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 132 • 1re SESSION • 42e LÉGISLATURE

TÉMOIGNAGES

Le mardi 29 janvier 2019

Président

M. Bob Zimmer

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

Le mardi 29 janvier 2019

● (1535)

[*Traduction*]

Le président (M. Bob Zimmer (Prince George—Peace River—Northern Rockies, PCC)): Bonjour à tous. Nous sommes en 2019, donc je vous souhaite à nouveau la bienvenue au Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique dont c'est la réunion 132 .

Avant de nous tourner vers nos invités, nous avons quelques affaires du Comité à régler. Il n'est pas nécessaire de passer à huis clos.

La plupart d'entre nous connaissent le grand comité international et le travail que nous avons accompli à Londres. Charlie, Nathaniel et moi-même y sommes allés fin novembre pour en discuter avec les représentants de huit autres pays. Le Canada reprend le flambeau. Nous serons l'hôte de cette réunion, le 28 mai, à Ottawa; voilà ce que nous proposons. Nous avons cherché une date qui conviendrait à tout le monde, dans la mesure du possible, et cela semble être le 28 mai.

Je voulais la soumettre au Comité pour m'assurer que vous êtes d'accord avant de passer à la prochaine étape. Il s'agira d'une réunion d'une journée entière, semblable à celle de Londres. Elle commencera le matin. Nous tiendrons des réunions pendant toute la journée. Nous terminerons probablement vers 16 h 30. Ensuite, nous passerons à d'autres activités.

M. Raj Saini (Kitchener-Centre, Lib.): Cela tombe quel jour de la semaine?

Le président: Un mardi.

M. Raj Saini: D'accord. C'est bien.

Le président: Je voulais avoir de la rétroaction là-dessus. Peut-être que vous pourriez lever la main ou me dire « C'est bon. Nous pouvons procéder ».

M. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Oui, c'est bon. Nous pouvons procéder.

Le président: Nate, vous vouliez en parler. Allez-y.

M. Nathaniel Erskine-Smith: Dans la mesure où vous avez besoin de l'opinion du Comité, je dirais que votre mandat comme président est de décider en notre nom de prendre les arrangements nécessaires pour que la réunion se tienne au Canada, d'inviter les parlementaires et les pays qui ont participé au Royaume-Uni, à tout le moins, et si nous voulons élargir la réunion, de prendre les mesures nécessaires, pour ce faire.

Le président: Parfait.

Est-ce que cela suffit?

Monsieur Kent.

L'hon. Peter Kent (Thornhill, PCC): Monsieur le président, quelles sont les exigences concernant le soutien financier dans le cas d'une réunion comme celle-là? Faudrait-il faire appel au comité de liaison?

Le président: C'est une bonne question. Il y a une limite d'environ 40 000 $, alors il faut rester en deçà de ce montant. Je ne pense pas que cela pose problème.

Mike.

Le greffier du Comité (M. Michael MacPherson): En gros, c'est ce que nous chercherions à faire. Nous rembourserions les témoins qui ont témoigné devant le Comité comme nous le ferions dans le cadre d'une réunion régulière. Cependant, les députés d'ailleurs, par exemple ceux de la Chambre des communes en Angleterre ou en Australie, paieraient leur propre déplacement pour se rendre ici, comme nous avons assumé les coûts du nôtre lorsque nous avons assisté à la première réunion.

L'hon. Peter Kent: Qu'en est-il de l'utilisation de nos installations?

Le président: Allez-y, Mike.

Le greffier: Nous n'avons pas à nous inquiéter: nous aurons un budget pour tout couvrir.

L'hon. Peter Kent: C'est bien.

Le président: Nous allons travailler beaucoup avec Mike et les analystes à nous assurer que tout se réalise. Nous voulons que cet événement soit vraiment la prochaine étape de ce que nous avons déjà accompli. Nous nous réjouissons à cette perspective.

L'hon. Peter Kent: Oui.

Le président: Avez-vous des commentaires, monsieur Angus?

M. Charlie Angus (Timmins—Baie James, NPD): Non. Il est clair que nous voulons que les choses avancent, alors je dis que c'est à vous qu'il revient de prendre les mesures nécessaires. Nous pouvons discuter plus tard du thème et de ce dont la communauté internationale voudra parler. Nous pouvons le faire à une date ultérieure.

M. Nathaniel Erskine-Smith: Peut-être que les analystes peuvent nous élaborer un modèle de proposition. J'aimerais simplement faire remarquer que Sheryl Sandberg fait une tournée pour s'excuser; alors voilà. Vous savez tout.

Le président: Nous allons dresser une liste de témoins et vous tenir informés des personnes que nous inviterons à la réunion. Je pense que ce nom fera partie de ceux qui figureront sur la liste.

Les membres ont-ils quelque chose à ajouter concernant le grand comité international? Avons-nous suffisamment d'information pour prendre une décision?

Merci à tous. Nous allons poursuivre dans cette lancée.

Nous avons maintenant l'avis de motion. Nous en avons parlé brièvement.

Monsieur Angus, la parole est à vous.

M. Charlie Angus: Les membres du sous-comité se sont réunis pour parler de l'orientation à suivre au cours des derniers mois. Nous avons notre étude sur la gouvernance numérique. Nous avons aussi discuté d'un certain nombre d'autres dossiers qui entreraient dans la rubrique des droits des citoyens à l'ère des mégadonnées. Il pourrait s'agir des questions d'éthique concernant l'intelligence artificielle ou des renseignements financiers des gens et ce qui se passe à cet égard. Je vais soulever ces sujets.

Nathaniel a dit qu'il voulait se pencher sur une partie de la terminologie. Je ne veux pas le faire aujourd'hui, mais je veux dire officiellement que nous envisageons de le faire. Une partie des questions que nous pourrions poser à M. Geist ou à Mme Cavoukian aujourd'hui, en ce qui concerne les droits des citoyens à l'ère des mégadonnées en général, pourrait s'y rapporter ainsi que les questions qu'ils pourraient vouloir aborder concernant la gouvernance numérique. Nous mènerons les deux études en parallèle, si bien que certains des témoignages pourraient être plus pertinents dans une étude que dans l'autre.

Je vais y revenir jeudi.

● (1540)

Le président: Vous allez mettre la question en veilleuse pour l'instant?

M. Charlie Angus: Oui.

Le président: Merci, monsieur Angus.

Pour en revenir à l'ordre du jour régulier, aujourd'hui nous accueillons deux témoins: M. Geist, titulaire de la Chaire de recherche du Canada en droit d'Internet et du commerce électronique, Faculté de droit, Université d'Ottawa, à titre personnel; et par téléconférence, Ann Cavoukian, Privacy by Design Centre of Excellence, Université Ryerson.

Nous allons commencer par vous, madame Cavoukian.

Mme Ann Cavoukian (Privacy by Design Centre of Excellence, Ryerson University, à titre personnel): Merci beaucoup.

Bonjour, mesdames et messieurs. Je suis ravie de pouvoir m'adresser à vous aujourd'hui. J'ai travaillé avec Michael pendant de nombreuses années, alors c'est merveilleux d'être ici avec lui pour parler de ces questions importantes.

Ce qui m'a frappée en ce qui concerne vos travaux — je vais simplement le lire à haute voix — est que votre comité doit « entreprendre une étude sur les services gouvernementaux numériques afin de comprendre comment le gouvernement peut améliorer les services offerts aux Canadiens tout en protégeant leur vie privée et leur sécurité ».

C'est d'une importance vitale. C'est ainsi que je veux aborder quelque chose que j'ai créé il y a des années et qu'on appelle la « privacy by design », soit la protection intégrée de la vie privée, qui vise à abandonner les modes de pensée à somme nulle qui dominent notre société. La somme nulle signifie qu'il est uniquement possible de réaliser des gains dans un secteur, la sécurité, mais toujours au détriment de l'autre, la protection de la vie privée, si bien que la somme des deux est nulle.

Ce modèle gagnant-perdant, fondé sur une solution au détriment d'une autre, est dépassé. J'aimerais aujourd'hui que vous adoptiez un modèle de somme positive. Une somme positive signifie simplement qu'on peut réaliser deux gains positifs dans deux secteurs en même temps. C'est une proposition gagnante sur toute la ligne.

Cela a commencé il y a des années. J'ai fait mon doctorat à l'Université de Toronto lorsque le père de la théorie du jeu, Anatol Rapoport, s'y trouvait. Nous avions l'habitude d'en discuter. Je me souviens d'avoir demandé pourquoi les gens optaient pour les sommes nulles. Je suis une éternelle optimiste. Je préfère nettement offrir de multiples solutions gagnantes que des compromis entre deux choses. Il m'a répondu que c'était simple, que les sommes nulles étaient la solution facile, car c'est beaucoup plus facile de donner une seule chose et d'ignorer tout le reste.

Je veux que vous en fassiez davantage et je pense que c'est ce que vous souhaitez. Vous voulez assurer le respect de la vie privée et la sécurité tout en améliorant les services gouvernementaux offerts aux Canadiens.

Mon cadre de protection intégrée de la vie privée est fondé sur l'intégration proactive de mesures de protection de la vie privée très nécessaires à l'élaboration de vos opérations et de vos politiques s'agissant de tous les nouveaux services que vous voulez élaborer ou de tout ce que vous voulez faire en matière d'utilité des données, mais nous le faisons en tenant compte des questions de protection de la vie privée et de sécurité. Il s'agit d'un modèle qui offre de multiples solutions gagnantes. Il fournit des services de protection de la vie privée et d'utilité des données aux particuliers. Vous pouvez remplir l'espace vide, mais il est inclusif et non exclusif. Un n'exclut pas l'autre. Mais comment faire les deux?

Je sais que je n'ai que 10 minutes et que j'en ai probablement déjà utilisé jusqu'à cinq, alors je serai brève pour la suite.

Dans le monde de la protection de la vie privée, il existe un concept clé appelé la minimisation des données, qui consiste à anonymiser les données pour pouvoir en tirer parti afin d'offrir aux Canadiens et aux particuliers des services très nécessaires dans d'autres secteurs d'intérêt sans qu'ils doivent renoncer à la protection de leur vie privée. Lorsqu'on anonymise des données personnelles identifiables, c'est-à-dire qu'on élimine les identifiants directs et indirects, on libère les données, si vous voulez, des restrictions en matière de protection de la vie privée, car c'est l'identifiabilité des données qui est à l'origine des questions de protection de la vie privée. Si les données ne peuvent être personnellement identifiées, d'autres questions pourraient y être associées, mais il ne s'agira pas de questions de protection de la vie privée.

La minimisation et l'anonymisation des données appuieront l'objectif d'obtenir ce que j'appelle de multiples gains simultanément, donc d'avoir une proposition gagnante sur toute la ligne. Je pense qu'elles accroîtront l'efficacité des gouvernements. Vous serez en mesure d'utiliser les données dont vous disposez tout en protégeant toujours les renseignements personnels des citoyens. C'est absolument essentiel.

Je serais ravie de vous en dire plus. Je pourrais parler sans fin de cette question, mais je tiens à respecter les limites de temps qui m'ont été imposées. Je me ferai un plaisir de répondre à vos questions.

● (1545)

Le président: Merci, madame Geist. Désolé, madame Cavoukian. Je me suis un peu emballé.

Des voix: Oh, oh!

Le président: La parole est maintenant à M. Geist pour 10 minutes.

M. Michael Geist (titulaire de la Chaire de recherche du Canada en droit d'Internet et du commerce électronique, Faculté de droit, Université d'Ottawa, à titre personnel): Très bien. C'est parfait. Je ne crois pas que ma femme nous écoute.

Des voix: Ha, ha!

M. Michael Geist: Bonjour à tous. Je m'appelle Michael Geist. Je suis professeur de droit à l'Université d'Ottawa, où j'occupe la Chaire de recherche du Canada en droit d'Internet et du commerce électronique. Je suis également membre du Centre de recherche en droit, technologie et société.

Mes domaines de spécialité sont, entre autres, la politique numérique, la propriété intellectuelle et la protection des renseignements personnels. J'ai siégé pendant de nombreuses années au conseil consultatif externe du Commissaire à la protection de la vie privée du Canada. J'ai eu le privilège de comparaître à maintes reprises devant des comités au sujet de questions liées à la protection des renseignements personnels, notamment en ce qui concerne la Loi sur la protection des renseignements personnels et les documents électroniques, ou LPRPDE, le projet de loi S-4, le projet de loi C-13, la Loi sur la protection des renseignements personnels, ainsi que l'étude réalisée par votre comité sur les médias sociaux et la protection de la vie privée. Je préside également le groupe consultatif sur la stratégie numérique de Waterfront Toronto, qui participe activement au processus de création d'une ville intelligente à Toronto, en collaboration avec Sidewalk Labs. Comme toujours, je suis venu témoigner à titre personnel, en tant qu'universitaire indépendant, et je ne représente que mes propres opinions.

L'étude menée par votre comité sur les services gouvernementaux et la protection des renseignements personnels offre une occasion exceptionnelle: celle de relever bon nombre des défis qui se posent aujourd'hui au chapitre des services gouvernementaux, de la protection des renseignements personnels et de la technologie. En effet, ce qui rend cette question si impérieuse, c'est qu'elle représente la convergence de plusieurs domaines: le droit relatif à la protection des renseignements personnels dans les secteurs public et privé, la gouvernance des données et les technologies émergentes. Le cas de Sidewalk Labs en est un bon exemple. Bien que ce projet ne concerne pas les services du gouvernement fédéral — il s'agit, bien entendu, d'un projet municipal —, les débats portent fondamentalement sur le rôle du secteur privé dans la prestation de services gouvernementaux, la collecte de données publiques et la surveillance ou l'engagement des gouvernements à tous les échelons. Ainsi, on ne sait pas encore tout à fait quelle est la loi applicable à ce projet. Est-ce la LPRPDE? Est-ce la loi provinciale sur la protection des renseignements personnels? Est-ce les deux? Comment pouvons-nous relever certains de ces nouveaux défis si le simple fait de déterminer la loi applicable nous donne toujours du fil à retordre?

Le message principal que je veux vous transmettre aujourd'hui est le suivant: l'étude des services gouvernementaux et de la protection des renseignements personnels exige plus qu'un examen étroit des mesures que prend le gouvernement fédéral pour fournir des services, évaluer les répercussions sur la protection des renseignements personnels et, par la suite, déterminer les règles ou règlements qui pourraient être modifiés ou adoptés en vue d'améliorer la prestation de services qui répondent aux besoins des Canadiens et qui s'accompagnent des garanties de confidentialité et de sécurité auxquelles les citoyens s'attendent à juste titre.

Selon moi, les services gouvernementaux de demain feront intervenir un écosystème beaucoup plus complexe qui s'étend au-delà des questions habituelles liées à la pertinence de la Loi sur la protection des renseignements personnels à l'ère du numérique. En raison du chevauchement entre les régimes public et privé, entre le fédéral, le provincial et le municipal, ainsi qu'entre les affaires intérieures et étrangères, il nous faut plutôt une évaluation globale qui reconnaît que la prestation des services dans un monde numérique suppose nécessairement plus qu'une seule loi. Ces services porteront sur des questions concernant l'échange d'information au sein d'un gouvernement ou entre plusieurs gouvernements, l'endroit où les données sont stockées, le transfert d'information au-delà des frontières et l'utilisation de l'information par les gouvernements et le secteur privé pour, entre autres, l'analyse des données et l'intelligence artificielle.

En d'autres termes, cela comprend la Loi sur la protection des renseignements personnels, la LPRPDE, les accords commerciaux qui contiennent des règles sur la localisation et le transfert des données, le Règlement général sur la protection des données, les traités internationaux, notamment les travaux qui seront entrepris à l'OMC sur le commerce électronique, les fiducies de données communautaires, les politiques en matière de gouvernement ouvert, le droit d'auteur de la Couronne, les normes du secteur privé et les technologies émergentes. C'est un domaine complexe et difficile, mais non moins exaltant.

Je serai heureux de revenir sur bon nombre de ces sujets durant la période des questions, mais vu que le temps passe, je vais aborder un peu plus en profondeur la Loi sur la protection des renseignements personnels. Comme les membres du Comité le savent, il s'agit de la loi fondamentale pour la collecte et l'utilisation de renseignements personnels par le gouvernement. À l'instar de nombreux auteurs d'études, les commissaires fédéraux à la protection de la vie privée qui se sont succédé ont essayé de sonner l'alarme au sujet de cette loi, qui est jugée dépassée et inadéquate. Les Canadiens s'attendent avec raison à ce que les règles de protection des renseignements personnels qui régissent la collecte, l'utilisation et la communication de leurs renseignements personnels par le gouvernement fédéral répondent aux normes les plus strictes. Cependant, depuis des décennies, nous ne répondons pas à de telles normes. À mesure qu'augmente la pression pour de nouvelles utilisations des données recueillies par le gouvernement fédéral, il devient de plus en plus nécessaire d'instaurer une loi « adaptée aux fins visées ».

J'aimerais souligner trois problèmes en particulier concernant les règles fédérales régissant la protection des renseignements personnels et leurs répercussions. Le premier a trait au pouvoir d'établissement de rapports. L'incapacité de procéder à une véritable réforme de la Loi sur la protection des renseignements personnels pourrait être attribuable, en partie, au manque de sensibilisation du public à la loi et à son importance. Les commissaires à la protection de la vie privée ont joué un rôle important pour ce qui est de sensibiliser la population à la LPRPDE et aux préoccupations générales en la matière. La Loi sur la protection des renseignements personnels a désespérément besoin d'un mandat similaire pour l'éducation du public et la recherche.

De plus, l'idée de prévoir simplement un rapport annuel est vraiment le reflet d'une époque révolue. Dans notre contexte actuel où les nouvelles nous parviennent 24 heures sur 24 grâce aux médias sociaux, il n'y a pas lieu de restreindre la capacité de diffuser de l'information — de la vraie information, surtout celle qui touche la vie privée de millions de Canadiens — afin qu'elle demeure à l'abri du public tant qu'un rapport annuel n'est pas déposé. Si le commissaire juge qu'il est dans l'intérêt public de le faire, le Commissariat doit certes avoir le pouvoir de divulguer l'information en temps utile.

● (1550)

Le deuxième point consiste à limiter la collecte de renseignements. Comme vous l'avez entendu à maintes reprises, la Loi sur la protection des renseignements personnels est malheureusement loin de répondre aux normes d'une loi moderne sur la protection des renseignements personnels. En fait, à une époque où le gouvernement est censé servir de modèle, il en demande beaucoup moins de lui-même que du secteur privé.

Toute réforme valable devrait, à mon sens, limiter la collecte de renseignements, ce qui caractérise les mesures législatives s'appliquant au secteur privé. Le gouvernement devrait, lui aussi, être tenu de ne recueillir que les renseignements qui sont strictement nécessaires à ses programmes et activités. C'est particulièrement pertinent en ce qui concerne les nouvelles technologies et l'intelligence artificielle.

Le commissaire à la protection de la vie privée du Canada — qui, je le sais, viendra comparaître plus tard cette semaine —, a récemment présenté un rapport sur le recours à l'analyse des données et à l'intelligence artificielle pour l'exécution de certains programmes. Le rapport fait mention de plusieurs exemples, dont le projet pilote d'analyse prédictive pour les visas de résident temporaire d'Immigration, Réfugiés et Citoyenneté Canada, qui utilise l'analyse prédictive et la prise de décision automatisée dans le cadre des processus d'approbation des visas; l'utilisation, par l'Agence des services frontaliers du Canada, de l'analyse avancée dans le cadre de son Programme national de ciblage afin d'évaluer l'information sur les passagers pour tous les voyageurs aériens arrivant au Canada; et l'utilisation croissante de l'analyse avancée par l'Agence du revenu du Canada pour trier, catégoriser et coupler les renseignements sur les contribuables en fonction des indicateurs perçus de risque de fraude.

Ces technologies offrent évidemment un énorme potentiel, mais elles peuvent aussi encourager une augmentation de la collecte, de l'échange et du couplage des données. Cela exige des évaluations rigoureuses des facteurs relatifs à la vie privée et des analyses des coûts-avantages connexes.

Enfin, il y a la question de la transparence en ce qui concerne les atteintes à la sécurité des données. Comme vous le savez sûrement, l'adoption de lois obligeant la notification en cas d'atteinte à la sécurité est devenue chose courante dans le domaine de la protection des renseignements personnels dans le secteur privé, et il est évident depuis longtemps qu'il faut exiger la même chose dans la Loi sur la protection des renseignements personnels. Malgré l'importance d'une telle mesure, il a fallu plus d'une décennie pour adopter et mettre en oeuvre, au Canada, des règles de notification en cas d'atteinte à la sécurité des données dans le secteur privé et, en dépit de cela, nous attendons toujours l'équivalent au niveau du gouvernement fédéral.

Encore une fois, comme vous n'êtes pas sans le savoir, les données révèlent que des centaines de milliers de Canadiens ont été touchés par des atteintes à la sécurité de leurs renseignements personnels. Le taux de signalement de ces cas demeure faible. Si nous tenons à ce que la population ait confiance en la sécurité de leurs renseignements personnels, il faut clairement des règles sur la notification obligatoire en cas d'atteinte au sein du gouvernement.

À cela s'ajoutent les règles et les politiques générales sur la transparence, un sujet qui est étroitement lié à la question des atteintes à la sécurité des données. En un sens, l'objectif stratégique consiste à favoriser la confiance des citoyens à l'égard de la collecte, de l'utilisation et de la communication de leurs renseignements grâce à l'adoption d'approches transparentes et ouvertes en matière de mesures de protection stratégiques et au recensement de cas où nous n'avons pas été à la hauteur.

Ces derniers temps, l'accent a été mis sur la production de rapports de transparence dans le secteur privé. Ainsi, les grandes sociétés Internet comme Google et Twitter ont publié des rapports de transparence, et d'importantes entreprises canadiennes de communications comme Rogers et Telus leur ont emboîté le pas. Toutefois, aussi étonnant que cela puisse paraître, il y a encore des entreprises récalcitrantes. Par exemple, Bell, le plus grand joueur parmi ce groupe, ne publie toujours pas de rapport de transparence en 2019.

Cependant, ces rapports ne représentent qu'un côté de la médaille. Les gens seraient bien mieux informés des demandes et des notifications si les gouvernements publiaient, eux aussi, des rapports de transparence. Il n'est pas nécessaire d'y inclure les enquêtes en cours, mais il n'y a pas vraiment de raison pour que le gouvernement ne soit pas tenu de répondre aux mêmes attentes que le secteur privé en matière de transparence.

Au bout du compte, nous avons besoin de règles qui favorisent la confiance de la population à l'égard des services gouvernementaux en veillant à ce qu'il y ait des mesures de protection adéquates et des mécanismes de transparence et de notification pour donner aux citoyens l'information dont ils ont besoin au sujet de l'état de leurs données et des niveaux d'accès appropriés afin de maximiser les avantages des services gouvernementaux.

Il n'y a là rien de nouveau. Le seul aspect qui est peut-être nouveau, c'est que ce travail doit se faire dans un contexte caractérisé par des technologies changeantes, des flux d'information à l'échelle mondiale et une ligne de démarcation de plus en plus floue entre les secteurs public et privé sur le plan de la prestation des services.

Je me ferai un plaisir de répondre à vos questions.

Le président: Merci, madame Cavoukian et monsieur Geist.

Nous allons commencer par M. Saini. Vous avez sept minutes.

M. Raj Saini: Bonjour, madame Cavoukian et monsieur Geist. C'est toujours un plaisir de recevoir ici d'éminents experts. Je ferai de mon mieux pour poser des questions succinctes.

Monsieur Geist, relativement à l'un des points que vous avez soulevés, vous avez parlé des différents ordres de gouvernement. Je viens d'une région du pays où il existe quatre paliers de gouvernement: fédéral, provincial, régional et municipal. Dans le modèle que nous avons étudié auparavant, soit le modèle estonien, il y a ce qu'on appelle le principe de la demande unique, par lequel tous les renseignements sont diffusés une seule fois, même s'il faut reconnaître que l'Estonie est un petit pays qui ne compte probablement que deux niveaux de gouvernement. Au Canada, dans certains cas, nous en comptons trois ou quatre.

Comment pouvons-nous protéger les renseignements personnels des Canadiens? Chaque ordre de gouvernement a une fonction différente et une responsabilité différente. Au lieu de fournir toute l'information une seule fois au gouvernement fédéral, puis au gouvernement provincial, puis au gouvernement régional et, enfin, à l'administration municipale — et, comme vous le savez, il est possible d'échanger les renseignements, qu'il s'agisse de dossiers d'impôt, de dossiers de santé ou de casiers judiciaires —, par quel moyen pouvons-nous protéger les renseignements personnels des Canadiens, tout en améliorant l'efficacité des services gouvernementaux?

● (1555)

M. Michael Geist: Vous soulevez là un point intéressant. À certains égards, cela fait ressortir un aspect — comme Ann s'en souviendra, et je suis sûr qu'elle aura des observations à faire là-dessus —, car lorsque nous nous apprêtions à créer une loi fédérale sur la protection des renseignements personnels dans le secteur privé au Canada, nous étions aux prises, en quelque sorte, avec presque la même question: comment faire en sorte que tous les Canadiens aient le même niveau de protection des renseignements personnels aux termes des lois, peu importe l'endroit où ils vivent et le palier de gouvernement en cause?

La triste réalité, c'est que, des décennies plus tard, cela n'est toujours pas le cas. Nous pouvons certes nous demander s'il y a lieu de trouver des mécanismes qui permettent aux gouvernements de collaborer plus activement pour régler ces questions. Il faut bien admettre pourtant, si nous voulons être sincères, que les provinces ont adopté différentes approches en ce qui concerne certaines des règles en matière de protection des renseignements personnels, et ce n'est là qu'un autre palier de gouvernement. Ainsi, la loi du Québec sur la protection des renseignements personnels dans le secteur privé a été adoptée avant la loi fédérale. Quelques provinces ont essayé d'établir des lois de nature semblable. D'autres ont instauré des lois portant sur des sujets plus précis. Le mécanisme prévu par la LPRPDE à cette fin consiste à déterminer si la loi est essentiellement similaire, mais dans la pratique, il y a encore de nombreux Canadiens qui, dans bien des cas, n'ont concrètement aucun moyen de protéger leurs renseignements personnels aujourd'hui, faute de lois provinciales ayant réussi à combler ces lacunes. C'est sans compter les autres paliers dont vous avez parlé. Il s'agit donc d'un enjeu constitutionnel épineux, qui soulève également diverses questions sur la teneur de certaines des dispositions.

M. Raj Saini: Madame Cavoukian, la prochaine question s'adresse à vous.

Parmi les caractéristiques fondamentales du modèle estonien, outre le principe de la demande unique, mentionnons la présence d'une forte identité numérique, mais par-dessus tout, l'interopérabilité entre les différents ministères gouvernementaux. Le modèle estonien est structuré de telle sorte qu'au lieu de recourir à une seule base de données, on en utilise plusieurs qui contiennent des renseignements très précis auxquels il est possible d'accéder. Cette infrastructure est appelée X-Road. Est-ce un modèle que nous devrions chercher à reproduire?

Par ailleurs, quel est l'avantage ou le désavantage d'avoir des données éparpillées? Cela comporte certains avantages, mais il y a aussi des désavantages. Quel serait l'avantage ou le désavantage de répartir les données et, surtout, de permettre aux Canadiens d'accéder plus facilement à l'information dont ils ont besoin?

Mme Ann Cavoukian: Je crois que c'est un excellent modèle, qui sera d'ailleurs de plus en plus répandu. C'est ce qu'on appelle un modèle de décentralisation: ainsi, toutes les données ne sont pas stockées dans une seule base de données centrale à laquelle peuvent accéder les diverses branches du gouvernement. Le problème avec la centralisation, c'est qu'elle présente un risque bien plus grand en ce qui concerne les atteintes à la sécurité des données et à la vie privée, l'accès non autorisé aux données par des employés curieux, les coups montés de l'intérieur, et j'en passe. Toutes les données seront exposées à un risque beaucoup plus élevé si elles sont entreposées dans un seul endroit central.

Vous vous souviendrez peut-être qu'il y a environ six mois, Tim Berners-Lee, l'inventeur du World Wide Web, s'était dit atterré et horrifié de voir que sa création soit devenue un modèle centralisé dans lequel tout le monde peut essentiellement s'introduire avec facilité et accéder sans autorisation aux données d'autrui. La centralisation prête également le flanc à la surveillance des activités et des mouvements des citoyens. Il y a donc plein de problèmes du point de vue de la protection des renseignements personnels et de la sécurité.

En Estonie, le modèle décentralisé est hors pair. On y trouve différentes grappes d'information. Chaque base de données contient des renseignements auxquels on peut accéder pour un but précis. C'est ce qu'on appelle souvent le but premier de la collecte des données, et les fonctionnaires sont astreints à des limites quant à l'utilisation des données. Ils doivent s'en servir aux fins prévues. Plus vous avez des grappes d'information décentralisées, plus il est probable que les données restent intactes et qu'elles soient conservées aux fins prévues, au lieu d'être utilisées systématiquement pour une foule de raisons qui n'avaient jamais été envisagées.

Vous avez ainsi beaucoup plus de contrôle, et les gens, c'est-à-dire les citoyens, peuvent être assurés de profiter d'un niveau accru de confidentialité et de sécurité relativement à ces données. C'est un modèle qui se répand, et vous en verrez beaucoup plus à l'avenir. Cela ne signifie pas que les autres branches du gouvernement ne peuvent pas accéder aux données. Elles ne peuvent tout simplement pas y accéder automatiquement et en faire ce que bon leur semble.

● (1600)

M. Raj Saini: C'est formidable. Merci.

J'ai une dernière question, monsieur Geist. Vous avez mentionné qu'il y aura une interface ou un lien entre le secteur privé et le secteur public. De toute évidence, les deux secteurs sont régis par deux régimes de protection des données personnelles différents. Plus important encore, lorsque nous examinons le modèle estonien, nous constatons qu'il s'agit de la technologie de la chaîne de blocs, une technologie sécuritaire et fiable.

Si l'on veut garder deux systèmes distincts, un pour le secteur public et un pour le secteur privé, la technologie doit être d'égale qualité de part et d'autre. Comme nous le savons, la technologie du secteur privé est parfois supérieure à celle du secteur public. Comment pouvons-nous transformer les deux afin de nous assurer que la fiabilité et l'efficacité de l'interface seront au rendez-vous pour le citoyen?

M. Michael Geist: Selon moi, la fiabilité est un principe juridique plutôt que technologique, et elle a tout à voir avec la fiabilité des données qui sont recueillies.

Pour ce qui est de veiller à ce que les secteurs public et privé utilisent la meilleure sécurité possible, je pense que nous avons vu certains des mécanismes, du moins dans le secteur public, grâce auxquels nous pourrions viser cela en conjonction avec les efforts que déploie le gouvernement pour tenter d'intégrer différents services de l'informatique en nuage. C'est une bonne illustration de la façon dont le gouvernement a reconnu que l'informatique en nuage pouvait susciter certaines préoccupations en ce qui concerne l'endroit où les données sont stockées et d'autres problèmes de localisation semblables. Toutefois, selon le fournisseur, cette technologie peut aussi offrir certains des meilleurs mécanismes de sécurité concernant l'emplacement des données stockées. Alors, la question est de savoir comment il est possible de profiter de cela tout en mettant en place les mesures de protection nécessaires. Nous avons vu certains efforts à cet égard.

Cela se résume en partie à l'étiquetage des différents types de données ou peut-être, surtout au niveau du gouvernement fédéral, à la création de différents types de règles pour différents types de données. Par ailleurs, je pense qu'il faudra être prêt à brouiller ces lignes de démarcation de temps à autre, tout en reconnaissant la nécessité de veiller à ce que les règles canadiennes soient applicables.

Le président: Merci, monsieur Saini.

Nous avons maintenant M. Kent, pour sept minutes.

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

Merci à vous deux d'être venus témoigner.

L'étude du gouvernement numérique est un vaste sujet. Nous l'avons amorcée l'an dernier, puis nous l'avons reléguée au second plan à cause de l'étude au sujet de Cambridge Analytica, Facebook et AggregateIQ.

Ma rencontre, l'année dernière, avec le premier ministre estonien, Juri Ratas a été une expérience fascinante. Il m'a montré la carte et la puce qu'elle contient. Essentiellement, ce sont à peu près toutes les informations d'une vie qui y sont stockées. Il y a eu quelques manquements et quelques pépins avec leur fabricant de puces, mais c'est un concept fascinant.

Ma question s'adresse à vous deux. Le modèle de gouvernement numérique estonien repose sur une démocratie naissante, compte tenu de l'effondrement relativement récent de l'Union soviétique. La société y est encore soumise, et elle a accepté la décision de ses nouveaux dirigeants d'imposer démocratiquement ce nouveau gouvernement numérique à la population. Or, ici, notre merveilleuse Confédération canadienne a été pendant plus de 150 ans le théâtre de remises en question démocratiques — non sans une certaine dose de scepticisme et de cynisme — à l'endroit du gouvernement relativement aux changements importants qu'il a tenté d'opérer et aux référendums qu'il a tenus sur diverses questions. Je me demande simplement, pour n'importe quel gouvernement, qu'il soit fédéral, provincial, régional ou municipal, et dans n'importe quel contexte, à quel point il est réaliste pour le Canada et les Canadiens de chercher à obtenir une seule carte à puce comme cela se fait en Estonie.

Madame Cavoukian, voulez-vous commencer?

Mme Ann Cavoukian: Pardonnez-moi, je secouais la tête. L'Estonie est très respectée, cela ne fait aucun doute. Personnellement, je ne miserais pas sur une seule carte avec une seule puce où seraient stockées toutes vos données. C'est un modèle centralisé qui, à mon avis, va être très problématique — et qui l'est déjà —, surtout à long terme.

Il y a tant d'avancées. Vous avez peut-être entendu parler de ce qui se passe en Australie. Les Australiens viennent d'adopter une loi qui permet au gouvernement d'accéder par voie dérobée aux communications chiffrées. Pourquoi les gens cherchent-ils à chiffrer leurs échanges? C'est parce qu'ils veulent les protéger et les mettre à l'abri du gouvernement ou de tierces parties, de parties non autorisées. L'Australie a adopté une loi qui lui permet d'accéder par la porte de derrière et à votre insu à vos communications chiffrées, et personne ne pourra vous dire si cela s'est fait ou non. Pour moi, c'est une situation consternante.

Personnellement, je ne suis pas en faveur d'une carte d'identité unique, d'une puce unique, de n'importe quoi d'unique.

Cela dit, je pense que nous devons aller au-delà des lois existantes pour protéger nos données et trouver de nouveaux modèles, et je le dis avec beaucoup de respect. J'ai été commissaire à l'information et à la protection de la vie privée de l'Ontario pendant trois mandats, soit durant 17 ans. Bien sûr, nous avions beaucoup de lois et je les observais scrupuleusement, mais elles n'étaient jamais suffisantes. C'est trop peu, trop tard. Les lois semblent toujours à la traîne des technologies et des dernières découvertes. C'est pourquoi j'ai créé Privacy by Design, c'est-à-dire la protection de la vie privée à l'étape de la conception. Je voulais un moyen proactif de prévenir les préjudices, un peu comme un dispositif de prévention médical. La protection de la vie privée à l'étape de la conception a été adoptée de manière unanime comme norme internationale, en 2010. Ses préceptes ont été traduits en 40 langues et ils viennent d'être inclus dans la dernière mesure législative à être entrée en vigueur l'année dernière, en Union européenne, nommément le Règlement général sur la protection des données. Les préceptes de la protection de la vie privée à l'étape de la conception y sont enchâssés.

La raison pour laquelle j'insiste là-dessus, c'est qu'il y a des choses que nous pouvons faire pour protéger les données, pour permettre l'accès aux données — dont l'accès numérique par les gouvernements, au besoin —, mais pas de façon systématique. Il n'est pas nécessaire de créer un modèle de surveillance aux termes duquel toute l'information se retrouverait au même endroit — une carte d'identité —, endroit auquel le gouvernement ou la police pourrait avoir accès.

Vous pourriez me dire que la police n'y aurait pas accès à moins d'avoir un mandat. Malheureusement, je dois dire que cela est absurde. Ce n'est pas vrai. Nous avons des exemples de la façon dont la GRC, par exemple, a créé ce que l'on appelle des Stingrays, c'est-à-dire des capteurs d'IMSI, pour International Mobile Suscriber Identity. Ces tours de téléphonie mobile usurpent l'identité des personnes afin de permettre aux agents d'accéder aux communications cellulaires de tout le monde dans un secteur donné. C'est ce qu'ils font lorsqu'ils recherchent un « méchant ». Bien sûr, s'ils avaient un mandat, je leur dirais: « Je vous en prie, soyez les bienvenus. Allez le chercher. » Mais en ont-ils un? Non. C'est quelque chose qu'ils faisaient sans que personne le sache, mais la CBC les a exposés et ils ont finalement dû reconnaître qu'ils le faisaient.

Avec tout le respect que je vous dois et sans vouloir dénigrer l'Estonie de quelque façon que ce soit, sachez que ce n'est pas la direction que je voudrais que nous prenions ici, c'est-à-dire celle d'une plus grande centralisation. C'est quelque chose que j'éviterais.

● (1605)

L'hon. Peter Kent: Merci.

Monsieur Geist, nous vous écoutons.

M. Michael Geist: Ann a soulevé un certain nombre de points très importants, notamment en ce qui concerne la centralisation.

En vous écoutant, je ne pouvais m'empêcher de penser à ce qui s'est passé jusqu'ici relativement au comité consultatif d'experts sur la stratégie numérique de Waterfront Toronto qui, je dois le reconnaître, a pris plus de place que ce à quoi je m'attendais. En tant que président de ce comité depuis la dernière année...

L'hon. Peter Kent: Je suis convaincu que nous aurons l'occasion d'en reparler.

M. Michael Geist: Je dois dire que lorsque l'on se penche là-dessus, il n'est pas question d'une carte d'identité unique. Il s'agit de prendre une parcelle de terrain relativement petite et de chercher à y intégrer certains types de technologies, des technologies émergentes, qui permettront la mise en oeuvre d'un « gouvernement intelligent ». La controverse qui en a découlé, et plus encore, le genre de discussion publique sur ce que nous sommes prêts à tolérer, sur les fournisseurs avec lesquels nous sommes à l'aise et sur le rôle que nous voulons que le gouvernement joue dans tout cela font ressortir certains des vrais défis. Il s'agit en un sens d'un petit projet pilote pour mettre à l'essai certaines technologies appuyant la notion de ville intelligente. L'évocation d'une carte unique pour toutes les données est un puissant catalyseur qui soulève toute une série de questions quant à notre environnement.

L'hon. Peter Kent: Je suis convaincu que dans les deux heures dont nous disposons, le Comité reviendra à la question plus générale du gouvernement numérique, mais pour l'instant, j'aimerais revenir à Sidewalk Labs. Il y a un peu de David et Goliath dans Sidewalk Labs, vu la façon dont Alphabet, la société mère de Google, a imposé sa façon de traiter avec la ville et les autres partenaires potentiels. Je pense que le départ de Mme Cavoukian témoigne de cela.

M. Michael Geist: Bien sûr, elle a quitté son poste de conseillère chez Sidewalk Labs. J'ai siégé au comité consultatif de Waterfront Toronto, et j'ai l'impression qu'il est encore tôt pour essayer de déterminer précisément à quoi ressemblera le projet d'aménagement définitif et s'il sera approuvé. C'est vraiment le but de ce groupe consultatif: essayer de mieux comprendre quels types de technologie sont proposés, quel type de gouvernance des données nous avons au chapitre de la propriété intellectuelle et de la protection des renseignements personnels, et veiller à ce que les conditions ne soient pas dictées. L'objectif est plutôt de chercher à ce qu'elles reflètent mieux ce à quoi la communauté pense.

● (1610)

Le président: Merci, monsieur Kent.

La parole est maintenant à M. Angus, pour sept minutes.

M. Charlie Angus: Merci, monsieur le président.

J'aimerais bien sûr commencer par une discussion sur Sidewalk Labs, car c'est une proposition très intéressante qui a assurément ouvert la porte à beaucoup de questions.

Madame Cavoukian, votre décision de quitter Sidewalk Labs a soulevé beaucoup de questions. Pouvez-vous expliquer pourquoi vous ne vouliez plus faire partie de ce projet?

Mme Ann Cavoukian: Je n'ai pas démissionné à la légère. Je tiens à vous en assurer.

Sidewalk Labs m'a engagée comme consultante pour intégrer la protection de la vie privée à l'étape de la conception — mon bébé, dont je vous ai parlé — dans la ville intelligente qu'ils projetaient de réaliser. J'ai dit: « Je serais très heureuse de le faire, mais sachez que je pourrais être un caillou dans votre chaussure, parce que cela nécessitera le plus haut degré de protection, et que pour avoir cette protection dans une ville intelligente... » Dans une ville intelligente, les technologies, les capteurs et tout le reste doivent être en fonction 24 heures sur 24, 7 jours par semaine. Les citoyens n'ont pas la possibilité de consentir ou non à la collecte de leurs données. Cela se fait en permanence.

J'ai dit que dans ce modèle, nous devons toujours dépersonnaliser les données à la source, ce qui signifie que lorsque le capteur recueille vos données — sur votre voiture, sur vous-même, peu importe —, vous devez les purger de tous les identificateurs personnels, qu'ils soient directs ou indirects, de manière à les rendre neutres. Vous devez encore décider qui va faire quoi avec ces données. Il y a beaucoup d'enjeux à considérer, mais ils ne seront pas liés à la protection des renseignements personnels.

Ils ne m'ont pas repoussée, croyez-le ou non. Je ne l'ai pas fait non plus. Ils ont accepté ces conditions. Je leur ai expliqué tout cela dès l'embauche initiale.

Ce qui s'est passé, c'est qu'ils ont été critiqués par un certain nombre d'intervenants en ce qui concerne la gouvernance des données. On voulait aussi savoir qui allait contrôler l'utilisation des données, de ces énormes quantités de données. Qui exercera le contrôle? On arguait que ça ne devait pas être seulement Sidewalk Labs.

Ils ont répondu qu'ils allaient créer une « fiducie de données civiques », qui se composerait d'eux-mêmes et de membres de divers gouvernements — municipaux, provinciaux, etc. —, et que diverses sociétés s'occupant de propriété intellectuelle allaient participer à sa création. Par ailleurs, ils ont dit: « Nous ne pouvons pas garantir qu'ils vont dépersonnaliser complètement les données à la source. Nous les encouragerons à le faire, mais nous ne pouvons en donner l'assurance. »

Quand j'ai entendu cela, j'ai su que je devais me retirer. Cela a été fait lors d'une réunion du conseil d'administration, à l'automne. Je ne sais plus quand. Michael s'en souviendra. Le lendemain matin qui a suivi la réunion, j'ai remis ma démission. Voici la raison que j'ai donnée: si vous laissez cette question à la discrétion des entreprises, vous pouvez être certains que cela ne se fera pas. Quelqu'un dira: « Non, nous n'allons pas anonymiser les données à la source. »

Les données qui ne sont pas anonymisées ont une valeur énorme. C'est le nec plus ultra. Tout le monde veut des données sous une forme qui permet d'identifier les gens. En gros, vous devez dire ce que j'ai dit à Waterfront Toronto par la suite. Ils m'ont appelée juste après ma démission, cela va de soi, et je leur ai dit: « Vous devez faire la loi. S'il y a une fiducie de données civiques — et peu importe qui est sur le coup, je m'en fiche —, vous devez leur dire qu'ils doivent anonymiser les données à la source, point final. Ce sont les conditions de l'accord. » Waterfront Toronto ne m'a pas repoussée.

C'est pour cette raison que j'ai quitté Sidewalk Labs. Je travaille maintenant pour Waterfront Toronto pour faire avancer les choses, parce qu'ils sont d'accord avec moi lorsque j'affirme qu'il faut anonymiser les données à la source et protéger les renseignements personnels. Je voulais qu'on ait une ville intelligente sur le plan de la confidentialité, pas sur le plan de la surveillance. Je fais partie du conseil international des villes intelligentes — des villes intelligentes de partout dans le monde — et presque toutes sont des villes intelligentes de surveillance. Pensez à Dubaï, à Shanghai et d'autres municipalités. La confidentialité y est absente. Je voulais que nous nous mobilisions pour montrer qu'il est possible de créer une ville intelligente où la vie privée n'est pas menacée. Je crois toujours que nous pouvons le faire.

M. Charlie Angus: Merci. Permettez-moi d'intervenir.

L'une des préoccupations que j'ai entendues de la part des citoyens de Toronto concerne la nécessité de protéger la vie privée dès la conception, certes, mais aussi celle d'avoir un engagement démocratique dès la conception. Dans le cas d'une ville, il s'agit d'avoir des espaces publics à l'intention des citoyens. Nous avons un problème. Nous avons un gouvernement provincial qui est en guerre avec la ville de Toronto et qui a supprimé un certain nombre de conseillers municipaux. Il y a donc un déficit sur le plan démocratique. Nous voyons Waterfront Toronto dans une situation intermédiaire, avec une province qui pourrait s'y opposer. Nous constatons que le gouvernement fédéral s'occupe continuellement de cette question par l'entremise des lobbyistes de Google, de sorte qu'il y a beaucoup de choses qui se passent en coulisse.

Quel est le rôle des citoyens en matière d'engagement? Si nous voulons aller de l'avant, nous avons besoin de voix démocratiques pour établir ce qui est public, ce qui est privé, ce qui devrait être protégé et ce qui est ouvert. Quant aux autres gros joueurs, nous avons affaire à la plus grande machine de données de l'univers. Cette société amasse de l'argent en recueillant les données des gens et c'est elle qui conçoit tout cela.

Madame Cavoukian, j'aimerais vous poser la question suivante — je n'ai pas beaucoup de temps, peut-être une minute — et j'aimerais ensuite entendre la réponse de M. Geist. Nous aurons peut-être une autre série de questions à ce sujet.

● (1615)

Mme Ann Cavoukian: Je tiens à m'assurer que je laisse à Michael du temps pour intervenir.

Nous avons besoin d'une grande transparence afin de déterminer au juste qui fait quoi et comment cette information est diffusée en ce qui concerne les données et les décisions prises par les divers ordres de gouvernement dont vous avez parlé, des ordres de gouvernement qui semblent toujours être à couteaux tirés. Je ne suis pas ici pour défendre les gouvernements, car il faut qu'il y ait un moyen d'interagir qui permet aux citoyens de participer et de comprendre ce qui peut bien se passer. C'est absolument essentiel. Je ne sous-entends pas que cette question n'est pas importante; je pense simplement que nous devrions nous soucier surtout des questions de protection de la vie privée afin de nous assurer qu'elles sont au moins cernées.

M. Charlie Angus: Monsieur Geist, qu'en pensez-vous?

M. Michael Geist: En réalité, je pourrais simplement formuler des observations à propos du rôle que joue mon groupe d'experts. Toutes nos réunions sont ouvertes au public. Le public peut avoir accès aux documents étudiés. En fait, d'un point de vue technologique, nous avons pris connaissance de certains des plans de Sidewalk Labs. Ils sont venus nous faire un exposé dans le cadre d'une réunion du groupe d'experts. Tout le monde peut assister à ces réunions, qui sont assidûment filmées. En fait, quelqu'un se présente à chaque réunion, filme son déroulement, puis affiche la vidéo sur YouTube. Des réunions supplémentaires ont été organisées. Le mois prochain, nous nous réunirons dans les locaux de MaRS, et la réunion portera précisément sur les fondations civiques.

Avec tout le respect que je vous dois, je dois admettre que la notion selon laquelle aucune discussion publique n'a lieu et aucun moyen d'avoir des discussions publiques n'existe contredit l'expérience que j'ai vécue jusqu'à maintenant au cours de la dernière année que j'ai passée ici, en ce sens que littéralement n'importe qui à Toronto peut assister à n'importe quelle réunion qui lui plaît.

M. Charlie Angus: Monsieur Geist, je dois dire, avec tout le respect que je vous dois, qu'on m'a appris — j'ai appris cela de Google — que les gens étaient frustrés parce que Google souhaite parler de la quantité de bois utilisée pour construire l'édifice. Voyons donc! Eric Schmidt se préoccupe maintenant de l'utilisation des produits du bois à Toronto? Ils parlent des données. Voilà ce que me disent les gens. Ils reviennent de ces réunions sans avoir obtenu de réponses.

M. Michael Geist: Voilà précisément ce dont nous parlons au cours des réunions de notre comité. Nous passons notre temps à parler des questions de gouvernance des données, de protection de la vie privée et de propriété intellectuelle. En fait, nous cherchons à déterminer les technologies qu'ils mettront en place, selon leurs dires, et les conséquences qu'elles auront sur la propriété intellectuelle, la protection de la vie privée et la gouvernance des données. Par exemple, l'idée de créer une fondation civique a été proposée à notre groupe en premier.

Comme je l'ai dit, est-ce que nous pourrions en faire davantage? Je suis certain que nous le pourrions mais, de mon point de vue, je peux dire que je vois les médias participer à nos réunions. Je vois des citoyens y assister. Je vois des articles publiés dans des blogues ou ailleurs qui découlent de ces réunions. Tout cela se déroule de façon complètement ouverte.

Le président: Merci, monsieur Angus.

Le prochain intervenant est M. Erskine-Smith, qui aura la parole pendant sept minutes.

M. Nathaniel Erskine-Smith: Merci beaucoup.

Je vous remercie tous deux de votre présence.

Pour commencer, j'aimerais clarifier un léger malentendu qui s'est immiscé dans certaines des questions de M. Kent en ce qui concerne l'identité électronique en Estonie. Les renseignements personnels ne sont pas centralisés dans un mini-ordinateur. En fait, le fondement même du gouvernement numérique estonien est la décentralisation. L'identité numérique est une carte d'identité qui permet aux Estoniens d'accéder au système, mais elle ne contient pas une foule de renseignements personnels.

Là où je veux vraiment en venir, c'est qu'à mon avis, l'utilité de notre étude consiste à demander comment nous pourrions appliquer le cadre de protection de la vie privée dès la conception à un gouvernement numérique, afin que nous puissions en fait améliorer les services que nous offrons aux Canadiens.

D'emblée, je vous ferais remarquer que, selon l'information publique produite par l'Estonie, près de 5 000 services électroniques distincts permettent aux gens de faire quotidiennement leurs courses sans jamais quitter leur ordinateur à la maison. En ma qualité de Canadien qui souhaite recevoir de meilleurs services de la part de son gouvernement, je veux avoir accès à ces services. Comment pouvons-nous atténuer dès le début du processus les préoccupations relatives à la protection de la vie privée afin que nous puissions bénéficier de meilleurs services?

Si nous examinons le modèle estonien, nous voyons qu'il y a une identité numérique. Les renseignements dont disposent les ministères sont séparés au moyen d'X-Road et de la technologie des chaînes de blocs. Puis il y a une transparence en ce sens que, lorsqu'un employé du gouvernement consulte mes renseignements, je peux voir qui l'a fait et quand cela a été fait grâce à l'horodatage. Si l'on ajoutait ces niveaux de détail à un système d'un gouvernement numérique, cette mesure suffirait-elle à répondre aux préoccupations relatives à la protection de la vie privée? Y a-t-il d'autres mesures que nous devrions prendre si nous envisageons de passer à un gouvernement numérique?

Je vais commencer par interroger Mme Cavoukian, puis M. Geist.

Mme Ann Cavoukian: Il y a un certain nombre d'éléments très positifs dans ce que vous avez décrit, dont la transparence associée à chaque service offert et la facilité avec laquelle les citoyens peuvent avoir accès à ces services en ligne.

Je tiens à formuler une observation à propos de la technologie des chaînes de blocs. Ne présumons pas qu'il s'agit là d'une merveilleuse technologie qui garantit l'anonymat, car ce n'est pas le cas. Cette technologie présente des avantages, mais elle peut aussi avoir des côtés négatifs. De plus, elle a été piratée. Je vais vous lire une phrase très courte tirée d'un texte portant sur le Règlement général sur la protection des données, le RGPD. Le RGPD est la nouvelle loi qui est entrée en vigueur en Union européenne. La phrase en question dit ce qui suit: « En particulier dans le cas de la technologie des chaînes de blocs, il n'y a pas d'autre solution que celle de mettre en oeuvre le cadre de protection de la vie privée dès la conception, étant donné que les ajouts habituels en matière d'amélioration et de protection de la vie privée ne satisferont pas aux exigences du RGPD ». Le RGPD a radicalement relevé la barre au chapitre de la protection des renseignements personnels. Les gens disent: « Utilisez bien entendu la technologie des chaînes de bloc, mais ne le faites pas sans mettre en oeuvre le cadre de protection de la vie privée dès la conception, car vous devez vous assurer que cette protection est intégrée dans la technologie des chaînes de blocs ». Certaines entreprises, comme Enigma, le font merveilleusement bien en prévoyant un niveau supplémentaire de protection des renseignements personnels.

Je tiens simplement à ce que nous fassions attention de ne pas adhérer à la technologie des chaînes de blocs ou à d'autres technologies sans regarder réellement sous le capot et sans observer ce qui se passe au chapitre de la protection des renseignements personnels.

● (1620)

M. Nathaniel Erskine-Smith: Je crois comprendre qu'en Estonie, ils utilisaient cette technologie avant qu'on lui attribue le nom de technologie des chaînes de blocs, mais c'est en 2002 que les Estoniens ont mis en oeuvre un système. Ils ont eu l'idée d'utiliser cette technologie pour transférer l'information d'un ministère à l'autre en arrière-plan. En tant que citoyen, lorsque j'ouvre une session, je n'aperçois qu'un seul portail mais, en arrière-plan, mes renseignements sont hébergés dans un certain nombre de ministères. Si ces ministères souhaitent échanger des renseignements, les voies nécessaires sont ouvertes uniquement au moyen de la technologie des chaînes de blocs, afin de garantir le caractère privé des échanges. Si je travaille à l'ASFC, je ne serai pas en mesure de consulter les renseignements qui sont enregistrés par les services d'emploi... mais je prends bonne note de votre préoccupation concernant la technologie des chaînes de blocs.

Avec tout le respect que je vous dois, j'imagine, ma question fondamentale... J'ai des questions plus particulières à poser, mais voici ma question générale. Si nous élaborons une identité numérique, que nous garantissons l'anonymat des données échangées entre les ministères, que je peux, en tant qu'utilisateur, ouvrir une session et exercer un contrôle sur mes renseignements et que cela constitue les trois pierres d'assise du système, est-ce que quelque chose m'échappera? Quelque chose d'autre m'échappera-t-il?

Mme Ann Cavoukian: Ce projet semble très positif. Vous intégrerez la sécurité dans [*Difficultés techniques*]

M. Nathaniel Erskine-Smith: Exactement. L'identité numérique est elle-même un dispositif de cryptage.

Mme Ann Cavoukian: Oui.

M. Nathaniel Erskine-Smith: Si j'ai bien compris, l'identité numérique en Estonie est elle-même un microprocesseur ainsi qu'un dispositif de cryptage. Elle vérifie donc mon identité.

Soit dit en passant, en ce qui concerne les Estoniens, le meilleur argument de vente — et je sais qu'il a peut-être inquiété M. Kent — qu'ils ont présenté à notre comité lors de leur visite était le fait qu'aucun vol d'identité n'était survenu depuis qu'ils avaient mis en oeuvre ce système — aucun vol d'identité. Pourquoi? Parce que s'ils perdent leur identité numérique, le certificat peut être révoqué facilement. Par conséquent, personne ne peut utiliser cette identité numérique pour avoir accès à des services en prétendant être quelqu'un d'autre.

Si ces éléments sont les trois pierres d'assise et si vous n'avez pas de réponses claires à donner à aucune... et vous dîtes que ces éléments semblent tous positifs, alors la question fondamentale est la suivante: Y a-t-il d'autres niveaux de sécurité que nous devrions prévoir pour nous assurer que le cadre de protection de la vie privée dès la conception est intégré dans les services du gouvernement numérique, comme l'Estonie le fait? quelque chose échappe-t-il à l'Estonie, ou devrions-nous faire comme elle?

Mme Ann Cavoukian: L'initiative de l'Estonie est très, très positive...

M. Nathaniel Erskine-Smith: Le...

M. Michael Geist: Si vous me permettez de répondre, je ne parlerai pas précisément de l'Estonie, mais je dirai qu'il y a deux éléments nécessaires. Pour un marteau, tout a l'air d'un clou. Pour un professeur de droit, tout a l'air d'un problème juridique. En ce qui concerne la question de décrire des normes principalement technologiques et d'affirmer que c'est la façon dont nous protégerons efficacement... Je comprends pourquoi cette idée est extrêmement attrayante, mais, à mon avis, il faudrait que vous mettiez aussi en place une loi correspondante.

Par ailleurs, un autre des enjeux dont je me soucie est bien entendu l'accès. Alors, qu'avez-vous besoin d'autre? Si vous voulez être en mesure d'adopter des services de ce genre, vous devez vous assurer que tous les Canadiens ont accès au réseau. Nous sommes encore aux prises avec un trop grand nombre de Canadiens qui ne bénéficient pas d'un accès à Internet abordable. Nous devons reconnaître qu'une partie de toute conversation concernant la façon dont nous pouvons offrir aux Canadiens des services de ce genre doit être consacrée à la question de savoir comment nous veillerons à ce que tous les Canadiens bénéficient d'un accès au réseau abordable.

M. Nathaniel Erskine-Smith: Je vous suis reconnaissant de vos observations.

Comme je vais manquer de temps, la dernière question que je poserai concerne la minimisation des données. D'une part, je pense qu'en général, l'Estonie suit cette règle mais, lorsque nous examinons les services gouvernementaux, nous pourrions dire, comme les entreprises le font, qu'un surcroît de données nous permettra d'offrir de meilleurs services aux consommateurs. En tant que gouvernement, nous soutenons que, dans certains cas, il est préférable d'avoir accès à un plus grand nombre de données. Je souhaite vous donner un exemple.

Très peu de Canadiens souscrivent au Bon d'études canadien. Tout le monde est admissible à l'Allocation canadienne pour enfants parce que c'est automatique, à condition de produire une déclaration de revenus. Par ailleurs, si nous connaissions tous les particuliers qui reçoivent l'Allocation canadienne pour enfants, nous saurions également qu'ils sont admissibles au Bon d'études canadien. Pour pouvoir sensibiliser les citoyens de façon préventive et leur dire en passant qu'ils ont droit de recevoir gratuitement des fonds pour l'éducation de leurs enfants et qu'ils devraient donc présenter une demande à cet égard, s'ils ne l'ont pas déjà fait, nous devons utiliser leurs renseignements personnels, idéalement dans le but d'améliorer les services. Dans ce contexte, y a-t-il des risques dont je devrais me préoccuper?

● (1625)

Mme Ann Cavoukian: Je ne crois pas du tout qu'il soit préférable de disposer d'un plus grand nombre de données.

Vous donnez un exemple très valable. Vous souhaitez sensibiliser les gens, mais l'utilisation des données à des fins jamais prévues comporte de nombreux risques. En théorie, nous fournissons des données au gouvernement dans un but particulier. Nous payons nos impôts, ou nous prenons une mesure quelconque. C'est là notre intention, et c'est donc l'objectif principal de la collecte de données. Vous êtes censés utiliser ces données dans ce but et limiter votre utilisation à cela, à moins d'obtenir un consentement supplémentaire auprès du sujet des données, c'est-à-dire le citoyen.

Dès que vous commencez à vous écarter de cette démarche pour ce que vous croyez être le plus grand bien des Canadiens, et que vous pensez qu'il vaut mieux pour eux que vous ayez accès à toutes leurs données et que vous puissiez leur envoyer des renseignements supplémentaires ou leur fournir des services supplémentaires... Ils ne veulent peut-être pas que vous fassiez cela. Ils ne souhaitent peut-être pas... La protection de la vie privée est une question de contrôle, soit le contrôle personnel de l'utilisation de vos renseignements personnels. Dès que vous commencez à élargir la portée de votre action parce que vous estimez — je ne veux pas dire vous personnellement — que le gouvernement sait ce qu'il faut faire mieux que quiconque, cela vous entraîne dans une voie de surveillance et de suivi, qui est tout à fait inappropriée. Je vous dis cela avec le plus grand respect, car je sais que vos intentions sont louables, mais je n'irais pas... De plus, lorsque vous avez des données inactives, d'immenses quantités de données inactives, cela représente un véritable trésor.

Le président: Merci, madame Cavoukian...

Mme Ann Cavoukian: C'est un véritable trésor pour les pirates informatiques et, tôt ou tard, des gens pirateront ces données. Cela attirera simplement les malfaiteurs.

Le président: Merci.

Comme des votes auront lieu à 17 h 30 et que le Comité doit prendre environ cinq minutes pour s'occuper de quelques travaux à huis clos, j'envisage que nous finissions si possible à environ 16 h 50.

Nous allons maintenant passer à M. Gourde, qui prendra la parole pendant cinq minutes.

[*Français*]

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

Je remercie les témoins d'être ici aujourd'hui.

Ma question est fort simple: est-il possible d'appliquer le modèle de l'Estonie au Canada, compte tenu de nos défis, des niveaux de gouvernance et de l'accessibilité à Internet sur un territoire aussi vaste?

Il y a des endroits au Canada où la connexion ne se fait pas. Si nous optons pour cela, il va tout de même falloir offrir deux niveaux de services aux Canadiens, pour ceux qui ne peuvent pas y accéder. Est-ce que cela vaut vraiment la peine?

Madame Cavoukian, vous pouvez répondre en premier.

[*Traduction*]

Mme Ann Cavoukian: Il est bien entendu extrêmement important d'améliorer le niveau des services offerts aux citoyens, et tout le monde, comme [*Difficultés techniques*], n'a pas un accès égal à Internet et à différents niveaux de technologie. Je pense que l'amélioration des services offerts aux particuliers, aux citoyens, est une entreprise très louable. Ce sont les moyens que vous employez pour le faire qui me préoccupent. Cela soulève toujours des interrogations. Comment pouvez-vous sensibiliser les gens et leur offrir davantage de services sans envahir leur vie privée, sans examiner les autres besoins qu'ils pourraient avoir? S'ils vous fournissent cette information, n'hésitez pas à agir, car cela constituera un consentement positif. Vous pourrez alors les faire bénéficier de services supplémentaires. Mais je ne veux pas que le gouvernement consulte les données dont il dispose déjà à propos des citoyens afin de déterminer si d'autres services pourraient leur être utiles.

Je pense que vous devez demander aux citoyens s'ils aimeraient se prévaloir de ces autres services. Ensuite, vous pourrez sans hésiter leur conseiller de travailler avec vous. Je ne crois pas que nous devrions faire cela en fouillant dans des bases de données à la dérive qui contiennent des renseignements sur nos citoyens.

M. Michael Geist: Je suis heureux que vous ayez soulevé de nouveau la question de l'accès. Comme je l'écris depuis un certain temps, j'ai longtemps pensé que l'une des vraies raisons pour lesquelles les gouvernements... Ce n'est pas du tout une question de partisanerie, car les gouvernements successifs ont peiné à composer avec ce problème. L'une des raisons pour lesquelles il est nécessaire d'investir concrètement pour garantir un accès à Internet universel et abordable, c'est qu'à mon avis, la possibilité pour le gouvernement de passer à un nombre de plus en plus important de services électroniques, et d'économiser ainsi, dépend de la disponibilité de cet accès.

Selon moi, vous avez tout à fait raison de dire que, tant que ce stade n'aura pas été atteint, il faudra essentiellement assurer un ensemble de services parallèles pour garantir un accès universel. Effectivement, vous ne pouvez pas priver certaines personnes de certains types de services gouvernementaux parce qu'elles n'ont pas accès au réseau. Pour une foule de raisons, il est sensé que le gouvernement investisse là où le secteur privé n'a pas voulu le faire. L'une de ces raisons est que cet accès profite au gouvernement, parce qu'à mon avis, il lui permet de favoriser le passage à certains services électroniques plus efficaces.

Manifestement, nous n'avons pas encore atteint ce stade. Des études ont révélé à maintes reprises qu'en ce qui concerne les services à large bande, nous ne disposons pas d'un accès universel abordable et qu'en ce qui concerne les services sans fil, nous continuons de payer certains des frais les plus élevés de la planète pour nous en prévaloir. Cela nous indique que nos politiques en vue de garantir des moyens de communication abordables au Canada continuent d'être grandement déficientes.

● (1630)

[*Français*]

M. Jacques Gourde: Ma dernière question est aussi fort simple.

Au Canada, disposons-nous de l'expertise requise en matière de programmation? Il semble que l'industrie connaisse une crise, une pénurie de programmeurs. Nous devons nous tourner vers l'extérieur du Canada. Il semble que trouver des gens très compétents soit vraiment compliqué. La nouvelle génération n'aime pas nécessairement ce genre de métier.

Une mise en œuvre de ces services par et pour les Canadiens risque-t-elle d'être difficile à réaliser?

[*Traduction*]

M. Michael Geist: Eh bien, en tant que fier papa de deux enfants qui étudient en ingénierie à l'Université de Waterloo, je doute que ce soit vrai. Je crois que de plus en plus de gens choisissent cette voie. Sur le campus de l'Université d'Ottawa, où je travaille, et à vrai dire, sur des campus partout au pays, les domaines des sciences, des technologies, de l'ingénierie, des mathématiques, et j'en passe, suscitent un énorme intérêt. S'il y a une pénurie de spécialistes, cela montre à quel point la demande est élevée. Ce n'est pas que personne ne se dirige dans ce secteur. Je crois que c'est certainement le contraire.

Mme Ann Cavoukian: Je suis d'accord avec Michael. Je pense que nous avons de très bonnes ressources au Canada. Elles seront peut-être insuffisantes demain, mais pour ce qui est de la jeune génération, je conseille de nombreux étudiants et je leur dis toujours qu'ils doivent s'assurer d'apprendre comment programmer. Ils n'ont pas à devenir des programmeurs, mais ils doivent comprendre comment les technologies fonctionnent. Il s'agit d'apprendre comment utiliser différentes techniques de programmation pour faire avancer ses intérêts dans des secteurs complètement différents, etc. Les fondements sont associés à la compréhension de certaines des nouvelles technologies. Je pense que c'est généralement reconnu maintenant.

Le président: Merci, monsieur Gourde.

C'est maintenant au tour de M. Baylis, qui dispose de cinq minutes.

M. Frank Baylis (Pierrefonds—Dollard, Lib.): Merci, monsieur le président.

J'aimerais tout d'abord revenir sur des précisions qu'a apportées Nate concernant la question de Peter sur l'Estonie. Je pense qu'il s'agit là de la base. Si nous passons à un gouvernement numérique, il nous faut une identité numérique.

Êtes-vous d'accord avec moi, madame Cavoukian? Avez-vous des réserves au sujet de l'idée de commencer avec une identité numérique?

Mme Ann Cavoukian: Pardonnez-moi, mais je vais dire que cela dépend de la façon dont elle est conçue.

Si elle est bien protégée, unique et chiffrée et que l'accès est très restreint, une identité numérique peut améliorer l'accès aux services, par exemple, mais le vol d'identité est un problème de grande ampleur. C'est le type de fraude à la consommation qui connaît la croissance la plus rapide, une croissance rapide jamais connue. Une identité numérique peut aussi...

M. Frank Baylis: Oui, mais concernant les nouvelles identités numériques, il y a la biométrie. Au bout du compte, on ne peut jamais empêcher un voleur d'agir, mais prenons l'exemple d'un individu qui trouve mon numéro d'assurance sociale. Si, plutôt, il constate que mon identité numérique est bien chiffrée, que des caractéristiques biométriques, le balayage oculaire, sont utilisés, par exemple, la probabilité qu'il vole cela est bien moindre que ce qu'il peut faire aujourd'hui. Je dirais que...

Mme Ann Cavoukian: Tant que les moyens biométriques sont bons ou qu'on a recours au chiffrement biométrique; il s'agit de chiffrer les données automatiquement de sorte que seul l'individu peut les déchiffrer avec ses propres identificateurs biométriques... Malheureusement, bien des risques sont associés à la biométrie; ce n'est donc pas gagné d'avance que les données biométriques sont associées à l'identité numérique. Il faut utiliser le chiffrement biométrique et s'assurer que c'est bien tenu. Je ne suis pas en désaccord avec vous, monsieur. Je dis seulement que tout se complique quand on entre dans les détails, et c'est ce que nous devons répondre ici.

M. Frank Baylis: Je comprends.

Voulez-vous intervenir là-dessus, monsieur Geist?

M. Michael Geist: Oui. Je profite de l'occasion pour répéter qu'à mon avis, les cadres stratégiques sur la technologie sont aussi importants que la technologie dans certains cas. Même dans la façon de formuler votre question, vous avez dit de façon convaincante les raisons pour lesquelles ces technologies...

M. Frank Baylis: Supposons que nous utiliserons la plus récente technologie. Cette technologie de pointe comprend toutes ces choses...

M. Michael Geist: Exactement.

M. Frank Baylis: ..., comparativement à mon numéro d'assurance sociale, par exemple. Si je vous le donne, c'est fait.

M. Michael Geist: Je comprends. L'idée d'utiliser les meilleures technologies est tout à fait sensée, mais cela s'accompagne de tout un volet de politiques. Je crois que nombreux seront ceux qui exprimeront des inquiétudes étant donné que d'après notre expérience, parfois on garantit que certains types de chiffrement ou d'autres technologies seront utilisés, et l'on dit « ne vous inquiétez pas, il n'y aura aucun accès possible », jusqu'à ce qu'on tombe sur un cas où l'on se dit que ce serait vraiment génial si les responsables de l'application de la loi y avaient accès seulement dans cette situation particulière...

● (1635)

M. Frank Baylis: Je crois que je comprends. Nous allons un peu loin.

Disons que nous commençons aujourd'hui. L'avantage de l'Estonie, c'est qu'il s'agissait d'un nouveau pays qui entreprenait quelque chose, de sorte qu'il n'a pas eu à transformer quoi que ce soit. On parle d'un petit pays peu peuplé, somme toute. Disons que nous commençons aujourd'hui. Il me semble que la première mesure à prendre... Je suis d'accord avec Mme Cavoukian: nous pouvons conserver cette séparation, et je conviens que c'est la démarche la plus sûre. Les Estoniens ont un élément central, de sorte qu'on a accès ici ou là, mais il ne s'agit pas d'une seule grande base de données.

Je crois également qu'il sera beaucoup plus facile de bâtir cela à partir de notre structure actuelle que d'essayer de... Je suis de cet avis, mais il me semble que si nous le faisons, nous devons commencer par un lien numérique, d'accord? Supposons que moi, Frank Baylis, j'utilise le système. On me demande de prouver que je suis bien Frank Baylis. À l'heure actuelle, on me demande de taper mon NAS, et c'est assez facile d'en faire l'exploitation frauduleuse, n'est-ce pas? En revanche, si l'on doit faire un balayage de mes yeux ou obtenir d'autres caractéristiques biométriques, et que je dois répondre à des questions, il me semble que, pour revenir à ce que vous disiez, on couvre la protection des renseignements personnels et la sécurité.

Je crois que c'est la première chose que vous avez déclarée, madame Cavoukian. Ne pouvons-nous pas partir de là et nous entendre là-dessus avant de passer à tout le reste?

Je vous redonne la parole. Je vous ai interrompu. Je m'en excuse.

M. Michael Geist: Au risque de dire qu'il s'agit d'un cercle vicieux, fournir des renseignements biométriques me pose problème à moins qu'un cadre juridique en matière de protection des renseignements personnels répondant aux normes actuelles en la matière ne soit établi au Canada.

M. Frank Baylis: D'accord. Alors vous dites qu'avant d'en arriver là, avant de nous engager dans cette voie, il vaudrait mieux que nous soyons absolument sûrs que la protection des renseignements personnels est assurée.

M. Michael Geist: Il ne s'agit pas seulement de cela. Un ensemble de règles qui remontent à des décennies s'appliquent à ce système.

M. Frank Baylis: Cela ne fonctionne pas.

M. Michael Geist: Je ne crois pas qu'il est possible de dire qu'on se tourne vers les moyens les plus modernes possible et le numérique le plus possible si l'on s'appuie sur des lois qui remontent aux années 1980 pour protéger le système.

M. Frank Baylis: Voulez-vous intervenir? Me reste-t-il du temps?

Le président: Si elle pouvait répondre en 20 secondes, ce serait bien.

Mme Ann Cavoukian: Monsieur Baylis, je veux seulement dire que je suis d'accord avec vous. Nous devons explorer les nouvelles technologies. Cela ne fait aucun doute. Pour ajouter à ce qu'a dit Michael, je dirais que nous devons seulement veiller à mettre nos lois à jour. Elles sont tellement dépassées. Nous devons nous assurer que la technologie nous permet vraiment de protéger l'information et que personne d'autre ne peut y avoir accès.

J'ai donné l'exemple du chiffrement biométrique. Les technologies de reconnaissance faciale qu'on voit un peu partout suscitent beaucoup d'inquiétudes à l'heure actuelle; on utilise la reconnaissance faciale à des fins jamais voulues. Je collabore avec une entreprise israélienne, D-ID, qui peut, en fait, masquer l'identificateur personnel de sorte qu'il soit impossible d'utiliser la reconnaissance faciale.

Il y a un certain nombre de difficultés. Je suis certaine que nous pouvons les régler pourvu que nous le fassions en amont afin de prévenir les préjudices.

Le président: Merci, monsieur Baylis.

C'est au tour de M. Kent. Il s'agit d'une autre intervention de cinq minutes.

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

La conversation est très intéressante. Elle sera abrégée en raison des votes, et j'en suis désolé. Vous pouvez vous attendre à ce qu'on vous rappelle tous les deux dans les jours et les mois à venir.

Dans deux ou trois rapports, notre comité a recommandé au gouvernement d'examiner le Règlement général sur la protection des données et de renforcer et moderniser le Règlement sur la protection des renseignements personnels du Canada dans son ensemble et les pouvoirs du commissaire à la protection de la vie privée.

Je me demande si vous pouvez prendre les dernières minutes que nous avons pour faire des mises en garde. Le gouvernement semble indiquer que le gouvernement numérique s'en vient, que c'est sur le point d'être présenté sous une forme ou une autre. Je me demande si vous avez tous les deux des mises en garde à faire au gouvernement avant qu'il n'aille trop loin.

Madame Cavoukian.

Mme Ann Cavoukian: J'appuie totalement le commissaire Daniel Therrien, qui demande au gouvernement fédéral une mise à jour de la LPRPDE, par exemple, qui remonte au début des années 2000. Il a dit également que nous devons ajouter à la nouvelle loi la protection de la vie privée dès l'étape de la conception, car après tout, elle a été intégrée dans le Règlement général sur la protection des données. Nous avons besoin de nouveaux outils. Nous devons agir en amont. Il nous faut déterminer les facteurs de risque et contrer les risques. Nous pouvons le faire.

Il est absolument essentiel de mettre les dispositions à jour. Il est indispensable de donner au commissaire les pouvoirs dont il a besoin, mais qu'il n'a pas présentement. J'ai été commissaire à la protection de la vie privée pendant trois mandats, et je peux dire que j'avais le pouvoir de rendre des ordonnances. J'y ai rarement eu recours, mais c'est ce qui me permettait d'arriver à une résolution informelle avec des organismes, des ministères qui ne respectaient pas les dispositions sur la protection de la vie privée. C'était une bien meilleure façon de travailler.

J'avais le bâton. Si je devais rendre une ordonnance, je pouvais le faire. C'est ce qu'il manque au commissaire Therrien. Nous devons lui donner ce pouvoir supplémentaire et intégrer dans la nouvelle loi la protection de la vie privée dès l'étape de la conception de sorte que le gouvernement ait des mesures supplémentaires lui permettant d'examiner de façon anticipée un modèle de prévention, un peu comme un modèle médical de prévention. Ce serait bien plus facile si nous avions cela. Alors, la tâche du commissaire à la protection de la vie privée serait grandement allégée.

Merci.

● (1640)

L'hon. Peter Kent: Monsieur Geist.

M. Michael Geist: J'aimerais tout d'abord féliciter votre comité pour les rapports qu'il a produits au cours de la dernière année environ. Je crois qu'ils sont excellents et qu'ils ont alimenté bon nombre de discussions publiques à cet égard. Je crois que c'est vraiment utile.

J'ignore ce que pense le gouvernement à ce sujet. Je sais qu'il a tenu une consultation concernant une stratégie nationale sur les données. Je suppose qu'à certains égards, j'attends de voir ce qui en résultera. En ce qui concerne la stratégie nationale sur les données, pour revenir à ce que j'ai dit, si l'on adopte une approche holistique qui tient compte du fait qu'une partie de ce dont il est question dans ce contexte, inclut des questions liées à la gouvernance des données, à la LPRPDE, au secteur privé, au secteur public et à la Loi sur la protection des renseignements personnels — dont certaines des questions concernant l'application qu'a soulevées maintes fois le commissaire à la protection de la vie privée —, j'en conclus qu'on reconnaît qu'il est extrêmement important de procéder de la bonne façon pour un certain nombre de raisons, dont la possibilité d'utiliser certains des services en ligne que le gouvernement pourrait vouloir établir.

L'hon. Peter Kent: À quel point le consentement est-il essentiel dans ce processus?

M. Michael Geist: Le consentement est considéré comme un principe fondamental depuis longtemps. Je crois que l'une des raisons pour lesquelles nous sommes confrontés à certaines de ces questions nous ramène à la question de M. Erskine-Smith, soit pourquoi nous ne pouvons pas trouver un moyen d'informer quelqu'un et essayer de faire les choses de la bonne façon. Le problème, c'est en partie que théoriquement, nous pourrions déterminer si nous pouvons trouver un mécanisme qui permettrait aux citoyens de consentir à ce que le fournisseur de services — dans ce cas, le gouvernement — les informe des services auxquels ils ont droit. Je dirais que nos normes de consentement sont devenues tellement polluées par les normes peu élevées de la LPRPDE que peu de gens ont confiance en ce que signifie le consentement à ce moment-ci.

L'une des choses que nous devons, à mon avis, reprendre, c'est d'essayer de trouver des mécanismes pour que le consentement explicite soit vraiment explicite, éclairé. Nous nous sommes vraiment égarés sur ce plan. Le Règlement général sur la protection des données sera peut-être l'un des éléments moteurs à cet égard.

Le président: Il vous reste 30 secondes, monsieur Kent.

L'hon. Peter Kent: Madame Cavoukian.

Mme Ann Cavoukian: Je suis entièrement d'accord avec Michael. Il a tout à fait raison de dire que la notion de consentement n'existe presque pas tellement elle a été réduite.

Vous voyez, il est essentiel qu'il y ait un contrôle pour le consentement. La protection de la vie privée consiste à contrôler l'utilisation de ses données. Si une personne n'y consent pas de façon positive, affirmative, elle ne sait pas ce qu'il advient de ses données. On ne peut s'attendre à ce que les gens essaient de déchiffrer le jargon juridique contenu dans les conditions d'utilisation et les politiques de confidentialité pour trouver la disposition de non-participation leur permettant de refuser que les données soient utilisées à d'autres fins; la vie est trop courte. Personne ne le fait, mais ce n'est pas parce que les gens ne se soucient pas grandement de la protection de leur vie privée.

Au cours des deux dernières années, tous les sondages d'opinion publique de Pew Internet Research ont montré que la proportion des gens qui sont inquiets à propos de la protection de leur vie privée se situe dans les 90 %. Cela fait bien au-delà de 20 ans que je travaille dans le domaine, et c'est la première fois que je vois qu'une aussi grande proportion de gens se disent préoccupés à cet égard: 91 % des personnes sondées sont très inquiètes pour leur vie privée et 92 % craignent la perte de contrôle sur leurs données.

Un fort consentement positif est essentiel.

Le président: Merci, madame Cavoukian.

C'est maintenant au tour de M. de Burgh Graham, qui dispose de cinq minutes.

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

Anita voulait d'abord poser une question très brève. Je poserai mes questions par la suite.

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

Puisque mon collègue m'a cédé une partie de son temps d'intervention, je vous serais reconnaissante de répondre brièvement.

Je veux signaler à quel point je suis heureuse que nous accueillions encore une fois un spécialiste qui représente l'Université d'Ottawa, qui se trouve ici, à Ottawa. C'est bien que M. Geist soit parmi nous.

Monsieur Geist, vous avez parlé de l'analyse prédictive à laquelle le gouvernement a déjà recours. Il y a l'exemple de la fraude à l'ARC et la capacité de prédire. Si nous devions opter pour la minimisation des données et l'utilisation des données uniquement aux fins pour lesquelles elles ont été recueillies, cela empêcherait-il le gouvernement d'utiliser ce type d'analyse prédictive?

● (1645)

M. Michael Geist: Pas nécessairement. Je vais commencer par cela. Pensez à la controverse qu'on a vue l'an dernier dans l'affaire de Statistique Canada et des données bancaires. J'ai pensé qu'une des véritables faiblesses de Statistique Canada était son incapacité à démontrer que l'organisme ne pourrait pas atteindre ses objectifs s'il ne collectait pas des quantités massives de données bancaires des Canadiens. De même, par rapport à votre question, je suppose que cela dépend. Si des preuves démontrent que la quantité de données actuelle ne permet pas une aussi grande efficacité qu'avec un plus grand volume de données, il faut alors en tenir compte dans l'analyse coûts-avantages. Il pourrait être sensé d'en collecter plus, dans certains cas, mais je pense qu'il vous incombe de faire cette analyse avant même de collecter des données en disant: « Plus nous avons de données, mieux c'est. »

Mme Anita Vandenbeld: Merci.

M. David de Burgh Graham: Monsieur Geist, je veux d'abord vous remercier de votre commentaire sur l'accès à Internet. Actuellement, dans ma circonscription, comme je l'ai indiqué à maintes reprises sur de nombreuses tribunes, moins de la moitié de la population a une connexion à 10 mégabits par seconde ou plus rapide. Encore aujourd'hui, dans ma circonscription, beaucoup ont un accès par satellite ou même par ligne commutée. Nous en avons assez d'être laissés pour compte dans ce dossier; je vous remercie d'avoir soulevé ce point.

En ce qui concerne la collecte de données, comment peut-on prévoir, définir et déclarer quelles données sont nécessaires ou non? On dit qu'on ne collecte que le nécessaire. Comment est-ce déterminé?

Mme Ann Cavoukian: Puis-je prendre la parole?

M. David de Burgh Graham: N'importe qui peut répondre.

Mme Ann Cavoukian: Ce qu'il faut savoir, lorsqu'on collecte des données du public, c'est que les gens ne fournissent pas leurs renseignements personnels pour que vous les utilisiez à votre guise. Ils vous les donnent pour une raison précise. Ils doivent payer leurs impôts; c'est obligatoire. Ils en sont conscients. Ce sont des citoyens respectueux des lois. Ils vous donnent les renseignements nécessaires, mais cela ne veut pas dire pour autant que vous — le gouvernement — pouvez les utiliser comme vous voulez. Ils vous les donnent à des fins précises. C'est le principe de la spécification des finalités, de la limitation de l'utilisation. Vous êtes tenus d'utiliser les renseignements uniquement aux fins précisées. C'est un principe fondamental de la protection des renseignements personnels et des données. Les données à caractère personnel, qui sont de nature délicate, doivent servir aux fins prévues.

Michael a mentionné la débâcle lorsque Statistique Canada voulait obtenir les données financières de tout le monde auprès des banques. Vous plaisantez? Je suis certaine que vous êtes conscients de l'indignation que cela a suscitée. Ils voulaient collecter les données de 500 000 ménages. Multipliez cela par quatre. C'est totalement inacceptable.

Vous devez indiquer très clairement comment vous comptez utiliser les données et obtenir le consentement pour cette fin précise.

M. David de Burgh Graham: C'est exactement à cela que je voulais en venir.

Je veux revenir sur quelque chose qui s'est produit récemment aux États-Unis.

Récemment, l'Electronic Frontier Foundation — ou EFF — a découvert que les systèmes RAPI, les systèmes de reconnaissance automatique des plaques d'immatriculation, forment un réseau aux États-Unis et échangent des informations sur les déplacements des gens au pays, ce qui n'est manifestement pas ce à quoi ces appareils devaient servir.

Où se situe la limite entre collecte de données volontaire et involontaire? Par exemple, devriez-vous être informé si un système RAPI enregistre votre numéro de plaque d'immatriculation lors de votre passage? Si oui, devriez-vous avoir un droit de retrait en bloquant votre numéro de plaque, sachant que ce n'est pas la raison d'être de ce système et que c'est illégal, à bien des égards? Où se situe la limite pour ce genre de choses?

J'ai seulement une minute, environ.

Mme Ann Cavoukian: Les plaques d'immatriculation ne sont pas censées être utilisées à cette fin. Elles ne sont pas censées servir à surveiller vos déplacements. C'est ainsi que la surveillance prend une ampleur considérable.

J'ai une petite histoire cocasse à raconter. Steve Jobs, le fondateur d'Apple, évidemment, avait l'habitude d'acheter une nouvelle Mercedes blanche tous les six mois, moins un jour. Il retournait alors son véhicule et en achetait un autre identique. Pourquoi? Parce qu'à l'époque, en Californie, la plaque d'immatriculation n'était pas obligatoire; les gens avaient six mois pour immatriculer leur véhicule. Il ne voulait pas être suivi. Donc, tous les six mois, moins un jour, il retournait le véhicule et en achetait un autre, et ainsi de suite.

Ce n'était qu'un exemple. Les gens ne veulent pas être suivis. Ce n'est pas la raison d'être des plaques d'immatriculation. Il faut recommencer à utiliser les renseignements personnels aux fins prévues. Voilà l'objectif.

M. David de Burgh Graham: D'accord.

Si on ne centralise pas, dans une certaine mesure, qu'on maintient le cloisonnement actuel qu'on voit au gouvernement et qu'on n'améliore pas la convivialité, quelle est l'utilité de tendre vers un gouvernement intelligent?

Mme Ann Cavoukian: Eh bien, « gouvernement intelligent » ne signifie pas qu'il faut identifier tout le monde et suivre leurs activités. En tout respect, ce n'est pas ce qu'on entend par « gouvernement intelligent ». Si c'est la définition qu'on lui donne, alors il n'y a plus de liberté. Ce ne sera plus une société libre et ouverte. Il faut s'y opposer. On entend par là qu'il faut assurer la prestation de services modernes à un grand nombre de personnes tout en respectant leur droit à la vie privée. On peut faire les deux; cela doit être l'objectif.

Le président: Merci. Le temps est écoulé.

Le prochain intervenant est M. Angus, pour trois minutes, encore une fois.

Avant que vous ne commenciez, je précise que nous avons un peu de temps. La sonnerie se fera seulement entendre à 17 h 15. Nous poursuivrons la réunion jusqu'à 17 h 5, environ. Donc, prenez votre temps. Je pense que nous avons assez de temps pour que tout le monde puisse terminer.

Allez-y, monsieur Angus.

● (1650)

M. Charlie Angus: Merci.

À l'opposition, une de nos préoccupations au fil des ans portait sur l'idée de donner plus d'outils à la police, car si on lui en fournit, elle les utilise. Mon collègue, M. Erskine-Smith, laisse entendre que si nous obtenons les données et les renseignements personnels de tout le monde, le gouvernement pourra les aider en leur envoyant de l'information.

Je siège à l'opposition depuis 15 ans, et j'ai souvent vu des gouvernements utiliser ces ressources pour faire la promotion d'un formidable plan de lutte contre les changements climatiques ou d'une excellente prestation fiscale pour enfants. Personnellement, je trouve très préoccupant que vous ayez les données de tout le monde, car cela vous donnerait la possibilité de diffuser de tels messages dans les mois précédant une élection.

Je représente une région rurale où beaucoup de gens ont très difficilement accès à Internet, mais on dit pourtant aux personnes âgées que les formulaires papier ne sont plus acceptés et qu'ils doivent présenter des demandes en ligne.

Nous obligeons les citoyens à prendre le virage numérique. Les citoyens sont obligés d'utiliser des moyens numériques pour communiquer avec le gouvernement, mais ils ne veulent pas que le gouvernement communique avec eux par la suite. Donc, quelles protections devons-nous mettre en place pour limiter la capacité d'un gouvernement d'utiliser cette quantité phénoménale de données pour faire de l'autopromotion au détriment, sans doute, des autres partis politiques?

M. Michael Geist: Je peux commencer.

Vous avez soulevé deux enjeux distincts. D'abord, le fait qu'on oblige les gens à faire le virage numérique, un enjeu que nous avons déjà abordé brièvement. Je pense qu'il est frappant de voir que cet enjeu est soulevé par les députés des deux côtés, ce qui est le cas depuis de nombreuses années. J'ai comparu devant divers comités et nous avons discuté du problème de l'accès. Je dois avouer que je trouve toujours aussi mystérieux qu'on n'ait pas réussi à progresser plus efficacement pour combler le fossé numérique...

M. Charlie Angus: Il existe toujours.

M. Michael Geist: ... qui perdure. Une partie de la solution consiste à affirmer que tous ont besoin d'un accès abordable. Voilà ce qu'il faut faire, et il faut prendre un engagement en ce sens.

En outre, essentiellement, vous avez parlé de ce qui se produit lorsque les données sont utilisées à des fins bien différentes des attentes des gens ou de ce qu'ils avaient prévu. Dans le secteur privé, on dirait que c'est une atteinte à la vie privée. Vous collectez les données en m'informant de l'usage que vous en ferez. Si vous les utilisez ensuite à des fins pour lesquelles vous n'avez pas obtenu le consentement adéquat, je peux alors, théoriquement, prendre des mesures contre vous ou porter plainte, à tout le moins.

Une partie du problème — et cela nous ramène même à la discussion avec M. Baylis —, c'est qu'à l'échelon fédéral, nous n'avons pas encore de lois assez étoffées pour empêcher que les données soient utilisées à mauvais escient. Au fil de nombreuses années, en particulier à l'époque où l'on discutait de l'accès légal et d'autres choses du genre, on revenait très souvent à l'idée qu'il faut absolument utiliser les données que nous avons. On trouvera toujours une raison pour le faire. Je pense qu'il faut à la fois établir un ensemble de règles et des cadres pour assurer la mise en place de mesures de protection appropriées accompagnées d'une surveillance adéquate. En fin de compte, je pense que vous devez veiller à ce que les gouvernements, comme les entreprises, reconnaissent qu'ils causent un tort considérable à l'écosystème de l'information lorsqu'ils utilisent les données de façon trop agressive, ce qui a pour effet, à terme, de saper la confiance du public, non seulement à leur égard, mais aussi à l'égard des gouvernements en général.

M. Charlie Angus: C'est aussi une question de démocratie, parce que même s'ils disent avoir l'intention d'obtenir le consentement et que 10 % de la population le donne, ils obtiennent tout de même les informations, peut-être même de bons renseignements et de bonnes nouvelles qui pourraient être à leur avantage sur le plan démocratique.

Il y a un enjeu distinct dont nous n'avons pas parlé, je pense, soit la nécessité de protéger l'égalité démocratique des citoyens, tant ceux qui choisissent de donner leur consentement que ceux qui ne le donnent pas. S'ils ont affaire avec le gouvernement, c'est parce qu'ils n'ont pas le choix et parce qu'ils doivent régler un problème avec leur carte d'assurance sociale ou avec l'ARC, par exemple. Voilà pourquoi ils les obtiennent; l'information n'est pas fournie sans raison.

Pour moi, c'est semblable aux cases qu'il faut cocher pour donner son consentement avec les entreprises du secteur privé. Si le gouvernement utilisait cela, il s'en donnerait à coeur joie jusqu'à l'élection.

M. Michael Geist: Je pense que vous avez raison. Je pense que le consentement demeure très faible, mais il convient de reconnaître — et je sais que le Comité a aussi discuté de cet aspect — que nos partis politiques ne sont toujours pas visés par de telles règles de protection des renseignements personnels.

M. Charlie Angus: Voulez-vous que cela figure au compte rendu?

Des voix: Ha, ha!

M. Michael Geist: Quant à l'idée d'affirmer qu'il s'agit d'une question de démocratie, oui, c'est une question de démocratie. Cela pose véritablement problème que nos partis politiques puissent collecter des données sans être tenus de respecter des normes en matière de protection de la vie privée semblables à celles qu'on impose à toute société privée.

Le président: Merci, monsieur Angus.

Il nous reste deux intervenants, puis nous arrivons à la fin de la réunion.

Nous avons Mme Anita Vandenbeld et M. Picard.

● (1655)

M. Michel Picard (Montarville, Lib.): Je cède la parole à Mona.

Le président: Allez-y.

[*Français*]

Mme Mona Fortier (Ottawa—Vanier, Lib.): Merci, monsieur le président.

J'ai deux questions à poser.

Nous avons abordé ce point brièvement, mais il est important de le comprendre. La collecte de données et l'accès à celles-ci sont perçus négativement par certaines parties de la population canadienne. Il est dommage que certains de ces outils, dont des travaux mis en œuvre par Statistique Canada, soient utilisés par des partis politiques pour faire peur aux Canadiens et aux Canadiennes. Nous parlons ici des tiers partis.

Comment pouvons-nous gagner la confiance des Canadiens et des Canadiennes en vue de mettre en vigueur certaines de ces mesures qui ont comme but, ultimement, de permettre aux Canadiens d'accéder au gouvernement et de leur offrir des services?

[*Traduction*]

Mme Ann Cavoukian: J'aimerais seulement dire une chose. Il y a plusieurs choses que nous pouvons faire, évidemment, mais vous avez demandé comment nous pouvons regagner la confiance du public à l'égard des activités du gouvernement. Respectueusement, je dirais qu'il y a eu l'an dernier une chose qui a miné cette confiance encore plus. La commissaire fédérale à la protection de la vie privée a demandé au premier ministre Trudeau d'inclure les partis politiques dans les lois sur la protection de la vie privée, et il a refusé. Essentiellement, il a choisi de ne pas aller dans cette direction.

C'était extrêmement décevant. Pourquoi les partis politiques ne seraient-ils pas soumis aux lois en matière de protection de la vie privée, à l'instar des entreprises et des ministères? Malheureusement, peu de mesures sont prises pour accroître la confiance à l'égard du gouvernement. Je pense, respectueusement, que c'est un aspect très négatif. Je pense que c'est ce genre de choses...

En outre, M. Trudeau a appuyé Statistique Canada dans ses efforts pour obtenir les renseignements financiers très sensibles du public. Cela a suscité une forte opposition. Cela n'a pas été divulgué, mais les banques ont offert au statisticien en chef de Statistique Canada... Elles ont dit: « Nous allons analyser les données et vous les remettre après avoir retiré tous les renseignements qui permettent d'identifier les personnes. Vous pouvez avoir les données dont vous avez besoin, mais la confidentialité sera protégée puisque nous retirerons les identificateurs. » Quelle a été la réponse de Statistique Canada? « Non, nous voulons les données en format identifiable. » D'après ce qui m'a été dit en toute confidentialité, Statistique Canada voulait faire beaucoup de recoupements avec les données financières très sensibles de la population. C'est totalement inacceptable.

Madame, ce n'est qu'un exemple de ce qui contribue à éroder la confiance plutôt qu'à la renforcer.

Merci.

[*Français*]

Mme Mona Fortier: Monsieur Geist, que feriez-vous?

[*Traduction*]

M. Michael Geist: Il m'est difficile de suivre Ann sur ce point. Elle a donné deux exemples. Je vais vous en donner un autre, un très petit exemple qui ne fait pas les manchettes.

J'ai participé activement à l'élaboration de mesures législatives qui ont mené à la création de la liste des numéros de télécommunication exclus et de la loi antipourriel. Les partis politiques se sont toujours exclus eux-mêmes, au nom de la démocratie. Si vous voulez commencer à parler des façons d'assurer le respect, les partis politiques doivent d'abord cesser de s'exempter de l'interdiction de faire des appels indésirables à l'heure du souper et d'envoyer des pourriels.

Je pense que le respect commence par le respect de la vie privée des Canadiens. Il est juste de dire que lorsqu'il est question de restrictions réelles et de la capacité d'utiliser l'information, les partis politiques... Je pense qu'il faut que ce soit tout à fait clair: c'est arrivé sous des gouvernements conservateurs et sous des gouvernements libéraux. Cela ne se limite pas au gouvernement actuel. Je dirais qu'au fil de l'histoire, les gouvernements ont toujours été plus à l'aise, concernant les questions de protection de la vie privée, d'établir des normes élevées pour tout le monde sauf pour eux-mêmes. On le voit dans les exemptions, on le voit dans l'incapacité, pendant des décennies, de faire une véritable mise à jour de la Loi sur la protection des renseignements personnels, et on le constate dans les exemples que Mme Cavoukian vient de donner.

[*Français*]

Mme Mona Fortier: Je vous remercie.

Monsieur Picard, voulez-vous poser l'autre question?

[*Traduction*]

Le président: Merci. Le temps est écoulé.

Madame Cavoukian, monsieur Geist, merci d'être venus. C'est un sujet important. Comme nous l'avons mentionné, nous nous sommes heurtés à cet iceberg à maintes reprises, et il semble prendre continuellement de l'ampleur. Merci du temps que vous nous avez accordé aujourd'hui.

Nous passons à huis clos pendant cinq minutes pour traiter de travaux du Comité.

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