crois vraiment qu'il faut en tenir compte?

Le président: Vous avez déjà pris une minute de plus. Si vous pouvez le faire en 10 secondes, allez-y.

Mme Amanda Clarke: Ce n'est qu'un dernier petit point. Je ne l'ai pas encore vu mentionner dans la transcription des discussions, mais comme certaines des délibérations du Comité n'ont pas encore été rendues publiques, il se peut qu'on en ait déjà parlé.

Je voudrais recommander au Comité d'aborder tout particulièrement la question de la souveraineté des données autochtones dans le cadre de ses travaux. Je ne suis pas une experte en la matière, mais je peux proposer des personnes à qui vous devriez vous adresser. Cette question soulève des préoccupations tout à fait uniques en ce qui concerne la manière dont le gouvernement du Canada recueille et utilise les données relatives aux peuples autochtones et, en particulier, la façon dont les services sont offerts à ces collectivités. Sachant que ces données ont constamment servi à marginaliser et à opprimer les peuples autochtones, je crois qu'il incombe à votre comité de consacrer du temps à cette question.

Merci.

Le président: Merci, madame Clarke.

C'est maintenant au tour de Jeffrey Roy, qui dispose de 10 minutes.

M. Jeffrey Roy (professeur, School of Public Administration, Dalhousie University, à titre personnel): Merci beaucoup.

Je vais tout simplement lire une brève note d'allocution pour me forcer à ne pas dépasser le temps de parole qui nous est alloué aujourd'hui.

Bonjour, monsieur le président, mesdames et messieurs les membres du Comité et chers collègues. Je tiens à remercier le Comité de me donner l'occasion de témoigner aujourd'hui. Je suis heureux de participer à cette discussion sur un sujet aussi important, à savoir la façon dont les gouvernements peuvent accroître et améliorer les capacités en matière de services numériques, tout en protégeant les renseignements personnels et la sécurité des citoyens et de tous les intervenants.

Je vais commencer par m'appuyer sur quelques-unes des observations réfléchies faites par le commissaire à la protection de la vie privée lors de sa comparution devant le Comité la semaine dernière. J'ai retenu trois points en particulier: premièrement, l'importance de la feuille de route de la stratégie de données du gouvernement du Canada; deuxièmement, la différence entre les notions d'obstacles et de mesures de protection; troisièmement, le modèle estonien, comme point de comparaison pour le Canada et d'autres pays.

À mon avis, la feuille de route de la stratégie de données est un point de référence important dans ce débat, comme l'a fait remarquer le commissaire à la protection de la vie privée. Il s'agit d'une discussion approfondie des possibilités et des défis, à la lumière des efforts cumulatifs déployés par les gouvernements libéraux et conservateurs au cours de la dernière décennie, ainsi que des efforts similaires à tous les ordres de gouvernement et dans les secteurs privé et sans but lucratif.

Les capacités guidées par les données sont maintenant largement considérées comme des catalyseurs essentiels de l'innovation en matière de services dans le monde numérique d'aujourd'hui. De telles capacités présupposent souvent, voire exigent, l'échange de données entre de nombreuses entités gouvernementales; pourtant, la feuille de route décrit avec justesse le secteur public comme un environnement fragmenté, dont la structure est souvent plus verticale qu'horizontale, comme Amanda l'a mentionné, et qui comporte toutes sortes d'obstacles législatifs et culturels, lesquels entravent l'adoption d'une approche pangouvernementale.

De son point de vue, le commissaire à la protection de la vie privée fait remarquer que « ce qui est un obstacle juridique pour certains peut être considéré par d'autres comme une garantie de protection de la vie privée ». À mon avis, la tâche essentielle de votre comité est de concilier les tensions inhérentes à cette observation perspicace avec les réalités changeantes de la société d'aujourd'hui et les nouvelles possibilités offertes par la numérisation. Même si je salue le travail crucial accompli par le commissaire à la protection de la vie privée pour protéger et faire respecter les droits en matière de protection des renseignements personnels, il n'en demeure pas moins que de nombreux obstacles législatifs, organisationnels et politiques entravent une innovation accrue au chapitre de l'échange de renseignements et de données.

Plusieurs projets pilotes menés dans l'ensemble du pays, à tous les ordres de gouvernement et faisant intervenir parfois plus d'un palier de gouvernement, ont démontré comment les renseignements et les données peuvent être échangés sans mettre en péril la protection de la vie privée. Cependant, de tels projets pilotes vont trop souvent à contre-courant de l'administration publique traditionnelle et des notions exclusives de protection et de contrôle.

À une époque où l'ouverture et l'engagement sont au coeur des modèles de gouvernance réseautée et agile, modèles qui défient les hiérarchies traditionnelles, il est normal que la protection des renseignements personnels soit une notion contestée. Bien qu'une grande partie de la société demeure profondément préoccupée par la protection des renseignements personnels, d'autres gens ont tout simplement renoncé à ce concept qu'ils jugent désuet et irréaliste. Pour combler cet écart grandissant, il faut une confiance envers les mécanismes de gouvernance publique et collective, et les principaux vecteurs d'une telle confiance sont l'ouverture et le dialogue, en gros, de la part des institutions politiques.

À cet égard, et cela rejoint votre point, l'Estonie est un brillant exemple d'un pays qui a adopté des technologies à source ouverte et des solutions de pointe en vue d'offrir des services en ligne plus intégrés. Un élément central de la réussite bien établie de l'Estonie dans ce domaine, c'est l'engagement politique soutenu et transpartisan pour faire de la transformation numérique un projet sociétal au lendemain de l'effondrement de l'Union soviétique.

En ce qui concerne l'histoire politique et les structures institutionnelles, un pays qui se compare mieux au Canada est l'Australie, laquelle constitue une autre étude de cas convaincante. Malgré les échecs numériques et les atteintes à la vie privée dont on a largement fait état et auxquels aucun pays n'échappe, l'Australie s'est hissée progressivement aux premiers rangs dans le cadre des sondages menés par les Nations unies sur le cybergouvernement à l'échelle mondiale au cours de la dernière décennie — ce qui est en corrélation inverse avec le rendement du Canada —, en partie grâce à un dialogue politique fructueux et à un engagement solide à l'égard de questions numériques de la part des élus de la Chambre et du Sénat.

Une telle connaissance des réalités politiques permet de faciliter l'acceptation de la culture numérique dans la société en général. En outre, l'Australie a créé récemment un nouvel organisme national, composé de représentants du fédéral et des États, qui se consacre à l'élaboration de solutions en matière de cybersanté et, par extension, qui concilie la protection des renseignements personnels et l'échange de données dans ce domaine crucial. Même si j'ai beaucoup de respect pour les limites et les avantages du fédéralisme, le Canada doit tirer une leçon importante au chapitre de la réforme des soins de santé, soit la nécessité d'une plus grande collaboration intergouvernementale au moment de concevoir de nouveaux cadres numériques pour des politiques communes et des modes de prestation plus virtuels.

● (1550)

De façon plus générale, l'absence d'une collaboration plus robuste au Canada, particulièrement en ce qui concerne le financement et le partage de la responsabilisation sur le plan politique, est un facteur important qui freine le progrès et l'innovation en matière de services numériques. La présence d'une multitude de centres de services du secteur public dans les grandes villes et les villes de taille moyenne ne fait que mettre en évidence ce point, car cela encourage davantage chaque palier de gouvernement à se concentrer sur son propre ensemble de services, et ce, en grande partie, de façon séparée.

Bien sûr, le Canada n'est pas le seul pays à se heurter à de tels problèmes. D'ailleurs, j'agis actuellement comme expert-conseil auprès de l'OCDE pour contribuer à une étude inédite qui porte sur le gouvernement numérique du point de vue infranational et intergouvernemental. Un thème qui ressort de ce projet est le rôle essentiel d'une architecture de gouvernance holistique pour le secteur public dans son ensemble.

Permettez-moi de faire deux dernières observations. Tout d'abord, la protection des renseignements personnels à l'ère du numérique ne devrait pas être présentée uniquement, ou même principalement, comme une question de droits. Les citoyens ont, eux aussi, des responsabilités à assumer s'ils veulent devenir des « militants de données », pour reprendre l'expression employée par Nora Young, une journaliste de CBC, dans son livre intitulé *The Virtual Self*.

Un nouveau contrat social pour l'ère du numérique ne peut reposer sur des promesses irréalistes concernant des droits absolus en matière de protection des renseignements personnels, surtout dans un monde où les gouvernements, eux-mêmes, doivent contester de tels droits pour une foule de raisons. Bien entendu, le secteur privé assume également d'importantes responsabilités à l'égard des clients et de tous les intervenants. Un dialogue plus poussé constitue une première étape essentielle pour la sensibilisation du public et l'action collective. De plus, selon moi, il est nécessaire de miser sur de nouvelles formes de participation plus directe des citoyens à la conception de solutions de services numériques.

J'en viens à ma dernière observation, à savoir le rôle essentiel que joue le pouvoir législatif en matière de capacités de prévention, pour ainsi dire, afin de mieux comprendre les défis et les risques qui nous attendent. Le Comité a sans doute entendu des experts parler du potentiel des technologies de chaîne de blocs, que certains pourraient associer aux cryptomonnaies comme Bitcoin.

Outre l'adoption généralisée de la chaîne de blocs en Estonie, la Finlande déploie ce genre de technologies pour offrir des services de soutien aux réfugiés, alors qu'un autre projet pilote finlandais encourage les producteurs agricoles et les gouvernements locaux à travailler ensemble pour améliorer les services d'emploi dans les collectivités rurales. L'Union européenne a financé plusieurs projets pilotes semblables axés sur la chaîne de blocs; il convient d'ailleurs de souligner que le Parlement européen a nommé un conseiller spécial chargé de la chaîne de blocs afin de faciliter l'apprentissage collectif.

Pour terminer, je tiens à féliciter le Comité des efforts qu'il déploie en tant qu'important catalyseur du renforcement de l'innovation numérique dans la prestation des services publics, et j'attends avec impatience vos questions.

Le président: Merci encore une fois.

Le dernier témoin que nous allons entendre aujourd'hui est M. Eaves. Vous avez 10 minutes.

M. David Eaves (conférencier en politiques publiques, Digital HKS, Harvard Kennedy School, à titre personnel): Merci.

Bonjour à tous.

Je m'appelle David Eaves, et je suis chargé de cours ici, à l'Université Harvard. J'enseigne la technologie au service des gouvernements et la transformation numérique à la Harvard Kennedy School. Cela dit, je suis né et j'ai grandi à Vancouver Quadra; je connais donc Mme Murray, qui est peut-être présente parmi vous. J'habitais dans sa circonscription jusqu'à il y a quelques années.

Je me penche également sur la question de la transformation depuis maintenant une quinzaine d'années, en plus de donner des conseils à ce sujet. En fait, j'ai déjà comparu à deux reprises devant votre comité pour parler des données ouvertes et de mon cadre pour les données ouvertes, l'information ouverte et le dialogue ouvert. Le tout a été, en quelque sorte, transposé dans le cadre stratégique qui, je crois, est encore largement utilisé pour assurer la transparence au sein du gouvernement.

Aujourd'hui, j'aimerais vous parler un peu de la transformation numérique et de ses répercussions sur la protection des renseignements personnels. Plus précisément, je m'intéresse aux questions de gouvernance et de confiance. Une chose que le président pourrait faire, s'il le souhaite... J'ai publié, aujourd'hui même, un article dans la revue *Policy Options* sur les leçons tirées de l'expérience estonienne. L'article porte sur des questions de gouvernance qui, à mon avis, sont particulièrement pressantes et qui doivent être abordées. Si le sujet vous intéresse, il vaudrait peut-être la peine de faire traduire ce texte pour que le Comité puisse le transmettre à tous ses membres.

Avant tout, je voudrais établir ce dont nous parlons réellement lorsque nous évoquons le cas de l'Estonie, en plus d'expliquer en quoi le modèle estonien est unique en son genre et digne de mention. Selon moi, il y a vraiment trois points que les membres du Comité doivent retenir au sujet des mesures prises par l'Estonie.

D'abord, elle a créé une série de ce que nous pourrions appeler des bases de données canoniques, dans lesquelles le gouvernement entrepose des renseignements sur ses citoyens — c'est-à-dire, leur lieu de résidence, leur numéro de permis de conduire, etc. Toutes ces données sont stockées dans des bases de données, mais elles sont conservées dans une seule base de données. Ainsi, il y a une base de données pour les adresses, une autre pour les permis de conduire, une autre pour quelque chose d'autre, et ainsi de suite.

Ensuite, les renseignements contenus dans ces bases de données sont reliés entre eux parce que chaque citoyen se voit attribuer un identifiant unique. Le numéro est lié à l'information versée dans les diverses bases de données, et il est donc facile d'extraire des éléments d'information disparates au sujet d'un citoyen et de les regrouper pour obtenir un portrait très clair de la personne, puis de transmettre ces renseignements aux différents organismes gouvernementaux à mesure qu'ils essaient d'offrir leurs services. C'est un modèle très différent de ce qu'on trouve dans la plupart des pays, dont le Canada, où ces bases de données ont tendance à fonctionner en vase clos, comme le disent mes collègues. Les renseignements sont stockés à plusieurs endroits. Ils ne sont pas partagés. Il est donc difficile d'obtenir une vue d'ensemble et de compiler tous les renseignements que l'on possède au sujet d'une personne, d'où la nécessité de les recueillir constamment.

Enfin, le troisième élément important, c'est que les Estoniens ont rassemblé les renseignements, les ont reliés aux individus au moyen d'identifiants uniques et ont rendu ces bases de données — ce que j'appelle l'« infrastructure de base » — accessibles à tout fonctionnaire dans l'ensemble des organismes gouvernementaux. Ils peuvent donc miser là-dessus pour créer de nouveaux services ou améliorer les services déjà offerts.

Ces trois innovations se trouvent, selon moi, au coeur même du sujet à l'étude et, à défaut de les comprendre, il sera très difficile de parler des innovations, des coûts ou des dangers qui nous attendent si nous voulons nous engager dans cette voie. J'aimerais d'abord expliquer au Comité en quoi consistent ces questions fondamentales.

Pourquoi est-ce important? Pour revenir un peu sur le point soulevé par le témoin avant moi, Amanda Clarke, une fois que cette infrastructure est en place, il est beaucoup plus facile d'innover et de créer de nouveaux services. Le gouvernement estonien fait une promesse essentielle à ses citoyens: il ne peut légalement demander qu'une seule information vous concernant, et ce, une seule fois. Si, disons, l'Agence du revenu Canada vous demande votre adresse, cela signifie que si vous allez au bureau des passeports, les agents auront votre adresse au dossier, et vous n'aurez pas à leur fournir l'information une fois de plus. L'avantage, c'est qu'au fur et à mesure que le gouvernement crée des services, il n'a plus besoin de recueillir et d'entreposer à nouveau tous ces renseignements. Les données se trouvent à un seul endroit, et vous pouvez les mettre à profit au moment de créer un nouveau service, sans devoir demander à les obtenir encore une fois et sans avoir à bâtir toute l'infrastructure liée à ce service pour stocker et gérer ces renseignements.

J'invite le Comité à se pencher sur trois questions clés.

Premièrement, en ce qui concerne la protection des renseignements personnels, j'aimerais que vous vous posiez au moins la question suivante: contre quel modèle de menace essayons-nous de nous protéger? Les gens ont principalement deux types de préoccupations à l'égard de la protection des renseignements personnels, surtout dans le contexte du gouvernement. D'abord, ils craignent qu'un acteur externe s'attaque au système et qu'il ait accès aux données personnelles que le gouvernement conserve. Il s'agit habituellement d'une puissance étrangère. Les gens ont peur qu'un tel acteur utilise ensuite ces renseignements pour miner le gouvernement ou peut-être même détruire la confiance dans les institutions gouvernementales et, par conséquent, amener les citoyens à refuser l'accès à l'information ou à ne pas faire confiance au gouvernement.

L'autre principale catégorie de menace à laquelle j'espère que vous consacrerez beaucoup de temps de réflexion, c'est le modèle de menace interne. À vrai dire, je suis beaucoup plus préoccupé par ce que mon propre gouvernement peut me faire que par ce qu'un gouvernement étranger pourrait me faire. Dans cet exemple précis, l'intervention d'un gouvernement peut varier, allant des activités de surveillance aux activités de portée relativement étroite.

● (1555)

Je suis particulièrement préoccupé par le fait que des ex-maris puissent utiliser leur accès à l'information gouvernementale pour trouver l'adresse de leur ex-conjointe et savoir ce qu'elles font. Ce sont des choses qui sont un peu partout, notamment dans les services de police, mais pas seulement là.

Même à petite échelle, ces choses se produisent et elles sont repérables. Les gens se souviendront peut-être que lorsque Rob Ford a été hospitalisé, ses dossiers de santé ont été examinés illégalement par plusieurs personnes qui avaient accès au système de l'hôpital. Or, il n'y a pas si longtemps, deux de ces personnes ont été accusées et mises à l'amende. D'une certaine façon, ce type d'accès, ce que vous pouvez faire avec les renseignements personnels d'une personne et la façon dont vous pouvez les faire circuler en tant qu'acteur interne m'inquiètent plus que ce qu'un intervenant externe peut faire. Il est très important de bien cibler l'objet de nos préoccupations.

Le deuxième élément, c'est que même si je suis préoccupé par les acteurs internes, cela ne veut pas dire que je veux leur imposer de tels fardeaux lorsque vient le temps pour eux d'utiliser ces types de systèmes ou d'y accéder. Permettez-moi de me faire l'écho des observations de Mme Clarke: l'amélioration de la sécurité peut être une bonne chose, mais si elle se fait au détriment de la convivialité, on se retrouve avec un système hautement sécurisé auquel personne ne peut avoir accès et que personne ne peut utiliser. Des étudiants qui travaillent ici, dans l'armée, me parlent du fait qu'en raison des importants dispositifs de sécurité qui leur sont imposés, il leur faut 45 minutes pour démarrer leur ordinateur portatif. À cause de cela, les gens évitent d'utiliser ces ordinateurs. Je ne suis pas sûr que nous voulons d'un système sécurisé au point de dissuader tout le monde de s'en servir.

Troisièmement, la protection des renseignements personnels n'est pas un absolu. Nous voulons un peu de flexibilité. Je ne veux peut-être pas que vous puissiez consulter mon dossier de santé, mais si je suis en train d'agoniser dans la rue, comme le dit mon collègue Jim Waldo, je serai hors de tout doute bien heureux que vous puissiez y accéder, et ce, même si je n'étais en état de vous en donner la permission. Nous avons besoin d'un système qui, tout en étant sûr, offre une certaine souplesse.

Mes principales recommandations à ce sujet sont... Avant même de commencer à se pencher sur la composante technique de leurs systèmes, les Estoniens ont fait beaucoup de travail pour adapter leurs lois sur la protection des renseignements personnels à la réalité du XXI^{e} siècle et, plus important encore, pour créer des systèmes de journaux et de vérifications afin que les citoyens puissent voir qui avait accès à leurs données, poser des questions sur la légitimité de ces accès et interpeller les autorités à cet égard.

La deuxième chose qui m'inquiète tout particulièrement, c'est le fait de déterminer si la mise en place de ce type d'infrastructure pourrait rompre le contrat social que le gouvernement a conclu avec ses citoyens. C'est peut-être un peu drôle à dire, mais la plupart des gens sont souvent très à l'aise de donner de l'information à leur gouvernement parce qu'ils croient que leur gouvernement n'a pas la capacité d'utiliser ces renseignements pour apprendre beaucoup de choses à leur sujet. Les gens sont disposés à donner des renseignements à l'État parce qu'ils ne pensent pas que le gouvernement a la compétence voulue pour faire des liens à partir de ces renseignements et ainsi créer un profil d'eux-mêmes.

Dans le type de monde que le gouvernement estonien a créé, ce n'est tout simplement plus vrai. La capacité du gouvernement de rassembler de l'information au sujet d'une personne et de vraiment comprendre l'ensemble de sa vie a été grandement améliorée. C'est le contexte et l'histoire très particuliers de l'Estonie qui ont fait en sorte que cela puisse se produire. Je ne sais pas tout à fait si l'on pourrait faire la même chose ici. J'encouragerais donc fortement le Comité à sonder la population canadienne afin de comprendre à quel point les gens seraient à l'aise de vivre ce genre d'expérience, et de cerner ce qu'ils veulent que le gouvernement sache à leur sujet et ce qu'ils veulent que le gouvernement soit en mesure de faire avec ces informations.

Selon moi, l'aspect particulièrement problématique de cet exercice sera sans doute le fait que les citoyens vous diront qu'ils veulent deux choses en même temps. Ils voudront que vous les traitiez comme le fait Amazon — nommément, que vous leur recommandiez de nouveaux services — et ils voudront des expériences personnalisées. Ils ne voudront pas avoir à redonner leurs renseignements encore et encore, mais ils diront: « Je vous défends d'utiliser mes données pour découvrir que je n'ai pas rempli correctement mes déclarations de revenus ou que je dois de l'argent au gouvernement pour telle ou telle autre raison, et je ne veux pas que vous envahissiez ma vie d'une façon qui pourrait me déplaire. » Je ne sais pas tout à fait s'il est possible d'avoir l'un sans l'autre. Or, advenant que ce soit possible, il va falloir réfléchir en long et en large sur les règles qui permettront d'en arriver là et d'encadrer cette pratique. Je ne pense pas que nous ayons même commencé à avoir la conversation publique qu'il faudra avoir pour interpeller et éduquer la population sur la façon d'en arriver là et pour évaluer son niveau d'aisance quant à la possibilité d'un tel avenir.

Enfin, je m'inquiète beaucoup de savoir qui va finir par construire — et surtout, par contrôler — cette infrastructure. Ces systèmes de base de données et les identificateurs uniques qui les accompagnent... J'ai récemment écrit un article sur un système similaire, en Inde, et je me suis demandé s'il y avait un moyen de construire cette infrastructure de manière à empêcher qu'un futur intervenant politique ou autre puisse en abuser, et la réponse courte est qu'il n'y en a pas. Il n'y aura pas de solution technologique aux types de problèmes de protection des renseignements personnels dont nous parlons. Il y a peut-être des technologies qui peuvent aider, mais en fin de compte, nous allons devoir compter sur des solutions de gouvernance. Quelle gouvernance faudra-t-il exercer pour protéger le public des intervenants actuels et futurs?

Pour ce qui est de l'avenir qui se présente à nous, je peux imaginer trois scénarios. Premièrement, nous pourrions décider que l'édification de cette infrastructure est tout simplement trop apeurante, et que nous ne sommes pas à l'aise avec un gouvernement qui en saurait autant à notre sujet.

Il y a un deuxième modèle, et c'est celui de procéder comme les Estoniens l'ont fait, c'est-à-dire en veillant à ce que le système soit bien réparti, de sorte que les différents ministères possèderaient différents éléments de l'infrastructure de base et qu'ils partageraient leurs bases de données avec d'autres ministères. Selon moi, ce qui est dangereux avec ce scénario, c'est que la gouvernance est en fait assez faible à certains égards. S'ils font quelque chose d'inapproprié, certains ministères pourraient être réticents à couper l'accès des autres ministères à leurs données, parce qu'ils craindraient des représailles de leur part.

● (1600)

Enfin, la troisième option serait peut-être de la construire afin qu'elle soit très centralisée, et de créer de nouveaux modèles de gouvernance autour de l'institution centrale.

J'ai presque fini, monsieur.

Le président: Allez-y, finissez.

M. David Eaves: Sauf qu'avec ce scénario, j'aurais peur qu'un intervenant unique se mette à contrôler l'ensemble de l'infrastructure et qu'il utilise cette mainmise pour exercer un contrôle sur d'autres secteurs de l'État afin d'empêcher ces derniers de lancer certains services ou de les forcer à concevoir des services qui feraient leur affaire plutôt que ceux que le Parlement ou le ministère voudrait offrir.

Ma recommandation ici serait de faire un examen approfondi des modèles de gouvernance qu'il sera nécessaire de mettre en place.

Je vais m'arrêter là. Je pourrai toujours répondre à vos questions.

Le président: C'est parfait. Merci beaucoup.

Nous allons commencer la première série de questions de sept minutes. M. Saini, vous avez la parole.

M. Raj Saini (Kitchener-Centre, Lib.): Bonjour à tous.

Monsieur Eaves, je vais commencer par vous parce que vous vivez dans la ville où je suis allé à l'école. Je suis allé à Northeastern, à Boston, alors commençons par vous.

Vous avez parlé du concept de l'État-plateforme. Laissons de côté la protection des renseignements personnels et examinons l'infrastructure de base, ce qui, à mon avis, est un bon moyen de reconnaître l'ampleur des ramifications réelles d'un tel exercice. Comme vous le savez, en tant que pays développé, nous n'avons pas la même latitude que l'Estonie qui, après avoir obtenu son indépendance, est virtuellement partie d'une feuille blanche. Dans une certaine mesure, une partie de l'Inde — cela peut varier selon l'endroit où vous poser les yeux — a aussi la chance de partir d'une feuille blanche. Mais nous sommes un pays avancé. Nous avons des systèmes de pointe, des systèmes qui sont en place depuis 20 ou 30 ans. Nous avons une certaine façon de faire les choses, certains protocoles.

Cependant, avec l'Estonie, nous avons affaire à un gouvernement unitaire et à une population d'à peine 1,3 million d'habitants. Au Canada, nous avons deux problèmes. Nous avons un partage interministériel de l'information et, en raison de notre fédéralisme, chaque ordre de gouvernement contrôle différents pans de l'information. En Estonie, il y a la route X qui traverse un palier de gouvernement unique avec des bases de données distinctes, mais ici, dans certains cas... Là d'où je viens — c'est la région de Waterloo —, nous avons quatre paliers de gouvernement: municipal, régional, provincial et fédéral.

En supposant que nous utilisions ce modèle estonien dans lequel toute l'information est répartie dans plusieurs bases de données plutôt que d'être conservée au même endroit — ce qui nécessiterait également un certain niveau de sécurité —, comment faudrait-il procéder, sachant que nous avons quatre paliers de gouvernement différents qui ont chacun leurs propres responsabilités fondamentales?

● (1605)

M. David Eaves: Toutes les contraintes que vous venez de mentionner... Les Estoniens travaillaient effectivement à partir d'une page blanche, ce qui signifie qu'il n'y avait pas d'infrastructure existante. Il est beaucoup plus facile de construire quelque chose à partir de rien que d'essayer de reconstruire un avion alors qu'il est en plein vol.

Pour y arriver, je crois qu'il faut être en mesure d'intervenir sur deux fronts à la fois. En fait, je pense que les défis techniques d'édification de cette infrastructure seront beaucoup moins grands que les défis en matière de gouvernance. Il est extrêmement difficile de trouver des moyens d'amener les gouvernements à s'entendre sur la façon de partager l'information et les données, alors nous aurions intérêt à rassembler dès maintenant les avocats dans une même salle, car il leur faudra probablement de très nombreuses années avant de trouver un terrain d'entente qui leur conviendra.

En fait, je parlais justement de cela aujourd'hui. Dans la débâcle de HealthCare.gov, pour ce site Web, les données dont les gens avaient besoin pour s'inscrire aux soins de santé aux États-Unis provenaient de 12 organismes différents au sein du gouvernement fédéral seulement. Je crois qu'il a fallu un an et demi pour négocier des ententes afin qu'il n'y ait qu'un seul service pour l'ensemble des intervenants du gouvernement fédéral, service dont la fonction allait être de regrouper les données dans un seul système pour la prestation d'un seul type de service. Alors, il vaudrait mieux commencer à penser à cela dès maintenant.

L'autre chose que je tiens à vous dire, c'est que si vous vous contentez de faire cela, vous n'y arriverez jamais. Il faut une fonction de coercition. Par exemple, il faudrait trouver le service essentiel qui, à votre avis, aurait le plus d'impact sur les Canadiens, celui dont la simplification aurait le plus d'intérêt pour la cause. Une fois ce service trouvé, il faudrait commencer sur-le-champ à circonscrire les données qu'il sera nécessaire d'obtenir des divers intervenants provinciaux, locaux, ministériels et fédéraux, et à intégrer ces données pour la mise au point d'un projet très pratique et très réel. Il ne faudrait pas être trop ambitieux. Vous devriez vous focaliser sur un seul service. Ce sera probablement une bonne façon d'en apprendre beaucoup sur ce que vous allez devoir faire.

M. Raj Saini: Ma deuxième question s'adresse au professeur Roy. D'autres nous ont dit que les données recueillies par le gouvernement ne devraient être utilisées que pour les raisons pour lesquelles elles sont recueillies. Je pense que l'idée que vous avez soumise était de limiter l'usage qui peut être fait des données. Lorsque nous examinons le modèle de l'Estonie, nous constatons qu'il s'agit d'un modèle avec un seul point d'entrée. Or, si nous instaurons ce système au Canada et que nous tentons de faire progresser l'idée d'un gouvernement numérique, il ne pourra y avoir de répétition continue de l'information.

Maintenant, la façon dont cela fonctionne en Estonie, c'est que vos renseignements de base — adresse, date de naissance, numéro d'assurance sociale ou autre — sont regroupés au même endroit et qu'ils sont acheminés là où il faut lorsque vous ouvrez une session. Encore une fois, je crois que ce concept de droit reconnu en Estonie est ce que l'on appelle le concept du guichet unique. Comment pouvons-nous faire cela ici? Comment allons-nous faire en sorte d'avoir le même effet? Le but du gouvernement numérique est de rendre les choses plus efficaces et plus faciles. Comment pouvons-nous mettre cela en place ici?

Considérons la complexité du pays. Reconnaissons que notre population est 20 ou 25 fois celle de l'Estonie. Dans d'autres domaines, nous sommes un pays avancé. Comment allons-nous pouvoir appliquer ce concept? Or, si nous n'avons pas ce concept de guichet unique, l'efficacité ne sera pas au rendez-vous et nous n'obtiendrons pas l'appui du public, ce qui est l'autre aspect dont vous avez tous parlé, je crois.

M. Jeffrey Roy: Je pense que c'est l'une des contradictions ou l'un des paradoxes les plus intéressants du gouvernement à l'heure actuelle, cette notion de protection des renseignements personnels et cette idée d'utiliser les renseignements uniquement pour la raison pour laquelle ils sont recueillis... Soyons clairs, cela entre en contradiction avec une bonne partie de ce que les gouvernements promettent de réaliser, nommément ces modèles de services qui seraient mieux intégrés et plus axés sur les citoyens. Il y a donc là une contradiction.

David Eaves pourrait certainement parler de l'Estonie beaucoup mieux que moi, mais avant la réunion, j'examinais certains travaux que le gouvernement australien a effectués durant la dernière année au sujet de la gouvernance des données. Les Australiens sont en train de préparer un nouveau cadre législatif pour répondre à la question que vous vous posez. À la fin de l'année dernière, ils ont publié un document de réflexion sur le partage et la réutilisation des données dans le secteur public et sur la façon dont cela pourrait fonctionner à partir d'un cadre de protection des renseignements personnels qui reconnaîtrait le besoin de limites et de transparence.

Pour être très concret — à tout le moins, à court ou à moyen terme —, il faudra qu'il y ait une clause d'exclusion pour que les gens aient le sentiment de ne pas participer. Je vais vous donner deux exemples. D'abord il y a eu ce qui s'est passé en Colombie-Britannique il y a plusieurs années lorsqu'a été lancée la nouvelle carte de services intégrés qui regroupait le permis de conduire et la carte d'assurance-maladie. En concertation avec le commissaire à la protection des renseignements personnels de cette province, nous avons décidé de permettre aux citoyens qui n'étaient pas à l'aise avec cette intégration de se retirer. Je crois qu'une petite minorité a choisi de le faire, et l'option existe encore aujourd'hui.

Le deuxième exemple concerne la santé numérique, plus particulièrement la nouvelle agence de santé qui a été mise sur pied en Australie afin de doter chaque citoyen d'un dossier de santé. Là aussi, très clairement, il y a une clause d'exclusion qui permet aux particuliers de faire retirer leur dossier numérique du système. Je ne sais pas s'ils peuvent le faire eux-mêmes ou s'il faut qu'ils présentent une demande par l'intermédiaire du système. Je présume que la création de ces nouveaux modèles devra se faire selon une approche progressive, mais il faudra qu'il y ait une certaine option de retrait.

Enfin, j'aimerais revenir à ce que j'ai dit plus tôt au sujet du travail de votre comité et de la nécessité d'avoir un débat public plus large sur le degré d'aisance des citoyens à l'égard du partage des données. En outre, il serait important de faire participer davantage les citoyens au débat en ayant, peut-être, des groupes consultatifs de citoyens, des comités de surveillance citoyenne, etc. Cela fournira un apport tangible à la compréhension des compromis et des solutions qui seront proposés dans les prochaines années.

● (1610)

M. Raj Saini: Merci.

Le président: Le prochain intervenant est M. Kent, qui dispose de sept minutes.

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

Je vous remercie tous de votre présence et des renseignements que vous nous communiquez aujourd'hui.

Madame Clarke, vous avez parlé de la nécessité de trouver un juste équilibre entre le rôle du secteur public et du secteur privé dans l'élaboration d'un gouvernement numérique efficace, que ce soit uniquement à l'échelle fédérale ou, ultérieurement, au niveau des autres paliers de gouvernement du Canada. Nous disposons de deux exemples. L'un d'eux est le système de paie Phénix qui a échoué ou qui est en voie d'échouer. Dans le cas de ce système, l'organisme d'approvisionnement avait éliminé certains des éléments complexes que le développeur d'applications numériques recommandait, afin que le système puisse se mettre au diapason des marchés et verser les salaires de façon efficace, et cela a abouti à la catastrophe que nous voyons aujourd'hui.

Par contre, il y a les Sidewalk Labs de Toronto, les petits frères de Google auxquels la ville a accordé tout le contrôle et permis de développer... dans le plus grand secret — un secret plus grand que bon nombre de Torontois et d'autorités numériques le souhaiteraient, à tel point que Jim Balsillie, un ancien dirigeant de BlackBerry, a déclaré ce qui suit: « [ce] n'est pas une ville intelligente. C'est une expérience de colonisation en matière de capitalisme de surveillance ».

Comment pouvons-nous trouver ce juste équilibre? Le gouvernement doit-il se renseigner davantage afin d'être un acheteur averti et un superviseur éclairé de la façon dont un service gouvernemental numérique devrait être développé et exploité?

Mme Amanda Clarke: Voilà une excellente question.

Je n'ai pas eu le temps de la soulever au cours de mon exposé. Je pense que, si vous mettez l'accent sur la question des services numériques, une grande partie de cette conversation doit porter sur la conception et la livraison des produits, ainsi que sur l'approvisionnement.

Je crois qu'il y a deux choses intéressantes qui se produisent en ce moment au chapitre de l'approvisionnement. Comme je l'ai mentionné au cours de mon exposé, l'une d'elles est qu'au début, un grand nombre d'enthousiastes de la numérisation des services gouvernementaux pensaient, en particulier à l'aube de l'ère des données ouvertes, que les gouvernements n'auraient plus à élaborer bon nombre de leurs services numériques. Ce modèle n'a pas fonctionné pour un certain nombre de raisons. L'une des plus importantes raisons était que les gouvernements allaient devoir continuer de développer bon nombre de leurs services de base, non seulement ceux axés sur la clientèle, mais aussi leurs systèmes internes comme les systèmes de paie ou les systèmes de messagerie électronique. En réponse à cela, nous avons observé, entre autres, un intéressant retour de l'État dans le secteur de l'approvisionnement, de sorte que nous voyons des chefs de file du domaine de la numérisation des services gouvernementaux investir beaucoup d'argent dans leur capacité interne afin de devenir des acheteurs avertis dans ce secteur.

Je dirais que l'exemple des Sidewalk Labs de Toronto et celui du système de paie Phénix découlent en partie d'un même problème. Dans le cas de Toronto, les membres du conseil d'administration de Waterfront Toronto — et dans le cas gouvernement du Canada, je suppose que ce serait les fonctionnaires de Travaux publics — n'étaient pas suffisamment compétents pour faire des choix judicieux à propos des systèmes dont ils avaient besoin.

L'autre phénomène intéressant, à mon avis, qui survient dans ce secteur, c'est la façon dont nous demandons initialement ce que le système doit nous fournir. Nous cessons de concevoir, en particulier, les services axés sur la clientèle en fonction des structures et des besoins internes du gouvernement. Au lieu, nous nous inspirons d'un domaine appelé la pensée conceptuelle pour mener dès le début des recherches approfondies sur les utilisateurs et la façon dont ils utiliseront le service. Ensuite, vous structurez tout approvisionnement ou toute conception de services que vous pourriez avoir à réaliser en fonction des résultats de ces recherches.

Un système comme Phénix aurait pu être évité de bien des façons en réalisant ce genre de recherche dès le début et en prenant conscience des aspects complexes du système et de ce dont vous aviez besoin. Ces essais par les utilisateurs vous permettent d'expérimenter sur une échelle réduite avant de signer un contrat à long terme — ce que nous appelons un contrat légué. Ces essais vous permettent souvent de prévoir les fonctions que le service numérique devra offrir avant même de l'essayer. Si vous examinez les grands échecs passés de la TI à l'échelle mondiale, vous verrez qu'ils découlent de ces contrats légués qui n'ont pas commencé par des essais à petite échelle menés par des utilisateurs. HealthCare.gov a été mentionné, par exemple.

● (1615)

L'hon. Peter Kent: Merci beaucoup, madame. Vos réponses étaient très instructives.

Monsieur Roy.

M. Jeffrey Roy: L'exemple des Sidewalk Labs est intéressant. Dans ce cas, je garde un peu plus l'espoir qu'avec davantage de transparence et de négociation ouverte, un cadre surgira qui équilibrera les intérêts publics et privés. Je pense qu'il sera très important à l'avenir de tirer des leçons des exemples de ce genre.

En plus des commentaires d'Amanda Clarke, il y a un autre point que j'aimerais faire valoir, et c'est le fait qu'un mécanisme doit être mis en place afin de faciliter le dialogue public dont nous parlons. Je sais qu'à l'heure actuelle, le gouvernement de l'Australie est en train de créer le nouveau poste de commissaire en chef des données et de nommer quelqu'un à ce poste. Je ne peux pas entrer dans les détails à ce sujet, alors je ne vais pas prétendre être un expert en la matière. Bien entendu, le gouvernement du Royaume-Uni compte déjà un dirigeant principal des données.

Aussi important que soit le rôle du commissaire à la protection de la vie privée — et je ne laisse nullement entendre qu'il devrait être réduit —, il doit y avoir un moyen d'envisager ces données comme un actif ouvert et de nouer un dialogue avec le public et les intervenants à propos des compromis qu'il convient de faire pour aller de l'avant. L'idée d'avoir quelqu'un — qui relève du pouvoir exécutif ou qui occupe un nouveau poste potentiellement indépendant — qui serait en mesure de sensibiliser davantage les citoyens pourrait être l'un des moyens de favoriser le dialogue public qui, nous en convenons tous, sera requis à l'avenir.

L'hon. Peter Kent: Monsieur Eaves.

M. David Eaves: Je vais simplement formuler deux observations.

Premièrement, je dirais que l'un des aspects qui rend ce sujet particulièrement complexe et que je tiens à ce que tout le monde comprenne dans la salle, c'est que nous parlons de passer de systèmes que nous qualifions d'intégrés verticalement, dans lesquels vous gérez des éléments comme des passeports, à un système au sommet duquel nous envisageons de combiner plusieurs niveaux de systèmes horizontaux qui vous permettront par la suite d'assurer rapidement la prestation de nouveaux services, de manière à ce que, par exemple, le service de délivrance des passeports puisse accéder à divers services intégrés horizontalement et extraire l'information nécessaire.

La raison pour laquelle je vous suis reconnaissant de votre question, monsieur Kent, c'est que je suis beaucoup plus préoccupé par la gouvernance de ces systèmes horizontaux. Le fait est que, si vous ne menez pas à bien la gouvernance d'un système intégré verticalement, cette erreur sera coûteuse — pour reprendre l'argument de Mme Clarke —, mais il sera possible d'y remédier à moyen — ou long — terme, et cela ne nuira pas à toutes les autres activités du gouvernement. Toutefois, si nous ne menons pas à bien la gouvernance de l'un de ces systèmes horizontaux, ce problème est en fait très grave, parce qu'il a une incidence sur tous les systèmes qui reposent sur lui.

Par conséquent, il est absolument impératif que votre comité réfléchisse longuement aux conséquences de cette approche sur la protection de la vie privée, la sécurité et la conception des systèmes, parce que cette approche a des effets secondaires sur la situation de tous les autres intervenants.

Je pense qu'il est très probable que certains de ces systèmes horizontaux appartiendront au secteur privé et seront maintenus par lui. Par exemple, il est peu probable qu'à long terme, le gouvernement canadien construise et maintienne son propre nuage. Il demandera probablement à un intervenant du secteur privé de le faire.

Alors, l'un des aspects qui pourraient devenir problématiques, c'est le fait que l'intervenant du secteur privé déterminera les investissements à faire, la façon d'élargir cette infrastructure, ainsi que les futures fonctions qu'elle offrira. Ces décisions restreindront le champ d'action du gouvernement du Canada et pourraient même être prises d'une façon qui limite notre capacité de choisir des concurrents lorsque nous souhaiterons développer d'autres systèmes plus tard.

Par conséquent, nous ferions mieux de perfectionner et nuancer notre compréhension des actions de ces intervenants, parce qu'ils pourraient décider de limiter nos options de certaines façons que nous ne percevrons pas immédiatement.

● (1620)

L'hon. Peter Kent: Merci.

Le président: Merci, monsieur Kent.

Le prochain intervenant est M. Angus, qui dispose de sept minutes.

M. Charlie Angus: Merci, monsieur le président.

Eh bien, j'ai en main mon téléphone gouvernemental, et je reçois constamment des messages qui m'indiquent que je dois invoquer telle ou telle fonction immédiatement. Lorsque j'essaie d'invoquer cette fonction, on m'informe que je ne suis pas autorisé à le faire parce que cette fonction ne reconnaîtra pas mon téléphone.

Tout cela est intéressant, mais ce n'est pas le sujet de discussion de notre comité. Nous sommes membres du comité responsable de la protection des renseignements personnels, de l'éthique et de la responsabilisation, et non du comité des opérations gouvernementales. Il y a de nombreuses choses géniales que nous pourrions entreprendre. Nous pourrions tenter de dire que nous offrons de meilleurs services gouvernementaux et, si nous croyons être en mesure de redresser la situation, je pense que c'est formidable. Cependant, la tâche de notre comité consiste à protéger les droits des citoyens, un point c'est tout.

Je suis un peu préoccupé, monsieur Eaves. Je vous ai peut-être mal entendu, mais citiez-vous Nora Young lorsque vous avez parlé du fait que les citoyens devaient défendre leurs données et que les gouvernements devaient contester le droit à la vie privée? Quelle était cette citation?

M. David Eaves: Je ne crois pas il s'agisse de moi, monsieur.

M. Charlie Angus: Je suis désolé.

Monsieur Roy.

M. Jeffrey Roy: Il s'agissait de moi.

La citation elle-même se limitait à la partie portant sur la « défense des données ». Elle ne laissait pas entendre que les citoyens doivent contester les actions des gouvernements. Je tiens simplement à être clair à ce sujet.

M. Charlie Angus: Vous avez dit quelque chose à propos du fait que les gouvernements devaient contester quelque chose.

M. Jeffrey Roy: Je soulignais le fait que, parfois, les gouvernements doivent restreindre le droit à la vie privée pour diverses raisons ou envisager d'imposer des limites à cet égard, que ce soit pour apporter des améliorations aux services ou pour les intégrer au chapitre de l'échange d'information, ou pour une foule de raisons liées à la sécurité, lorsque l'information est communiquée pour diverses raisons mettant l'accent sur la sécurité publique et des considérations de ce genre.

Je ne suggérais pas que les gouvernements ne respectent pas le droit à la vie privée. Je laissais simplement entendre que la protection des renseignements personnels est une considération que les gouvernements doivent concilier avec d'autres considérations. Nora Young faisait valoir surtout que les citoyens doivent faire preuve d'un certain sens des responsabilités à l'égard de la propriété de leurs propres données, et qu'ils doivent réfléchir à ce qui advient de ces données et faire de leur mieux pour le comprendre.

M. Charlie Angus: D'accord, merci.

Monsieur Eaves, j'ai été très intéressé de vous entendre dire que vous êtes plus préoccupé par ce que votre propre gouvernement fera de vos données. On nous dit constamment que les gens obtiennent des renseignements seulement à bon escient. Les agents de police obtiennent des données auprès des entreprises de télécommunications seulement parce que c'est important, mais ils le font encore et encore sans mandat, ce qui porte atteinte aux principes de base du système judiciaire.

Au Canada, nous rencontrons sans cesse des problèmes liés à la collecte de renseignements privés. Comment pouvons-nous protéger les droits des citoyens peut-être contre l'État tentaculaire ou peut-être contre des gens qui pensent que quelqu'un pourrait être un terroriste ou simplement une personne problématique? Ces gens ont la capacité de consulter toutes les données sans restriction.

Êtes-vous préoccupé par les limites qui s'imposent et par la façon de protéger les droits des citoyens?

M. David Eaves: Mon deuxième grand point était lié au fait de rompre le contrat social. Je pense que certaines personnes ne font pas confiance à l'État. Par conséquent, elles ne veulent communiquer aucune donnée. D'autres pensent que l'État est incompétent. Ils sont donc contents de fournir des données à l'État parce qu'ils ne croient pas qu'il soit capable de relier ces données pour en faire quelque chose d'intéressant. Enfin, d'autres personnes sont disposées à fournir des données, et n'y voient pas d'objection, parce qu'elles font confiance au gouvernement.

Je pense que le modèle dont nous parlons avec les Estoniens est tellement radicalement différent de ce que nous avons aujourd'hui que nous devons avoir une discussion très intentionnelle au sujet de l'aspect que pourrait prendre le nouveau contrat social. L'une des mesures que prennent les Estoniens et qui constituent, à mon avis, une part importante de ce contrat social, c'est le fait qu'ils tiennent un registre de toutes les personnes qui consultent vos données. Vous pouvez, en tout temps, ouvrir une session, examiner la liste des personnes qui ont jeté un coup d'œil à vos données, puis porter plainte. Vous pouvez demander pourquoi cet agent de police ou ce médecin examine ces données. Lorsque j'ai parlé au dirigeant principal de l'information de l'Estonie, il m'a dit qu'au début, ils ont poursuivi très agressivement certaines personnes qui examinaient des données qu'elles n'étaient pas censées examiner, afin de redéfinir la culture au sein du gouvernement à propos de la nature d'un comportement approprié.

J'ai l'impression que des activités de ce genre devront probablement être exercées dans notre environnement, mais il faudra qu'elles soient équilibrées par celles des services de police, qui voudront avoir accès à ces données, après avoir présenté un mandat légitime.

M. Charlie Angus: Bien sûr, cette demande serait accompagnée d'un mandat, le cas échéant. En ce qui concerne le gouvernement, des employés de l'ARC ont espionné les renseignements financiers de certaines personnes. S'il existe un mécanisme de protection qui nous permet en fait de voir que des données ont été consultées... Parfois, il se peut que ce soit légal — et s'il est légal de les examiner, alors c'est utile —, mais nous devons le savoir.

Toutefois, je suis préoccupé par ce que vous avez dit au sujet du développement de l'infrastructure. Est-ce qu'il sera public, ou privé? De plus, il y a la question des Sidewalk Labs et de Google. Google a été exclu des applications d'Apple, parce qu'il n'était pas possible de faire confiance à l'entreprise et parce qu'elle espionnait les gens. Et pourtant, nous allons lui confier l'infrastructure d'un important centre urbain. Comment pouvons-nous dire que, si des espaces publics existent, ils devront être...? Comment pouvons-nous faire confiance à Google? Je ne fais pas confiance à cette entreprise.

Amanda Clarke a demandé si elle pouvait répondre à cette question.

● (1625)

Mme Amanda Clarke: Je pense que vous avez raison de mentionner l'exemple des Sidewalk Labs à Toronto comme une situation que nous ne voudrions pas reproduire, mais il se peut que cette situation commence et s'arrête là. Je pense que l'un des enseignements que nous pouvons tirer de cette catastrophe, c'est justement le fait que votre comité et d'autres décideurs ne devraient pas planifier la participation d'intervenants privés dans la prestation de services numériques ou dans des projets de numérisation.

Je m'entends avec M. Eaves pour dire que non seulement des intervenants privés joueront invariablement un rôle dans les infrastructures et que nos gouvernements se fieront sur eux pour protéger les renseignements personnels, mais aussi qu'ils concevront des services, qu'ils assureront leur prestation et qu'ils géreront des données.

Je crois que la véritable question devient la suivante: comment pouvons-nous structurer ces marchés de manière à prévenir certains des problèmes que M. Eaves a exposés avec raison, à mon avis? Mais aussi...

M. Charlie Angus: Il me reste seulement une minute, alors je vais devoir vous interrompre ici.

Mme Amanda Clarke: Oui, bien sûr. Allez-y.

M. Charlie Angus: Pour ce qui est des données détenues par les Autochtones, je peux vous dire que j'ai travaillé pour un gouvernement des Premières Nations. Je leur disais sans cesse à quel point nous les apprécions et qu'ils pouvaient nous confier leurs données, par exemple sur leurs territoires de trappe et leurs sites sacrés, pour que nous les aidions à cartographier le tout. Ces données représentent le seul pouvoir entre les mains de la communauté, car le ministère des Affaires indiennes contrôle tout le reste. Les Autochtones ne vont donc pas simplement nous les remettre.

Comment pensez-vous que nous puissions discuter du droit des Autochtones à l'autonomie gouvernementale après 250 ans de mauvaise foi au Canada? Comment pouvons-nous interpeller une communauté autochtone pour discuter de la signification des données et de la façon de les protéger? Je crois que vous avez soulevé là un point très important.

Mme Amanda Clarke: Oui, je pense que ce sont toutes des questions cruciales. Comme je l'indiquais, ce n'est pas mon domaine d'expertise. L'organisme NordOuvert a accompli un travail vraiment intéressant auprès de communautés des Premières Nations en Colombie-Britannique. Il y a aussi des travaux très prometteurs qui ont été réalisés dans ce domaine en Nouvelle-Zélande. Je pense qu'il est vraiment essentiel de donner voix au chapitre aux Autochtones dans ce processus étant donné que, comme vous l'avez indiqué avec justesse, le pouvoir vient de l'information. C'est le cas pour ces communautés qui ont vu traditionnellement le gouvernement canadien ne pas utiliser ces données d'une manière susceptible d'améliorer leur sort, c'est le moins que l'on puisse dire. En toute franchise, je crois que nous pourrions trouver d'excellents exemples de cas où les données ont plutôt servi à marginaliser et oppresser les Autochtones. Cela s'inscrit dans un passé colonialiste structurellement violent. Il est donc vraiment primordial que l'on en débatte.

M. Charlie Angus: Merci.

Le président: Merci, monsieur Angus.

Nous écoutons maintenant M. Erskine-Smith.

M. Nathaniel Erskine-Smith: Merci beaucoup.

Je veux commencer par une mise en situation très simple. J'ai un numéro d'assurance sociale. Je me demande la plupart du temps à quoi cela peut me servir. Je vais maintenant choisir un mot de passe pour ce numéro d'assurance sociale, puis le gouvernement va me remettre une clé RSA avec code en rotation pour l'instauration d'un système d'identification à deux facteurs. Je peux d'ores et déjà accéder directement à l'Agence du revenu du Canada. Mon épouse peut utiliser le même système lorsqu'elle est en congé de maternité et veut obtenir de l'assurance-emploi. Lorsque je demande un nouveau mot de passe, c'est également ce système que j'utilise. Pourquoi faudrait-il compliquer les choses à ce point?

Monsieur Eaves.

M. David Eaves: Il faut se demander quelles sont les répercussions d'un tel choix.

Disons que votre numéro d'assurance sociale est actuellement votre identifiant unique. Vous allez devoir le fournir toutes les fois que le gouvernement obtient des informations à votre sujet, que ce soit à l'échelon fédéral, provincial ou local. Quelqu'un pourra se dire alors qu'il lui suffirait d'interroger différentes bases de données pour en tirer des renseignements vous concernant, identifiant à l'appui, et s'en servir pour créer un profil de vous qui pourrait avoir son utilité, mais dont il pourrait fort bien également se servir à mauvais escient.

M. Nathaniel Erskine-Smith: Excellent. C'est vraiment intéressant.

Poussons les choses un peu plus loin. On se retrouve avec un registre central de la population où figurent des renseignements de base, comme le nom, l'adresse, le numéro de téléphone et peut-être même l'adresse courriel. J'ose espérer que le gouvernement est capable de communiquer avec moi par courriel comme je le faisais avec mes clients. Soit dit en passant, il est étrange que je ne puisse pas obtenir les résultats de mes analyses sanguines par courriel alors même que je pouvais me servir de ce moyen pour transmettre des avis juridiques souvent confidentiels.

Il y a donc un registre de la population avec mes renseignements de base. À l'heure actuelle, mon numéro d'assurance sociale est la seule donnée à mon sujet dont disposent tous les ministères, en dehors de ce registre de la population. Il y a une couche de protection additionnelle qui fait en sorte que l'on ne sait rien de moi tant et aussi longtemps qu'il est impossible d'établir les liens nécessaires. Ainsi, les intervenants du système de santé peuvent connaître les résultats de mes analyses sanguines qui sont rattachées à mon numéro d'assurance sociale, mais pas à mon nom. S'ils ont besoin de connaître mon identité, ils doivent d'abord consulter le registre de la population. Il y a donc cette strate que nous ajoutons.

Nous avons ensuite une couche de sécurité supplémentaire qui nous vient de la Loi sur la protection des renseignements personnels ou de n'importe quel autre instrument de gouvernance que nous souhaitons adopter pour régir les demandes de renseignements entre les différentes bases de données. Ce sont donc les éléments constituants du système et, si nous parvenons à superposer adéquatement ces couches de protection, nous pouvons raisonnablement nous attendre à ce que le système fonctionne bien.

● (1630)

M. David Eaves: Je suis d'accord.

Je suis un peu déchiré. C'est un sujet qui me passionne, car c'est la vision d'avenir que je veux partager avec mes étudiants. C'est le résultat que nous cherchons à atteindre. Tous les éléments que j'aborde avec vous aujourd'hui viennent avec leur lot de questionnements.

Qu'adviendra-t-il si nous parvenons à nos fins? Comment les choses se passeront-elles dans ce nouveau monde que nous cherchons à créer? Sur quels éléments devons-nous axer notre réflexion en vue d'atténuer d'éventuelles répercussions néfastes?

Je vous dirais que vous comme moi ne faisons pas partie des gens ayant eu à subir les formes les plus extrêmes de violence qu'un État peut exercer à l'encontre d'un individu. Si vous aviez toujours vu l'État comme une entité hostile et peu accommodante, vous seriez sans doute profondément inquiets à l'idée d'un État tout-puissant capable d'utiliser ces renseignements à votre détriment.

M. Nathaniel Erskine-Smith: Oui, je comprends.

Dans votre article, vous énoncez quatre préoccupations. La première concerne le contrat social. Supposons que ce système est déployé à grande échelle — si l'on en arrivait éventuellement à cela — sur une base volontaire dans un premier temps. Quelqu'un comme vous ou moi ayant assez confiance pour tout au moins faire l'essai du système peut choisir de le faire, et ceux qui sont trop inquiets n'y sont pas obligés.

Est-ce que l'on ne pourrait pas respecter ainsi le contrat social, tout au moins au départ?

M. David Eaves: Peut-être au départ, mais il y a deux préoccupations qui en découleraient à mon sens.

Il y a d'abord le fait que les gens les plus susceptibles d'avoir besoin de l'aide de l'État sont généralement ceux qui risquent le plus d'être marginalisés. Je peux très bien m'imaginer un système à deux vitesses où les mieux nantis, qui n'ont pas vraiment affaire régulièrement avec l'État, se retrouvent à lui transmettre très peu d'information et à donc être moins bien connus du gouvernement, alors que les plus nécessiteux et ceux qui sont marginalisés doivent communiquer à l'État de grande quantité de données. L'État se retrouve ainsi en position d'exercer une surveillance soutenue sur ceux-là mêmes qui sont les moins aptes à se protéger.

M. Nathaniel Erskine-Smith: Si c'est facultatif, alors c'est le statu quo pour ceux qui ne font pas confiance au système, et le gouvernement doit encore composer avec les difficultés déjà existantes quant à la gestion des données. Ces problèmes ne sont pas nouveaux pour les gouvernements. Il y a effectivement des échanges de renseignements entre les différentes agences d'un gouvernement. Il y a des mécanismes prévus à cette fin dans la Loi sur la protection des renseignements personnels ainsi que dans la Loi sur la communication d'information ayant trait à la sécurité du Canada.

Qu'est-ce qui change lorsque l'on passe au numérique?

M. David Eaves: Bien des choses changent. Il est notamment possible de prendre des mesures d'une portée beaucoup plus vaste.

Les données sont peut-être déjà numériques, mais pour que l'on puisse échanger de l'information entre les ministères afin de savoir exactement qui est David Eaves et déterminer quels fichiers concernent ce David Eaves-ci, plutôt qu'un autre David Eaves, il faut que quelqu'un ait la motivation d'assembler toutes les pièces du puzzle. En revanche, dans un monde où tout est relié à un identifiant unique permettant de déterminer avec exactitude à qui se rapportent tous les renseignements à notre disposition, je peux faire la même chose à très grande échelle. Je peux même le faire simultanément pour les 33 millions de Canadiens.

On pourrait peut-être intégrer à cela un algorithme d'apprentissage automatique pour savoir quels services sont offerts à qui et déterminer par exemple qui est musulman et qui est chrétien. Toutes ces choses deviendraient possibles dans ce monde nouveau qui n'a rien à voir avec celui que nous connaissons actuellement.

J'ai la ferme conviction que nous devons faire la transition vers cet idéal-là, mais je veux vraiment que nous déterminions au préalable quels sont les modèles de gouvernance requis.

M. Nathaniel Erskine-Smith: Vous avez raison.

Je suppose qu'il faut alors s'interroger au sujet du modèle de gouvernance déjà en place. On nous a répété à maintes reprises qu'il n'était pas à la hauteur pour l'application de la Loi sur la protection des renseignements personnels. Reste quand même que c'est le modèle de gouvernance que nous avons pour l'instant.

Est-ce que le cadre en place est déficient à ce point? Il permet déjà de régir les échanges de données entre les institutions. Du simple fait que l'on autorise maintenant les interactions entre ces différentes instances, en présumant que le registre de la population pourrait servir de point de départ, cela ne m'apparaît pas trop inquiétant, car ces organismes ont toute l'information en main et qu'il deviendra ainsi plus facile d'avoir accès à leurs services.

Même en supposant au départ que l'on ne mette pas à jour la Loi sur la protection des renseignements personnels — bien que je sois d'avis que nous devrions revenir à la charge avec des recommandations en ce sens —, je ne comprends pas vraiment en quoi le défi en matière de gouvernance est différent, car nous disposons déjà d'un cadre à cette fin, soit la Loi sur la protection des renseignements personnels.

M. David Eaves: Je m'inquiète du fait que la Loi sur la protection des renseignements personnels dans sa forme actuelle entrave certains types d'activités et d'innovations qui seraient souhaitables, sans pour autant nécessairement empêcher d'autres types d'activités qui le seraient moins. C'est ce qui me préoccupe quant aux dispositions actuelles de cette loi. Je ne crois pas qu'elle soit vraiment déficiente, mais j'estime qu'une certaine forme de révision s'impose sans doute.

Il faut se demander, chose plus importante encore, dans quelle mesure la population a véritablement son mot à dire? Même suivant un régime facultatif... C'est ce que l'on a fait en Inde où l'identifiant unique était en théorie optionnel. Cependant, la solution de repli pour ceux qui choisissaient de ne pas utiliser l'identifiant unique était si déficiente quant aux services accessibles que tout le monde a finalement adhéré au système. On peut alors se demander si les gens y adhèrent parce qu'ils sont heureux de transmettre ces renseignements au gouvernement et qu'ils croient que celui-ci va s'en servir en toute bonne foi, ou s'ils ont plutôt en fait l'impression de ne pas vraiment avoir le choix étant donné toutes les tracasseries auxquelles ils s'exposent. Je pense qu'il faut vraiment prendre le temps de tirer les choses au clair à ce sujet.

Le président: Merci, monsieur Erskine-Smith.

Je veux juste indiquer à Mme Clarke qu'elle ne doit pas hésiter à ajouter son grain de sel. Il revient à chaque membre du Comité de décider à qui il adresse ses questions, mais vous pouvez très bien intervenir sans avoir été interpellée si vous avez un complément d'information à fournir.

● (1635)

Mme Amanda Clarke: Très bien.

Je voulais seulement...

Le président: Sauf que nous n'avons plus de temps pour l'instant...

Des voix : Ah, ah!

Le président : Nous passons à M. Gourde pour les cinq prochaines minutes, et peut-être aurez-vous la chance de vous exprimer à nouveau.

À vous la parole.

[*Français*]

M. Jacques Gourde (Lévis—Lotbinière, PCC): Cela va me faire plaisir, monsieur le président.

Ma question s'adresse à Mme Clarke.

Au Canada, des services numériques sont présentement offerts dans chaque ministère, et ils sont en constante évolution.

Le projet de redéfinir les services numériques destinés aux Canadiens suppose soit de sauvegarder ce qui existe, soit de jeter le bébé avec l'eau du bain.

À qui cela servira-t-il? Le projet profitera-t-il aux Canadiens ou au gouvernement, qui pourra donner plus de services? Permettra-t-il de favoriser l'interconnexion entre certains ministères? Les Canadiens souhaitent-ils que les ministères se parlent entre eux sur leurs dossiers, s'ils ne l'ont pas demandé?

Aucun citoyen dans ma circonscription n'est venu me voir pour me dire qu'il voulait qu'un représentant de l'Agence du revenu du Canada communique avec quelqu'un du ministère de la Citoyenneté et de l'Immigration, par exemple. Personne ne le demande, et je n'ai pas l'impression que les Canadiens ont demandé au gouvernement de redéfinir l'ensemble du numérique au Canada. Il ne faut pas se le cacher, si nous nous penchons à nouveau sur le numérique, il ne sera pas question de millions, mais bien de milliards de dollars au chapitre des dépenses. Le projet va durer très longtemps; en fait il ne sera jamais fini.

Selon vous, madame Clarke, qui tirera le plus de bénéfices du projet de redéfinir ou de recommencer le monde numérique au Canada?

[*Traduction*]

Mme Amanda Clarke: C'est une excellente question. On s'est déjà interrogé à maintes reprises sur les désirs véritables des citoyens. Je ne crois pas que nous disposions vraiment de données probantes à ce sujet pour l'instant.

Il y a deux éléments à considérer pour répondre directement à votre question : « Est-ce que c'est ce que les gens veulent? » Dans un premier temps, il arrive parfois que les gens ne sachent pas ce qu'ils veulent vraiment jusqu'à ce que... Ils ne sont pas conscients de l'ampleur des améliorations qui pourraient être apportées. Vos commettants ne demandent pas nécessairement que l'on aille de l'avant, mais si on leur démontrait comment il deviendrait facile de formuler une demande de service avec la saisie automatique de tous les renseignements personnels, ou à quel point l'organisation des services en fonction de ce que l'on appelle les événements de la vie pourrait faciliter leurs interactions avec l'État, ils seraient sans doute beaucoup plus favorables aux transformations qui sont envisagées en matière de gouvernance des données.

Certains se demandent peut-être ce que l'on entend par organisation des services en fonction des événements de la vie. Le gouvernement du Canada déploie des efforts en ce sens depuis un bon moment déjà. On vous a peut-être dit qu'il fut une époque où nous étions en quelque sorte un modèle à suivre en matière de gouvernement électronique. C'était le fruit du travail que nous avons accompli au départ en suivant les mêmes principes qui inspirent maintenant l'Estonie, c'est-à-dire que les citoyens qui interagissent avec l'État ne sont pas intéressés à savoir quel ministère fait quoi. Ils ne veulent pas être obligés de visiter toute une série de sites Web isolés. Ils s'adressent au gouvernement parce qu'ils viennent d'avoir un bébé et se demandent quelles sont les mesures à prendre en pareil cas.

Ils ne se demandent pas non plus à quel ordre de gouvernement ils ont affaire, et bien souvent ne comprennent pas qui est responsable de quoi, ce qui peut grandement compliquer les interactions avec l'État. Je crois que la mise en place du modèle horizontal d'une plateforme gouvernementale doit débuter par une évaluation des besoins des utilisateurs. C'est l'élément moteur indispensable, comme en témoigne l'expérience des gouvernements qui ont pavé la voie en ce sens.

En définitive, c'est purement une question d'optimisation du temps et des ressources. Il ne faut pas que les transactions avec l'État traînent en longueur. Dans une perspective plus générale, il en découle des répercussions sur le plan démocratique, car les gens dont les interactions avec l'État ne se déroulent pas bien en viennent à se demander à quoi servent leurs impôts. On se demande pourquoi toute cette bureaucratie et s'il n'y en a pas certains qui profitent de l'assiette au beurre, et le gouvernement ne manque pas alors d'affirmer qu'il va faire le nécessaire pour corriger toutes les lacunes.

Les critiques semblables reposent dans bien des cas sur une expérience très personnelle de mauvaises relations avec l'État. J'ai entendu de nombreux Canadiens y aller du même commentaire « Phénix est une véritable catastrophe. S'ils ne sont même pas capables de gérer un système de paye, comment peut-on leur faire confiance pour lutter contre les changements climatiques, appliquer une tarification sur le carbone, gérer les prestations pour enfants ou administrer le système scolaire? » La liste est longue, et je crois qu'il faut faire bien attention de ne pas négliger les enjeux plus globaux que cela fait intervenir.

Je conviens avec M. Angus qu'il y a une certaine zone grise quant au domaine de compétence et au mandat de votre comité qui s'intéresse à la protection des renseignements personnels et à l'éthique, et ceux d'autres comités qui se préoccupent davantage des opérations gouvernementales. Je crois que cela va exactement dans le sens de ce que nous avancions, à savoir que les enjeux stratégiques ne sont pas imperméables. À bien des égards, il y a un cloisonnement plutôt problématique entre les comités parlementaires. Les décisions que vous prenez et les recommandations que vous formulez en matière de protection de la vie privée ont de lourdes répercussions sur notre capacité à bien structurer et à bien gérer les services et les opérations du gouvernement. L'objectif ultime qui rallie le travail du comité des opérations gouvernementales, par exemple, et le vôtre, est la prestation de services gouvernementaux sur lesquels les Canadiens peuvent compter et qui alimentent une pleine confiance envers l'État.

Je suis donc assurément d'avis que vos commettants pourraient se réjouir grandement d'une telle avancée, et ce, même s'ils n'en font pas expressément la demande.

● (1640)

Le président: Merci. C'est tout le temps que vous aviez.

Les cinq prochaines minutes seront partagées entre Mme Vandenbeld et M. Picard.

Mme Anita Vandenbeld (Ottawa-Ouest—Nepean, Lib.): Merci. Je serai brève.

Ma question s'adresse à Mme Clarke. Je veux vous dire d'abord et avant tout que je me réjouis de pouvoir compter sur une expertise comme la vôtre ici même à Ottawa, soit à l'Université Carleton.

En ma qualité de députée représentant un grand nombre de fonctionnaires, je suis un peu inquiète de vous entendre dire que certains d'entre eux ne peuvent pas télécharger des outils pour leur travail, accéder à des sites Web ou même à un réseau sans fil. J'aimerais en savoir plus long à ce sujet. Est-ce une façon de faire qui est très répandue?

J'ai une autre question à vous poser. Vous avez étudié au Royaume-Uni et vous avez mentionné au départ les démocraties s'inspirant du modèle de Westminster. Est-ce que cette forme de gouvernement influe sur notre capacité à gérer une démocratie numérique?

Mme Amanda Clarke: Pour ce qui est du modèle de Westminster, je dirais que les tensions qui risquent le plus de se manifester découlent de l'opposition entre les structures verticales de reddition de comptes et ce modèle horizontal de plateforme gouvernementale, comme celui de l'Estonie, que nous préconisons de plus en plus.

Dans notre régime actuel, les éloges comme les reproches sont gérés suivant le concept de la responsabilité ministérielle. Lorsqu'un service offert est inadéquat ou que des fonds sont dépensés de façon irresponsable, c'est le ou la ministre qui doit rendre des comptes. Ce sont les ministres qui répondent aux questions à la Chambre des communes. D'un point de vue strictement pratique et concret, qui sera responsable devant le Parlement lorsque l'un de ces systèmes horizontaux faillira à la tâche?

Je veux qu'une chose soit bien claire. Il y a des façons de surmonter des difficultés semblables et le modèle de Westminster a l'avantage d'être intrinsèquement évolutif. Il est conçu pour pouvoir s'adapter aux réalités qui changent. Je pense que nous devrions nous pencher sérieusement sur ce que l'on appelle les modèles de responsabilisation horizontale ou de responsabilisation partagée. Ces enjeux étaient au coeur de nos discussions d'aujourd'hui. Ce n'est pas tant une question technique qu'une question de gouvernance. Il s'agit d'établir à l'avance quelles composantes du pouvoir bureaucratique et, en définitive, quels ministres seront responsables du déploiement de ces systèmes. Je crains fort que le modèle de gouvernance en plateforme ait suscité jusqu'à maintenant beaucoup d'enthousiasme sans que l'on tienne vraiment compte de cet aspect, notamment du fait que l'on s'est souvent contenté de réaliser des projets pilotes pour voir si cela pourrait fonctionner. Il faudra réfléchir à ces questions si l'on veut déployer le tout à plus grande échelle.

J'estime par ailleurs que vous devriez vous intéresser non seulement à la question de la responsabilité ministérielle, mais aussi aux enjeux liés à la gestion des données. Quelqu'un a demandé précédemment si la Loi sur la protection des renseignements personnels pouvait servir à cette fin. C'est effectivement l'un des outils que nous devons considérer pour régler toutes ces questions liées à la gestion des données, mais ce n'est pas le seul, et la loi n'offre pas un grand nombre de solutions.

M. Erskine-Smith a évoqué la possibilité de combiner toutes ces données afin d'offrir des services taillés sur mesure de telle sorte que l'on pourrait par exemple dire à quelqu'un: « Nous savons que vous avez eu un bébé. Vous êtes maintenant admissible à tel ou tel crédit d'impôt. » Il s'ensuit des préoccupations quant à la protection de la vie privée, mais il convient également de se demander comment on peut combiner ces données, si les citoyens veulent vraiment que l'État communique directement avec eux, et dans quelle mesure ils souhaitent que les différents ministères puissent avoir accès à ces renseignements. La protection de la vie privée est l'un des éléments à prendre en compte, mais il y a toute une série d'autres considérations qui entrent en jeu, notamment quant à savoir si l'on ne favorise pas ainsi certains groupes au détriment d'autres groupes.

Il faut encore là tenir compte de la perméabilité entre ces enjeux. C'est une question de protection de la vie privée, mais il faudra peut-être également concevoir des régimes entièrement nouveaux, pas nécessairement fondés sur la loi, mais plutôt sur les principes à respecter pour l'utilisation des données. C'est d'ailleurs la raison pour laquelle je soulignais le travail accompli dans le domaine de l'intelligence artificielle. C'est un excellent exemple d'un gouvernement fédéral qui se montre vraiment progressiste et ouvert à discuter de quelques-unes des questions éthiques très concrètes qui vont se poser lorsque l'intelligence artificielle sera utilisée pour l'élaboration des politiques. On peut faire la même chose pour bon nombre des considérations dont il est question ici.

M. Michel Picard (Montarville, Lib.): Merci.

J'entends parler de ce modèle estonien depuis des semaines. Qui y a travaillé, qui l'a mis à l'essai et sur quoi vous fondez-vous pour appuyer ce modèle? Votre enthousiasme me semble exagéré. Ma question s'adresse à tout le monde.

● (1645)

Mme Amanda Clarke: David, vous avez écrit l'article, alors je vais vous laisser aller au front.

Des voix: Oh, oh!

M. David Eaves: Le modèle estonien est apparu après que les Soviétiques ont quitté l'Estonie. Les Estoniens n'avaient que très peu de services et de processus opérationnels en place, presque aucune infrastructure, et ils devaient construire un État à partir de rien.

Je crois que les Estoniens ont été chanceux, parce qu'ils ont commencé à bâtir au moment où le Web faisait son apparition. Plutôt que de simplement tenter de reproduire les services étatiques des autres types de gouvernement, ils ont examiné la façon dont les informaticiens créaient les logiciels sur le Web — des systèmes d'exploitation répartis associés à des ensembles de données classiques — et ont voulu faire les choses différemment. Ils n'avaient pas le choix, puisqu'ils n'avaient que très peu d'argent; ils ne pouvaient pas se permettre de reproduire tous ces systèmes dans chaque ministère.

C'était à un moment précis dans le temps. Le leader du pays était assez jeune et a offert une couverture politique à ceux qui voulaient faire les choses autrement. Ce sont les causes historiques qui expliquent ce qu'ont fait les Estoniens. L'une des raisons pour lesquelles je crois que ce modèle vaut vraiment la peine d'être étudié — mais qu'on ne devrait probablement pas tenter de reproduire —, c'est que la situation du pays était tout à fait unique.

Le président: Merci, monsieur Picard.

La parole est maintenant à M. Kent. Vous disposez de cinq minutes.

L'hon. Peter Kent: Nous vous remercions de votre réponse, monsieur Eaves.

J'aimerais revenir à la question des modèles de menace. Plus tôt cette semaine, vous avez peut-être remarqué en lisant les bleus que Chris Vickery parlait du modèle estonien et de l'énoncé qui se trouvait sur le site Web du pays. On voulait se faire rassurant en disant que le site... n'avait été piraté qu'une seule fois. La Russie avait fait une tentative importante de pénétrer le système du pays en 2007. M. Vickery était convaincu qu'il était possible de pirater le système. Nous en avons ensuite discuté hors champ et nous avons pensé lui demander de faire une tentative de piratage en temps réel alors que nous le regarderions à partir d'Ottawa.

Que pensez-vous de l'évolution constante des modèles de menace? La menace nationale est peut-être plus importante, comme vous l'avez dit, pour la protection des renseignements personnels, mais nous savons que les gouvernements de la Russie et de la Chine travaillent constamment à pénétrer les systèmes gouvernementaux. Peu importe le nouveau système qui sera mis sur pied, il est presque certain — M. Vickery était fort convaincant à ce sujet — que quelqu'un trouvera une façon de le pirater.

M. David Eaves: Pour moi, il n'y a pas vraiment grand choix. Les acteurs étrangers s'intéressent déjà beaucoup à nos systèmes et ils les ont déjà pénétrés au cours de l'histoire. Je crois qu'il y a cinq, six ou sept ans, le système du Conseil du Trésor a été gravement compromis, au point où on a dû jeter la presque totalité des ordinateurs du ministère.

Je veux être clair. Ce n'est pas comme si le système actuel était sécuritaire et que nous voulions passer à un nouveau système non sécuritaire. Il faut penser aux types de menaces et à ce qu'ils signifient pour nous.

L'un des avantages du modèle actuel, c'est qu'en étant désorganisé pour nous, il l'est aussi pour un pirate. Donc, il risque de pénétrer un seul système et de ne pas voir grand-chose. Or, dans un système où il est très facile de trouver mon identifiant unique et où les liens sont plus importants, alors le pirate pourrait obtenir plus de renseignements, ce qui représente un nouveau type de menace.

En revanche, ce système peut être plus facile à défendre. À l'heure actuelle, la protection de vos renseignements repose sur la plus faible des bases de données dans lesquelles ils se trouvent, s'ils sont dans cinq bases de données différentes, par exemple. En Amérique, c'est Equifax ou d'autres bases de données de piètre qualité qui sont utilisées à grande échelle. Le regroupement nous permettrait peut-être de réunir nos ressources en matière de défense et de les concentrer.

Mais il y a des risques réels associés à cela également.

L'hon. Peter Kent: Monsieur Roy, qu'en pensez-vous?

M. Jeffrey Roy: Pour moi, c'est une question de résilience et d'ouverture. Si l'on revient au modèle estonien — et je comprends que vous commencez à être tannés d'en entendre parler —, lorsque le pays a décidé de passer au vote électronique, le gouvernement a utilisé un code source libre et a mis les gens au défi d'y trouver des failles. Un groupe de chercheurs en a trouvé et les a publiées en ligne. Mais cela n'a pas ébranlé la confiance des Estoniens; ils ont continué d'utiliser le vote électronique. On a simplement apporté certaines corrections. Pensons à ce qui s'est passé avec Apple la semaine dernière, nonobstant sa critique justifiée à l'égard de Facebook et de Google, comme l'a fait valoir M. Angus... Il y a eu atteinte à la confidentialité avec l'application FaceTime et la société a dû s'excuser.

En règle générale, et surtout en ce qui a trait aux architectures de TI, les gouvernements tendent à se centrer sur eux-mêmes, à utiliser des systèmes et des contrôles exclusifs pour minimiser les possibilités d'atteinte à la confidentialité et éviter que des renseignements ne soient divulgués. Toutefois, je crois qu'il faudrait plutôt regarder vers l'extérieur et être plus ouverts au sujet de nos vulnérabilités, et songer à la façon de les aborder de manière collective pour nous adapter et pour accroître la résilience de nos systèmes, sur le plan technique et sur le plan social, pour l'avenir.

● (1650)

L'hon. Peter Kent: Madame Clarke, nous avons le temps pour...

Mme Amanda Clarke: Je crois que c'est un excellent point, et j'abonde dans ce sens. Il faut qu'il y ait une confiance à l'égard du système pour que tout cela fonctionne. Ainsi, les gens auront aussi une certaine tolérance face à l'échec. Je ne dis pas que les gens vont laisser passer les atteintes importantes à la protection des données sans broncher ou en gardant le sourire. Ce que disent toujours les représentants des gouvernements qui innovent sur le plan numérique, c'est qu'on leur permet d'innover. La population est sûre que l'État a ses intérêts à coeur, qu'il sera ouvert et honnête au sujet des erreurs qui pourront se produire, et qu'il a les systèmes appropriés en place pour gérer ces erreurs afin qu'elles ne se répandent pas à grande échelle.

Je ne crois pas que nous ayons cette culture ici au Canada. L'un des témoins précédents — je crois que c'était M. Fishenden — a fait valoir qu'on pouvait mettre en place un nouvel organisme de surveillance non gouvernemental pour améliorer la culture de la confidentialité et de la reddition de comptes. Je ne suis pas du tout d'accord avec cela. Selon la tradition — et surtout au sein du gouvernement fédéral —, lorsqu'il y a des enjeux en matière de reddition de comptes, nous avons tendance à accroître la surveillance, à renforcer les règles et à imposer des sanctions verticales.

Ainsi, dans la fonction publique, on a une peur bleue d'essayer quelque chose de nouveau ou de différent parce que s'il y a un problème, la réaction sera si brutale qu'il faudra mentir et que de toute façon, il vaut mieux ne rien faire. C'est très frustrant pour les employés qui tentent de faire les choses autrement, mais cela met aussi un frein à l'innovation, qui repose souvent sur le travail des fonctionnaires. Il y aura un leadership parlementaire et les ministres devront l'appuyer, mais ce sont les fonctionnaires qui feront le travail ingrat si nous nous dirigeons vers ce type de modèle.

Je crois qu'un modèle qui se centre sur la responsabilité à des fins d'apprentissage pourrait permettre d'établir une culture gouvernementale qui respecte la confidentialité, mais qui nous permet aussi d'être plus novateurs dans nos services.

Oui, je crois que nous en avons besoin.

L'hon. Peter Kent: Merci, madame Clarke.

Le président: Le dernier intervenant est M. Sikand. Vous disposez de cinq minutes.

M. Gagan Sikand (Mississauga—Streetsville, Lib.): Merci.

J'aimerais tout d'abord remercier Mme Clarke pour son travail à la Bibliothèque du Parlement. Je suis le coprésident du comité BILI et nous parlons toujours de numérisation. Donc, merci.

J'aimerais vous faire part des réflexions que j'ai eues alors que j'écoutais vos témoignages. Vous pourrez les commenter ensuite.

Au départ, j'ai pensé à 1984, puis j'ai pensé à notre contrat social. J'ai pensé à ce qui se passerait si, comme l'Estonie, nous ne pouvions demander les données qu'une seule fois... D'accord, les données sont là, mais les gouvernements changent. J'ai pensé aux conséquences de cela. Si l'on va plus loin et qu'il y a une catastrophe naturelle, que les serveurs sont détruits, est-ce que le gouvernement sera, lui aussi, anéanti? Il y a les conséquences juridiques aussi, s'il faut redemander les renseignements; en Estonie, c'est impossible.

J'ai ensuite pensé aux attaques étrangères. Encore une fois, si un cheval de Troie éliminait les renseignements et que nous devions constamment transmettre nos données... Je pense aux répercussions sur la protection des renseignements personnels.

J'ai aussi pensé à Amazon, qui a ses propres serveurs et algorithmes. On se demande si le système sera public ou si le gouvernement devrait stocker ses données dans un nuage. L'Internet progresse, alors est-ce qu'on doit mettre des ressources là-dessus, dans les infrastructures?

Je me suis alors dit: « D'accord, si l'on passe au privé, qu'il y a des élections et que le gouvernement change, qu'on peut maintenant suivre les gens... » Quelqu'un a parlé de cela.

Après toutes ces réflexions, voici ma question: si nous réalisons une analyse coûts-avantages, allons-nous conclure qu'il faut passer au numérique?

Faites-moi part de vos idées.

● (1655)

M. Jeffrey Roy: J'aimerais commencer, si vous me le permettez. Pour revenir à la question des fournisseurs infonuagiques et d'Amazon, je crois que l'ancien gouvernement de l'Ontario avait commencé à impartir un certain nombre de ses serveurs de base de données aux services Web d'Amazon. Sur le plan de la confidentialité et de la sécurité, je crois qu'il est beaucoup trop ambitieux de vouloir que le secteur public crée les bases de données de l'avenir. Il est évident que Services partagés Canada a connu des difficultés. Ce n'est pas un secret. De nombreux problèmes sont survenus. Un député a parlé de Phénix tout à l'heure.

Il y a bien sûr certains défis et imperfections associés au travail avec le secteur privé, comme nous en avons discuté plus tôt. À mon avis, il faut faire affaire avec les entreprises technologiques les plus sophistiquées au monde. Elles ont la capacité requise sur le plan de la sécurité pour garantir la protection des renseignements personnels, comme Apple tente de le faire... peut-être plus que les sociétés de médias sociaux d'aujourd'hui. Bien sûr, Amazon et Microsoft misent beaucoup sur la sécurité de leur offre nuagique. Il faut que le secteur privé participe au dialogue sur la protection des renseignements personnels et il faut veiller à ce que ces intervenants soient responsables de la façon dont ils participent à l'infrastructure publique et des conséquences connexes. Je ne vois pas vraiment d'autre choix.

M. Gagan Sikand: Pour faire suite à cela, si la meilleure technologie provient d'un autre pays, alors notre souveraineté devient un enjeu. Avez-vous quelque chose à dire à ce sujet?

M. Jeffrey Roy: C'est pourquoi, malgré cette notion voulant que le nuage soit très poreux en raison des fermes de serveurs établies un peu partout dans le monde, bon nombre de pays ont négocié des accords selon lesquels les centres de données de certains types de données doivent se trouver à l'intérieur des frontières nationales.

Cela ne devrait pas restreindre le Canada qui a accès à plusieurs fermes de données de grandes entités établies ici. Souvent, ces entités passent inaperçues parce qu'elles ne veulent pas trop médiatiser leur emplacement. Je ne crois pas que cela représente une restriction. Pour me préparer à la réunion, j'ai lu la politique de confidentialité du programme en ligne de PC Optimum et on y indique clairement que l'entreprise ne peut garantir que les données ne seront pas partagées sur les serveurs d'autres pays.

C'est un défi, j'en conviens. Je ne dis pas que ce ne l'est pas, mais je crois qu'il y a des façons pour les gouvernements de stipuler... Par exemple, même Apple doit stocker des données d'iCloud en Chine, en vertu de la loi chinoise. La plupart des pays empruntent cette voie. Si certains ensembles de données se situent au pays en vertu de certains règlements et que d'autres données, moins délicates ou moins essentielles, peuvent être stockées dans d'autres couches du nuage, en veillant à ce que les acteurs privés soient transparents dans les diverses tribunes et qu'ils expliquent comment les données sont utilisées, alors on peut profiter d'une certaine souplesse.

M. Gagan Sikand: Merci.

Le président: Allez-y, monsieur Picard. Il vous reste deux minutes, si vous voulez poser une courte question.

M. Michel Picard: Elle sera très courte, en effet.

Quel est le seuil associé à la confidentialité de mes données? Qui détermine ce qui est privé et où s'arrête la collecte de données?

Je vais vous donner un scénario, qui se passe dans une petite ville. Si je marche dans la rue à 2 heures du matin, je ne veux pas que le gouvernement utilise la reconnaissance faciale et sache que j'étais là à cette heure ni avec qui j'y étais. J'ai le droit à une vie privée et je veux qu'on me laisse tranquille.

Toutefois, si je suis victime d'un délit de fuite, alors je veux qu'il y ait plein de caméras pour attraper le salaud qui m'a fait cela. Je veux sa plaque d'immatriculation, sa photo et tout le reste. Je me fous de la confidentialité.

Qu'est-ce qu'on peut faire? Qui décide de ce qui est privé ou non?

M. David Eaves: J'essayais justement de l'expliquer un peu plus tôt. Je crois que vous devez engager un dialogue avec le public, parce que j'avais exactement le même genre d'exemple concernant mes dossiers médicaux. Je veux que personne n'y ait accès en temps normal, mais si je me trouve étendu dans la rue, en train de mourir, je voudrai vraiment que certaines personnes y aient accès.

Honnêtement, la vérité, c'est qu'il n'y a pas de réponse simple à ce genre de questions.

L'une des principales choses que j'essaie de vous dire — et je pense que c'est la même chose pour Mme Clarke —, c'est que nous devons réfléchir à la culture et à la norme que nous voulons mettre en place au Canada pour la gestion de tout cela. Nous aurions l'occasion de faire les choses différemment, en ce moment, mais si le public n'embarque pas et que nous ne faisons rien, notre efficacité en souffrira. Ce sont tous les Canadiens qui en souffriront, mais pas nécessairement les citoyens d'autres pays du monde, puisqu'ils feront les choses différemment.

Comment pouvons-nous non seulement construire cette infrastructure, mais gagner l'acceptation du public et réussir à bâtir quelque chose qui inspirera confiance, une infrastructure que les gens jugeront fiable, non seulement sur le plan technique, mais aussi du point de vue de la protection des renseignements personnels?

Je m'excuse, mais je n'ai pas de meilleure réponse à vous donner.

● (1700)

Mme Amanda Clarke: Je pense que vous avez tout à fait raison: on veut le beurre et l'argent du beurre.

D'ailleurs, je crois que le Comité doit faire très attention dans son interprétation d'un grand nombre de données que nous avons actuellement sur les préférences des citoyens concernant la collecte et l'utilisation de données par le gouvernement, parce que la plupart des sondages ne présentent pas les deux côtés de la médaille de façon réaliste aux citoyens.

On trouve d'innombrables sondages qui laissent entendre que les Canadiens n'aiment vraiment pas qu'on recueille certains types de données, qu'on les utilise de certaines façons et qu'on les combine à d'autres ensembles de données. On demande aux gens s'ils voudraient que le gouvernement recueille des données et les utilise à des fins autres que celles pour lesquelles elles ont été recueillies au départ. Bien sûr, les gens répondent « non » quand la question est présentée sous cet angle.

Nous aurions besoin de sondages et d'études dans lesquels on demanderait aux gens s'ils accepteraient que leurs données soient utilisées à des fins autres que celles pour lesquelles elles ont été recueillies « si cela faisait réduire le temps d'attente dans les hôpitaux » ou « si cela permettait de vous informer de tous les avantages fiscaux dont vous ne vous prévalez pas actuellement qui pourraient vous faire économiser des milliers de dollars par année ».

Il faut présenter cette proposition de valeur, parce qu'à l'heure actuelle, la plupart de nos sondages sur les données demandent aux citoyens s'ils veulent qu'on les surveille et qu'on exploite leurs données à mauvais escient, en gros. Tout le monde dira non à cela. Ce n'est pas ce dont il s'agit ici. Ce sont là des compromis importants qui auront une incidence sur l'efficacité du gouvernement et la qualité des services qu'il offre. Il faut se poser des questions sur l'utilisation des données. Certaines seront liées à la protection des renseignements personnels, mais beaucoup plus entreront dans la sphère plus générale de la gouvernance.

Je pense qu'il faut faire très attention à la façon dont on interprète les données issues de ces sondages, parce qu'elles ne sont pas très utiles. Elles portent à croire qu'il vaudrait mieux ne pas aller de l'avant avec bon nombre des réformes que nous vous proposons parce que les citoyens ne se soucient que de la protection de leurs renseignements personnels, mais je ne suis pas certaine que ces sondages dépeignent le véritable compromis à faire.

M. Michel Picard: Effectivement.

Le président: Mme Murray voudrait poser une question.

Allez-y.

Mme Joyce Murray (Vancouver Quadra, Lib.): J'aimerais simplement remercier tous nos témoins.

David, j'ai bel et bien participé à cette réunion du Comité. Je vous remercie de votre travail. Je vous reverrai bientôt dans Vancouver Quadra.

Le président: Merci.

J'ai une dernière chose à mentionner, pour l'organisation des travaux du Comité. Le Budget supplémentaire des dépenses (B) a été déposé ce matin, donc je souhaite vous demander si vous voulez que le ministre comparaisse devant nous dans un avenir rapproché. J'en ai déjà parlé avec Mike, et il y aurait une possibilité le 19 ou le 21 mars. Avez-vous une préférence? Ce sont les dates possibles.

L'hon. Peter Kent: C'est la coutume.

M. Nathaniel Erskine-Smith: Cela ne me dérange pas.

Le président: D'accord, nous nous en occuperons.

Sur ce, je tiens à remercier tous les témoins de leur présence ici aujourd'hui. Je vous remercie de votre témoignage devant le Comité. Merci.

La séance est levée.