



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 027 • 1^{re} SESSION • 42^e LÉGISLATURE

TÉMOIGNAGES

Le jeudi 6 octobre 2016

—
Président

M. Blaine Calkins

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

Le jeudi 6 octobre 2016

• (1100)

[Français]

Le vice-président (M. Joël Lightbound (Louis-Hébert, Lib.)): Bonjour à toutes et à tous.

Je vous souhaite la bienvenue à cette séance du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique. Le président, M. Calkins, n'est pas ici aujourd'hui et je vais donc le remplacer. La réunion du Comité sera donc présidée en français.

Je veux remercier les différents témoins de leur présence parmi nous aujourd'hui, soit Mme Chantal Bernier, de Dentons Canada, qui a aussi été pendant six ans au Commissariat à la protection de la vie privée du Canada; Mme Monique McCulloch, de Services partagés Canada; et M. Maxime Guénette et Mme Marie-Claude Juneau, de l'Agence du revenu du Canada.

Chaque groupe aura 10 minutes pour faire une présentation et il y aura par la suite une période de questions de la part des membres du Comité.

Je vais commencer dans l'ordre que j'ai ici devant moi, soit avec vous, madame Bernier. Nous vous écoutons.

Mme Chantal Bernier (avocate-conseil, Groupe mondial de la vie privée et cybersécurité, Dentons Canada): Merci, monsieur le président.

Tout d'abord, j'aimerais mentionner le plaisir et l'honneur que je ressens de revenir devant vous aujourd'hui. C'est un retour pour moi. Je suis très honorée de pouvoir éclairer vos débats sur une question aussi importante.

Je vais faire ma présentation dans les deux langues officielles. Je suppose que 27 ans à titre fonctionnaire, cela laisse ses marques. Je vais donc commencer en français et je passerai par la suite à mes propos en anglais.

D'emblée, je vais vous dire que je suis totalement en accord avec les recommandations du commissaire à la vie privée de la protection de la vie privée du Canada sur la refonte de la Loi sur la protection des renseignements personnels. D'ailleurs, c'est le cadre de ma déclaration aujourd'hui.

Afin de ne pas dépasser le temps qui m'est imparti, j'ai choisi d'approfondir seulement quelques questions qui me paraissent prioritaires. Évidemment, je serai heureuse de répondre à toute autre question que je n'aurai pas traitée durant ma présentation. Sans plus tarder, je vais passer à la première remarque que je veux faire.

La première recommandation que je voudrais souligner est celle qui se rapporte à l'exigence d'accords écrits régissant la communication de renseignements personnels. À l'appui de cette recomman-

ation, je vous réfère à deux documents, à savoir le rapport du juge O'Connor, dans le cadre de la Commission d'enquête sur les actions des responsables canadiens concernant Maher Arar, ainsi que le rapport spécial intitulé « Mesures de vérification et de contrôle », que j'ai eu l'honneur de déposer au Parlement le 28 janvier 2014 avec l'appui de l'excellent personnel du Commissariat à la protection de la vie privée du Canada et l'apport — c'est important de le souligner — de cinq conseillers extérieurs spécialistes en matière de sécurité publique.

Commençons donc par le rapport d'enquête du juge O'Connor dans l'affaire Arar.

Le juge O'Connor a conclu que les autorités gouvernementales canadiennes, à cause du partage des données personnelles de M. Arar vers l'étranger, avaient contribué à la torture d'une personne innocente. Dans l'espoir que cela ne se reproduise jamais, il a recommandé que le Canada encadre mieux le transfert des renseignements personnels vers l'étranger. C'est là toute la pertinence de la recommandation du commissaire à la protection de la vie privée.

Dans l'introduction du rapport spécial que j'ai déposé le 28 janvier 2014, les experts que nous avons consultés ont fait ressortir par ailleurs comme changements déterminants au chapitre du contexte de la sécurité publique l'aplanissement des frontières territoriales, à savoir celles qui sont nationales et internationales, de sorte qu'il en découle une nécessité de partager des renseignements personnels.

Devant cette convergence de nécessité et de risques, je crois que l'exigence d'accords écrits qui encadrent mieux le partage de renseignements s'impose pour deux raisons majeures: d'abord, pour protéger les droits fondamentaux, et aussi, pour assurer la reddition de comptes de la part des agences gouvernementales pour ce qui est de la protection de ces droits fondamentaux. La recommandation du Commissariat est donc très pertinente et même urgente à cet égard.

• (1105)

[Traduction]

Passons maintenant à la deuxième recommandation que j'aimerais souligner dans ma liste de priorités. Il y a restriction de la collecte à un programme gouvernemental selon la pertinence à une activité.

À ce sujet, j'aimerais aller plus loin que le commissaire à la protection de la vie privée. J'appuie sans réserve sa proposition; toutefois, je préférerais ancrer l'obligation de nécessité non pas au programme ni à l'activité, mais à la Charte canadienne des droits et des libertés. Cela permettrait d'assurer une meilleure protection.

À vrai dire, permettez-moi de vous présenter un exemple concret dans le cadre du travail que j'ai effectué pendant presque six ans sur la façon dont l'ancrage, ne relevant pas du programme ni de l'activité, est supérieur.

Au CPVP, nous avons reçu en 2009 une évaluation des facteurs relatifs à la vie privée de la GRC afin d'assurer la mise en place d'un programme permettant l'installation d'une caméra sur les véhicules de la GRC afin de capter le numéro des plaques d'immatriculation. On l'a appelé le programme de reconnaissance automatique des plaques d'immatriculation qui permettrait de conserver de l'information portant notamment sur les mandats non exécutés ou les interventions qui devaient être réalisées et n'ont pas pu l'être, la suspension d'un permis de conduire.

Ce système permettrait de conserver les données qui concordent à de l'information dans la base de données de la police pendant deux ans et il conserverait les données sans correspondance pendant six mois. Autrement dit, les données — soit la reconnaissance de la plaque d'immatriculation de Mme Untel qui faisait son épicerie à ce moment-là à ce supermarché — seraient conservées pendant six mois malgré l'absence de contravention. Nous nous sommes interrogés sur cette question et la GRC a affirmé que cela faisait partie du programme et nous leur avons répondu que cette mesure ne répond pas à aucune norme de nécessité aux termes de la Charte et celle-ci a préséance sur toute autre loi. La GRC a donc éliminé l'information et n'a pas conservé les données de la personne innocente.

Cela, pour moi, indique véritablement qu'il existe une protection supérieure en établissant un lien à la Charte plutôt que d'invoquer le programme en guise de justification.

La troisième priorité que je tiens à souligner porte sur l'obligation pour les institutions fédérales de consulter le Commissariat à la protection de la vie privée au sujet des mesures législatives et des règlements qui ont des retombées sur la vie privée avant de les déposer. Pour moi, toute la logique de cette recommandation repose d'abord sur le rôle du commissaire comme agent du Parlement, puis du caractère fondamental du droit à la vie privée.

Examinons le rôle et le statut du commissaire. Le commissaire à la protection de la vie privée est un agent du Parlement. Qu'est-ce que l'on entend par là? Cela signifie qu'il a le mandat de protéger une valeur si chère à l'identité canadienne et à la démocratie que cela passe avant la partisanerie politique et le commissaire relève directement du Parlement.

De par ce statut et du fait que la protection de la vie privée ait été confiée à une institution dotée de ce statut, il est tout à fait logique que le commissaire soit consulté au sujet des lois ou des règlements avant d'en assurer le dépôt pour veiller à ce que ceux-ci permettent de protéger la vie privée.

L'exemple que j'utiliserai ici qui, à mon avis, illustre clairement l'avantage de cette recommandation repose sur la série de projets de loi qui sont soit morts au feuillet, soit retirés, soit adoptés avec réserves relativement à l'accès légal. Ces projets de loi n'étant pas du tout conformes, ils n'ont pas survécu à l'opposition des politiciens et ils étaient indéfendables. Ils ont suscité des débats acrimonieux et ont ébranlé la confiance du public envers les institutions gouvernementales. J'estime qu'une consultation préalable auprès du commissaire à la vie privée aurait permis la tenue d'un dialogue entre les auteurs de projets de loi à l'interne et le commissaire à la vie privée afin de trouver un juste équilibre dans les projets de loi avant de les déposer et cela aurait donc permis d'obtenir une mesure législative mieux équilibrée.

La Loi antiterroriste de 2015, en outre, aurait pu assurer un meilleur équilibre entre les besoins légitimes de l'État et les droits fondamentaux des citoyens. Maintenant, le gouvernement actuel doit refaire le travail pour obtenir l'équilibre nécessaire et satisfaction.

• (1110)

[Français]

Je conclurai donc que devant la collecte, l'usage et le partage croissant de renseignements personnels, il faut moderniser la Loi sur la protection des renseignements personnels pour que sa portée et son effet correspondent à la réalité des risques et au besoin de protection.

Sur ce, monsieur le président, je serai heureuse de répondre à toutes les questions des membres du Comité.

Le vice-président (M. Joël Lightbound): Je vous remercie, madame Bernier, pour vos propos très clairs.

Je vais maintenant demander à Mme McCulloch, de Services partagés Canada, de prendre la parole.

[Traduction]

Mme Monique McCulloch (directrice, Accès à l'information, Services partagés Canada): Bonjour.

Je vous remercie monsieur le président et membres du comité pour m'avoir convié à venir vous décrire le cadre adopté par Services partagés Canada pour respecter la Loi sur la protection des renseignements personnels. Nous avons le plaisir de nous joindre à vous cet avant-midi.

Je m'appelle Monique McCulloch. Je suis directrice de la division de l'accès à l'information et de la protection des renseignements personnels qui fait partie de la Direction des services ministériels à Services partagés Canada. Je suis la coordonnatrice pour l'ensemble du ministère et je suis chargée d'administrer les obligations législatives et stratégiques de l'AIPRP.

J'aimerais ajouter que je suis ici au nom de Violaine Sauvé, qui est chef de la protection des renseignements personnels à Services partagés Canada.

Avant de décrire le cadre de l'AIPRP, j'aimerais vous dresser un certain contexte sur le mandat de Services partagés Canada.

[Français]

Services partagés Canada a été créé dans le but de moderniser les services d'infrastructure de technologie de l'information pour mettre en place une plateforme sécuritaire et fiable de prestation de services numériques à l'intention de la population canadienne. Le ministère entend offrir un seul système de services de courriel, de centres de données regroupés, de réseaux de télécommunications fiables et sécuritaires et une protection contre les cybermenaces 24 heures sur 24, 7 jours sur 7, 365 jours par année.

[Traduction]

Services partagés Canada offre actuellement des services d'infrastructure de technologie de l'information pour 43 ministères, 50 réseaux, 485 centres de données et 23 000 serveurs.

Pour l'exercice 2015-2016, toujours en pleine croissance, le bureau de l'AIPRP a retenu les services de quatre employés à temps plein ainsi que de deux employés à temps partiel — un occasionnel et un étudiant — afin d'exécuter des activités liées à la Loi sur la protection des renseignements personnels. Dans le cadre du programme d'AIPRP, Services partagés Canada a consacré un peu plus de 411 000 \$ à l'administration de la Loi sur la protection des renseignements personnels.

[Français]

Depuis sa création en août 2011, Services partagés Canada a instauré un cadre fondé sur des politiques internes, des directives et de la formation, qui définit les procédures et processus de traitement de demandes d'accès aux renseignements personnels ainsi que les questions de politiques présentées au titre de la loi.

[Traduction]

La Division de l'AIPRP a mis en place un cadre de gestion en matière d'accès à l'information et de la protection des renseignements personnels, lequel établit une structure détaillée de la gouvernance et des responsabilités. Au total, 14 instruments de politique de l'AIPRP ont été mis en place à Services partagés Canada, y compris une directive sur la réalisation d'évaluations des facteurs relatifs à la vie privée, ainsi qu'une norme sur la gestion des atteintes à la vie privée. Ces instruments rendent compte des responsabilités de Services partagés Canada au titre de la Loi sur l'accès à l'information et de la Loi sur la protection des renseignements personnels en ce qui concerne les droits d'accès et la collecte, l'utilisation, la communication, la conservation et la destruction de renseignements personnels.

La Division de l'AIPRP est chargée d'élaborer, de coordonner et de mettre en oeuvre des politiques, des lignes directrices, des systèmes et des procédures efficaces en matière d'AIPRP au sein de Services partagés Canada, et de surveiller leur conformité. Ce travail permet au ministère de répondre aux exigences et aux obligations établies aux termes de la Loi sur l'accès à l'information et de la Loi sur la protection des renseignements personnels.

[Français]

En ce qui concerne le volume de demandes pour des renseignements personnels, j'aimerais maintenant vous faire part de quelques statistiques tirées du rapport annuel de l'exercice 2015-2016 concernant la Loi sur la protection des renseignements personnels.

Au total, 123 demandes en vertu de la loi ont été traitées, dont 120 ont été achevées avant la fin de la période considérée. Les 120 demandes pour des renseignements personnels ont été traitées dans les délais prescrits par la Loi et aucune plainte n'a été déposée.

[Traduction]

La Division de l'AIPRP de Services partagés Canada fait le suivi hebdomadaire de ses délais de traitement des demandes et surveille le calendrier de traitement de celles-ci. Des rapports mensuels sur le rendement sont remis à la haute direction.

En 2013, Services partagés Canada a également participé au projet pilote en ligne initial relatif à l'accès à l'information et à la protection des renseignements personnels. Dirigé par le ministère de la Citoyenneté et de l'Immigration et le Secrétariat du Conseil du Trésor, le projet avait pour objectif de faciliter et d'accélérer les droits d'accès de la population canadienne. Aujourd'hui, parmi les initiatives pour un gouvernement ouvert, les demandes en matière d'accès à l'information et de protection des renseignements personnels que reçoivent les ministères sont en majeure partie présentées en ligne.

• (1115)

[Français]

Monsieur le président, je termine sur ces mots et je répondrai maintenant aux questions des membres du Comité.

Le vice-président (M. Joël Lightbound): Merci beaucoup, madame McCulloch.

Je vais maintenant céder la parole à M. Guénette et à Mme Juneau, qui représentent l'Agence du revenu du Canada. Vous disposez de 10 minutes.

M. Maxime Guénette (sous-commissaire et chef de la protection des renseignements personnels, Direction générale des affaires publiques, Agence du revenu du Canada): Merci, monsieur le président et membres du comité.

Je m'appelle Maxime Guénette. Je suis sous-commissaire de la Direction générale des affaires publiques et chef de la protection des renseignements personnels à l'Agence du revenu du Canada.

Aujourd'hui, je suis accompagné de Mme Marie-Claude Juneau, directrice, Accès à l'information et à la protection des renseignements personnels à l'Agence. Certains d'entre vous vous souviendrez sûrement de Mme Juneau puisqu'elle s'est adressée à vous plus tôt cette année dans le cadre de votre examen au sujet de la Loi sur l'accès à l'information.

Nous sommes donc tous les deux heureux de nous adresser à vous aujourd'hui afin de vous appuyer dans votre étude sur les réformes à la Loi sur la protection des renseignements personnels.

Avec ses quelque 40 000 employés, l'Agence est l'une des plus grandes institutions du gouvernement du Canada. Très peu d'organismes fédéraux interagissent avec les Canadiens autant que l'Agence. Seulement en 2014-2015, l'Agence a communiqué avec 31 millions de particuliers et d'entreprises.

Par conséquent, l'Agence détient l'un des plus grands fonds de renseignements personnels du gouvernement du Canada, comme l'a reconnu le commissaire à la protection de la vie privée. Elle prend donc très au sérieux ses obligations en vertu de la Loi sur la protection des renseignements personnels et les instruments de politique connexes.

En effet, la confiance que les Canadiens accordent à l'Agence pour ce qui est de protéger leurs renseignements est la pierre angulaire du régime canadien d'autocotisation volontaire. Plus précisément, selon l'article 241 de la Loi de l'impôt sur le revenu et l'article 295 de la Loi sur la taxe d'accise, les employés de l'Agence ne peuvent pas divulguer de renseignements sur les contribuables, sauf si ces lois les y autorisent précisément. La violation de ces dispositions est une infraction criminelle et peut entraîner de lourdes peines pouvant même aller jusqu'à l'emprisonnement.

En reconnaissant donc l'importance essentielle d'une gestion saine de la protection des renseignements personnels, et en suivant la recommandation du commissaire à la protection de la vie privée, l'Agence a nommé son premier chef de la protection des renseignements personnels en 2013. J'ai moi-même l'honneur d'assumer ce rôle depuis le mois d'août 2016. J'occupe maintenant ce poste depuis deux mois.

[Traduction]

À titre de chef de la protection des renseignements personnels, je supervise toutes les activités de gestion de la protection des renseignements personnels à l'agence. Cette surveillance est éclairée par la mesure de rendement continue dans des secteurs clés, dont la technologie de l'information, la sécurité, les communications et la formation.

Dans le cadre de mes fonctions, je dois fournir une surveillance, des conseils et un soutien afin d'atteindre la conformité aux exigences législatives et stratégiques. En ma qualité de chef de la protection des renseignements personnels, je suis aussi tenu d'informer au moins deux fois par année le Comité de gestion de l'Agence et le Conseil de direction de l'Agence de l'état de la gestion de la protection des renseignements personnels. De plus, je préside un comité de la haute direction qui aborde les questions de cette nature comme faisant partie intégrante des activités de l'agence.

Au cours des dernières années, l'agence a apporté de nombreux changements technologiques afin de renforcer les mesures de gestion de la protection des renseignements personnels. Nous avons renforcé les contrôles de première ligne de nos systèmes afin de veiller à ce que les employés aient accès seulement aux systèmes informatiques de l'ARC dont ils ont besoin pour accomplir leurs tâches. Nous avons renforcé les contrôles finaux pour permettre à nos systèmes automatisés de mieux surveiller les opérations effectuées par les employés. La mise en oeuvre de ces mesures de contrôle sera terminée l'an prochain et elles découlent d'une recommandation formulée par le commissaire à la protection de la vie privée dans son rapport d'évaluation de 2013.

Grâce à une approche progressive, l'agence a mis en oeuvre jusqu'à maintenant six des neuf recommandations formulées par le commissaire à la protection de la vie privée lors de sa vérification de 2013. Trois de ces recommandations visent un investissement pluriannuel, donc leur mise en oeuvre se poursuit. Nous prévoyons y avoir donné suite en 2017.

Dans l'ensemble, l'ARC a investi plus de 10 millions de dollars et prévoit faire d'autres investissements importants pour enrichir ses contrôles de gestion de l'identité et d'accès afin d'améliorer la protection et la confidentialité des renseignements des contribuables et de réduire le risque de fraude interne.

Nous avons également amélioré nos procédures afin de traiter et de gérer les atteintes à la vie privée en vue de pouvoir déclarer plus rapidement les atteintes substantielles à la sécurité des renseignements personnels au Commissariat à la protection des renseignements personnels et au Secrétariat du Conseil du Trésor.

Comme vous le savez, les Canadiens sont au fait des nouvelles technologies et sont aussi des consommateurs avides des contenus offerts sur Internet. Ce qui fait d'eux des clients avertis. Ils s'attendent donc, à juste titre, à ce que leurs interactions en ligne avec les institutions gouvernementales aient lieu avec la même qualité et la même rapidité que celles qu'ils ont avec des fournisseurs de services comme Google et Amazon. Par exemple, nous nous attendons à ce que plus de 86 % des Canadiens produisent leurs déclarations de revenus en ligne l'an prochain. Nous nous attendons à ce que le taux atteigne probablement environ 90 % d'ici trois ans.

L'agence continue d'ailleurs à investir pour améliorer ses services aux Canadiens, notamment grâce à de constants investissements dans les solutions informatiques telles que Mon dossier, Gérer le courrier en ligne et l'application MonARC. Pendant que nous veillons à suivre les dernières tendances novatrices et pour offrir aux contribuables le service toujours plus rapide, fluide et centré sur l'utilisateur auxquels ils s'attendent, nous devons nous assurer de prendre les mesures nécessaires pour protéger les renseignements personnels recueillis dans le cadre de notre travail.

• (1120)

L'ARC évalue ses progrès technologiques nouveaux et modifiés, les programmes et les activités du point de vue de la protection de la vie privée au moyen d'évaluations des facteurs relatifs à la vie privée

(ÉFVP). Depuis le début de l'exercice, nous avons effectué 16 de ces évaluations et nous sommes sur le point d'en réaliser environ 18 autres d'ici la fin de l'exercice. Notre plan englobe 20 ÉFVP actives à ce moment-ci. Il s'agit là d'un moyen d'assurer un juste équilibre entre les attentes des Canadiens en ce qui concerne l'amélioration du service et de veiller à ce que les nouvelles initiatives soient conformes aux exigences de la protection de la vie privée.

[Français]

L'Agence s'efforce aussi de veiller à ce que ses employés soient bien conscients de leurs responsabilités en ce qui a trait à la protection des renseignements personnels dont ils ont la garde. Le Code d'intégrité et de conduite professionnelle de l'Agence et son Cadre d'intégrité ont été des outils importants pour illustrer, auprès des employés, à quel point la protection des renseignements personnels des contribuables est un élément central de leurs responsabilités, et ce, même après leur départ de l'Agence.

Malgré ces mesures et les nombreux efforts déployés pour protéger les renseignements personnels, malheureusement, des atteintes à la vie privée se produisent occasionnellement. L'Agence est tout à fait consciente qu'en raison de la nature des renseignements qu'elle détient, les atteintes à la vie privée qui l'affectent peuvent être hautement dommageables à certains particuliers ou à certaines organisations. C'est dans cette optique que l'Agence examine tout incident touchant une atteinte à la vie privée avec un très haut niveau de rigueur. Bien entendu, nous pouvons toujours faire mieux et l'Agence cherche toujours des moyens d'améliorer ses pratiques de gestion de la protection de la vie privée en apportant des changements aux programmes, aux politiques et à la technologie.

Nous consultons d'ailleurs régulièrement le Commissariat à la protection de la vie privée du Canada et le Secrétariat du Conseil du Trésor à ce sujet. L'Agence dispose de solides processus politiques et de procédures pour assurer la conformité à l'égard de la Loi sur la protection des renseignements personnels et des instruments de politiques connexes. Des mesures de contrôle sont en place et nous continuons à les évaluer et à les améliorer sur une base continue. La responsabilité de protéger les renseignements des Canadiens est d'une importance fondamentale pour l'Agence et pour ce qu'elle fait. C'est pourquoi nous continuons de consacrer des efforts importants afin de satisfaire les attentes des Canadiens à cet égard.

J'espère avoir fourni aux membres du Comité un aperçu utile du contexte opérationnel de l'Agence du revenu du Canada en ce qui a trait à la Loi sur la protection des renseignements personnels.

Mme Juneau et moi serons très heureux de répondre à vos questions.

Je vous remercie.

[Traduction]

Merci, monsieur le président.

[Français]

L'vice-président (M. Joël Lightbound): Je vous remercie beaucoup, monsieur Guénette.

Nous allons maintenant entreprendre la première série de questions, qui sera d'une durée de sept minutes.

Nous allons commencer sans plus tarder par M. Long.

[Traduction]

M. Wayne Long (Saint John—Rothesay, Lib.): Merci, monsieur le président et je remercie les témoins de leur présence ici cet avant-midi. Il s'agit là d'un sujet très intéressant.

Mme Bernier, je vais vous poser quelques questions. On cite votre nom dans un article affiché sur le site Web des nouvelles du réseau anglais de la Société Radio-Canada, qui s'intitule « Chantal Bernier affirme qu'Ottawa fouine sur les médias sociaux ». On enchaîne en affirmant que vous avez sonné l'alarme — ou brandi un drapeau si vous préférez — au sujet du gouvernement qui recueille trop de données sur les médias sociaux et de la notion que si l'on affiche de l'information sur les médias sociaux — et je suis très actif sur les médias sociaux, dont Facebook et Twitter — c'est de bonne guerre pour tout le monde. Dans cet article, vous précisez avoir des preuves de la collecte de renseignements de la part du gouvernement. Pour citer cet article:

Le bureau de Bernier indique que divers organismes gouvernementaux ont adressé presque 1,2 million de demandes de renseignements personnels au sujet de Canadiens auprès de grandes compagnies de télécommunications canadiennes...

Cela tient un peu de la petite histoire.

Je désire obtenir votre opinion à ce sujet et également vos commentaires relativement à l'affaire Cindy Blackstock. J'aimerais avoir votre avis et obtenir certains antécédents au sujet de cette affaire. Comment est-elle pertinente? Quel est votre point de vue?

Mme Chantal Bernier: Toute cette histoire est pertinente. C'est exactement là où j'aurai l'occasion de vous démontrer comment le geste ne convient pas parfois.

M. Wayne Long: C'est ce que nous voulons.

Mme Chantal Bernier: Permettez-moi de débiter par l'affaire Cindy Blackstock, car, lorsque je préparais mes observations, je me suis demandé si j'allais utiliser l'ÉFVP — Évaluation des facteurs relatifs à la vie privée — de la GRC ou l'affaire Cindy Blackstock. Dans ce cas-ci, j'ai choisi la GRC, ce qui a eu un résultat positif. La GRC a bien fait et compris son travail, mais il fallait nous inspirer de la Charte.

Dans l'affaire Cindy Blackstock, c'est ce qui s'est produit. Deux ministères — le ministère des Affaires autochtones, comme on l'appelait à l'époque, et le ministère de la Justice — ont surveillé les activités de Cindy Blackstock, activiste des droits des enfants des Premières Nations.

• (1125)

M. Wayne Long: C'était en 2014?

Mme Chantal Bernier: J'ai publié le rapport en 2013. Cela avait eu lieu avant ce moment, donc c'était il y a environ deux ou trois ans.

M. Wayne Long: D'accord.

Mme Chantal Bernier: En tout cas, ce qui est très important, c'est qu'elle a vu qu'ils surveillaient ses comptes Facebook et qu'elle est donc venue nous voir. Nous sommes allés dans les ministères, et ils ont dit: « Mais, bien sûr. C'est public. Elle l'a publié sur Facebook. » Ils n'étaient pas du tout malicieux. Ils ont agi de bonne foi, mais nous avons conclu qu'ils enfreignaient la Loi sur la protection des renseignements personnels, parce que l'article 4 de la Loi stipule que vous ne pouvez pas recueillir de renseignements personnels qui ne sont pas liés à vos activités ou vos programmes, et ce n'était pas lié à leurs activités ou à leurs programmes. Ils ont répondu: « Mais ce n'est pas des renseignements personnels. Elle les a mis sur Facebook. »

La question cruciale en cette époque de technologie est « Que sont les renseignements personnels sur le Net? » Ceci a été précisé dans l'affaire *R. c. Spencer*, 2014, par la Cour suprême du Canada, qui a statué que les renseignements personnels sur le Net ne sont pas

publics. Ils demeurent personnels, car les renseignements personnels sont tout renseignement concernant un individu identifiable. Par conséquent, les publications que Mme Blackstock partageait avec son auditoire Facebook constituaient des renseignements personnels qui n'étaient pas destinés au gouvernement, et que le gouvernement ne pouvait pas justifier leur collecte comme s'ils avaient été liés à son mandat, soit la Justice ou les Affaires autochtones et, par conséquent, il a contrevenu à la loi.

M. Wayne Long: J'aimerais simplement faire une intervention. Vous avez dit qu'elle a fini par réaliser qu'ils la surveillaient.

Mme Chantal Bernier: Oui.

M. Wayne Long: Comment a-t-elle pris conscience de cela?

Mme Chantal Bernier: C'est ce que je cherche à savoir. Je suppose qu'elle a dû avoir quelques indications. Le fait qui me revient à l'esprit c'est que je crois qu'elle a commencé à remarquer que des fonctionnaires se présentaient à ses discours, et c'est là qu'elle a fait le lien.

M. Wayne Long: D'accord.

Mme Chantal Bernier: C'est une grande perfectionniste. Elle est très respectée, très forte intellectuellement et très astucieuse; je pense donc qu'elle avait rassemblé plusieurs indices. En effet, c'est bel et bien ce qu'elle a fait.

Tout cela a vraiment commencé par un manque de clarté au sujet de ce qu'étaient les obligations des ministères, ce qui m'a amenée, dans le rapport du 28 janvier 2014, à recommander aux ministères de lire les lignes directrices du Secrétariat du Conseil du Trésor à propos de la question des réseaux sociaux que vous avez soulevée.

M. Wayne Long: Vous avez envoyé une lettre, je crois, au président du Conseil du Trésor Tony Clement à ce moment-là.

Mme Chantal Bernier: Oui.

M. Wayne Long: Je sais que des remarques ont été formulées à la Chambre des communes selon lesquelles le gouvernement de l'époque voulait se débarrasser du long questionnaire de recensement parce qu'il le considérait intrusif, mais il surveillait pourtant les médias sociaux.

Veillez continuer avec ce qui s'est passé.

Mme Chantal Bernier: Ce qui s'est passé, c'est que, à ma connaissance, il n'y a eu aucun changement. J'ai cherché une annonce de directives sur les médias sociaux. Je ne sais pas si mes collègues de la fonction publique, qui sont encore mes collègues, ont vu quelque chose. Je n'ai certainement vu aucune annonce à l'effet que le gouvernement allait se conformer.

Je dois vous dire que le cas de Cindy Blackstock était celui que nous avons rendu public, mais nous avons également eu, des années auparavant — et c'est dans l'un des rapports annuels du commissaire à la protection de la vie privée du Canada — une évaluation des facteurs relatifs à la vie privée d'une agence gouvernementale où ils voulaient suivre les réseaux sociaux des fonctionnaires pour s'assurer que leurs activités politiques n'étaient pas illégales ou interdites. Bien que l'objectif soit louable — oui, c'est vrai, je suis tellement fier que nous ayons une fonction publique non politique — vous ne pouvez pas surveiller les employés. C'est personnel.

Dans mon esprit, cela nécessite plus de précisions afin que des directives claires soient transmises aux ministères.

•(1130)

[Français]

Le vice-président (M. Joël Lightbound): Je vous remercie beaucoup, M. Long et Mme Bernier.

Cela conclut cette période de sept minutes dont vous disposiez vous, monsieur Long.

Je cède maintenant la parole à Mme Rempel.

L'hon. Michelle Rempel (Calgary Nose Hill, PCC): Je vous remercie, monsieur le président.

[Traduction]

J'aimerais simplement revenir, madame Bernier, au témoignage que vous avez présenté. Je souhaiterais seulement clarifier quelque chose.

Vous avez mentionné l'exemple de l'utilisation des données de Facebook, puis vous avez comparé cela à l'affaire *R. c. Spencer*, n'est-ce pas? Juste pour clarifier, je crois que la décision rendue dans l'affaire *R. c. Spencer* se rattachait davantage à l'utilisation d'adresses IP et à la collecte de métadonnées. Est-ce exact?

Mme Chantal Bernier: Absolument. Ce sont des situations complètement différentes. Dans l'affaire Spencer, ce qui s'est produit, c'est que M. Spencer avait de la pornographie juvénile sur son compte, et cela a été détecté. Sans mandat — ceci est très important — sans aucun mandat, la police est allée chez Shaw, son fournisseur de services Internet, pour obtenir ses renseignements personnels derrière l'adresse IP, ce qui fut fourni par Shaw.

L'hon. Michelle Rempel: Juste pour clarifier, pour le Comité, car j'écoutez votre témoignage, et vous avez utilisé l'exemple d'une publication sur Facebook ou de la publication d'informations personnelles sur Facebook, puis vous avez utilisé l'exemple de l'affaire *R. c. Spencer* pour justifier pourquoi une publication Facebook ne serait pas applicable. Souhaitez-vous toujours faire ce lien?

Mme Chantal Bernier: J'ai fait ce lien tout comme j'ai fourni divers exemples de la nécessité de clarifier la qualité des renseignements personnels comme « personnels » sur Internet.

L'hon. Michelle Rempel: Juste pour être parfaitement claire, diriez-vous que la publication de, disons, des activités familiales ou d'une page Facebook aurait la même portée que la décision de *R. c. Spencer*? Je vous ai entendue faire ce lien dans votre témoignage et je ne suis pas certaine que ce soit la même chose. Disons que c'était des métadonnées, n'est-ce pas, par rapport à un message de blogue?

Mme Chantal Bernier: Oui. Tout d'abord, dans le cas de Spencer, ce que la cour dit — et cela est très important — c'est que les renseignements personnels ne sont pas ce qu'ils sont, ce sont ce qu'ils révèlent. C'est une notion dynamique.

L'hon. Michelle Rempel: Pour clarifier, diriez-vous que si un blogue était publié sur Facebook, puis qu'un ministère du gouvernement ou une personne utilisait cette information, la portée serait identique à celle de la décision *R. c. Spencer*?

Mme Chantal Bernier: Je dirais que si la publication du blogue, sa publication sur Facebook, n'est pas conçue pour le gouvernement et que le gouvernement ne peut justifier l'avoir recueillie dans l'intérêt du public, dans le cadre de son mandat, c'est une violation de la loi.

L'hon. Michelle Rempel: Est-ce votre avis, ou pouvez-vous indiquer une jurisprudence pertinente qui montre cela?

Mme Chantal Bernier: Eh bien, j'aimerais souligner les conclusions que j'ai faites en ce qui concerne Cindy Blackstock. C'était exactement la conclusion. Nous avons dit, « Écoutez, vous les membres du gouvernement du Canada, les publications de Mme Blackstock étaient personnelles. Vous les avez recueillies sans pouvoir justifier que cela fut fait dans le cadre de vos programmes ou activités; par conséquent, vous les avez recueillies en violation de la Loi sur la protection des renseignements personnels. »

L'hon. Michelle Rempel: Encore une fois, à titre d'éclaircissement pour le Comité présent, et pour que cela soit reflété dans notre rapport, *R. c. Spencer* ne serait pas vraiment pertinent dans l'exemple que vous avez donné auparavant.

Mme Chantal Bernier: Pour moi, l'affaire *R. c. Spencer* est cruciale, car elle détermine les critères sur lesquels s'appuyer pour la publication de renseignements personnels sur Internet. Les critères ne sont pas les renseignements en soi, mais ce qu'ils révèlent. Par conséquent, si tout ce que vous avez est, disons, une adresse IP, ce n'est pas l'annuaire téléphonique. Vous ne pouvez pas l'utiliser sous une forme statique et dire que c'est juste un petit numéro. Cela équivaut à ce que je dis, « Veuillez me donner la clé de votre maison », et vous dites, « Non », et je dis, « Pourquoi pas? C'est juste une petite pièce de métal. » C'est une pièce de métal qui me permet d'entrer dans votre maison.

L'hon. Michelle Rempel: En tant que législateurs, vous pouvez comprendre qu'il y a probablement une certaine confusion. Je suis d'accord avec vous qu'il y a une différence entre le consentement en termes de... et je pense, par extrapolation, à ce que nous faisons des données volumineuses dans leur ensemble. Je ne voudrais certainement pas que les activités de ma carte de débit ou que les résultats de mes recherches sur Google soient informatifs. Je pense qu'il s'agit d'une intéressante discussion politique même pour les entreprises qui utilisent cette technologie.

Cependant, pour moi, mettre quelque chose dans une publication Facebook avec des paramètres publics s'apparente à coller quelque chose sur un poteau de téléphone. À quel moment, nous, les législateurs, devons-nous retirer la nature du consentement quant à la divulgation de renseignements qui sont du domaine privé? La divulgation de renseignements dans le domaine public n'est-elle pas une reconnaissance de votre consentement à faire cela? En tant que tels, les renseignements seraient considérés comme publics.

Si je fais une grande déclaration au sujet de mes activités du week-end dans un format papier et que je l'affiche à l'extérieur, j'assume que quelqu'un peut l'utiliser. Je ne vois pas vraiment en quoi cela diffère d'une divulgation sous format électronique.

•(1135)

Mme Chantal Bernier: Le fait est que le gouvernement ne peut pas l'utiliser, parce qu'il ne peut pas utiliser vos renseignements personnels à moins qu'il en démontre la nécessité. C'est les critères de la Charte.

L'hon. Michelle Rempel: C'est intéressant, donc le critère est nécessaire.

Mme Chantal Bernier: Exactement.

L'hon. Michelle Rempel: Il ne s'agit pas nécessairement de la divulgation de vos renseignements dans le domaine public. Ceux-ci pourraient encore être utilisés. Ce n'est pas exclu. Il faut simplement observer ce critère juridique.

Mme Chantal Bernier: La nécessité est le critère fondamental. Il est formulé à l'article 1 de la Charte. Il dit précisément, « dont la justification puisse se démontrer dans le cadre d'une société libre et démocratique ». L'arrêt Oakes, avec lequel vous êtes probablement familiarisé, a été interprété comme étant vraiment basé sur quatre critères: la nécessité; la proportionnalité de l'atteinte à cette nécessité; l'efficacité de cette intrusion, pour laquelle vous devez prouver le fonctionnement réel, et l'absence d'une solution de rechange moins intrusive. C'est vraiment la clé.

L'hon. Michelle Rempel: Je vous remercie.

Est-ce qu'il me reste un peu de temps?

Le vice-président (M. Joël Lightbound): Malheureusement, non, mais nous vous reviendrons peut-être plus tard, si nous avons un peu de temps.

Notre prochaine série de questions sera de M. Dusseault.

[Français]

M. Pierre-Luc Dusseault (Sherbrooke, NPD): Merci, monsieur le président.

Je remercie aussi les témoins qui comparaissent devant nous aujourd'hui.

Je suis heureux de vous revoir, madame Bernier.

Mes premières questions porteront sur la recommandation n° 5 du commissaire, soit celle qui propose d'accroître les motifs de recours devant la cour. Je pense plus particulièrement à la partie de la dernière phrase où il est question de « [...] conférer à la Cour le pouvoir d'ordonner une série de mesures de redressement, y compris pour dommages-intérêts. », ce qui n'est pas le cas présentement.

Madame Bernier, que pensez-vous de cette recommandation? Est-il possible pour une cour de justice d'imposer à une institution gouvernementale, qui aurait violé les droits d'un citoyen et où celui-ci aurait encouru de possibles conséquences financières, de payer des dommages et intérêts?

Mme Chantal Bernier: C'est bel et bien possible.

Vous savez peut-être que le commissaire a en fait révisé cette recommandation dans une lettre subséquente au mois de septembre. Il a corrigé ou révisé sa recommandation quant à son rôle d'ombudsman. En révisant la recommandation n° 6, il a dit que la recommandation n° 5 à laquelle vous faites référence deviendrait caduque.

Cela étant dit, reprenons l'hypothèse de départ qui est la base de votre excellente question. Il y a des précédents à ce sujet. Par exemple, en Europe, les commissaires à la vie privée ont le pouvoir d'imposer des amendes. Il y a donc une valeur pécuniaire, et ce, même pour des institutions gouvernementales dans des cas de violation de la vie privée.

M. Pierre-Luc Dusseault: D'accord.

Monsieur Guénette et madame Juneau, ce matin, en lisant les politiques d'accès du programme Mon dossier sur Internet, j'ai remarqué qu'à l'article 9, il est écrit ce qui suit:

L'ARC a pris toutes les mesures raisonnables pour assurer la sécurité de ce site web. Nous avons utilisé une technologie de chiffrement de pointe et avons intégré d'autres procédures pour protéger vos renseignements d'entreprise en tout temps.

Cependant, une petite phrase m'a fait sursauter. En effet, on peut lire ce qui suit:

Toutefois, Internet est un réseau public, et il existe une faible possibilité d'atteinte à la sécurité des données. Dans une telle situation, nous ne sommes pas responsables des dommages qui pourraient en résulter.

Je comprends par cette phrase que vous ne serez peut-être pas d'accord avec le commissaire dont la recommandation vise à accorder des dommages et intérêts à des citoyens dont la vie privée a subi une atteinte si celle-ci survient à cause du programme Mon dossier de l'Agence du revenu du Canada.

Est-ce exact?

• (1140)

M. Maxime Guénette: Je n'irais peut-être pas jusqu'à dire que nous ne serions pas d'accord avec le commissaire. Je pense que le cadre législatif actuel ne prévoit pas ce genre de choses, comme le fait d'obliger un organisme gouvernemental à payer des dommages et intérêts. Évidemment, si le cadre législatif est appelé à changer, il est possible que ce genre de mentions sur le site Web soit appelé à être modifié pour refléter le nouveau cadre législatif.

Pour revenir au fait qu'il existe un risque, nous avons bien évidemment adopté des mesures de cryptage. Le risque existe là où il y a un transfert d'informations entre le contribuable et l'Agence. Bien qu'il y ait un cryptage, il y a quand même un risque, si minime soit-il. Nous essayons de le minimiser lors de la transmission des données. C'est donc à cela que nous faisons référence.

M. Pierre-Luc Dusseault: En somme, si les données de millions de contribuables utilisant ce service étaient entre les mains d'une personne non autorisée et malveillante à cause d'un manque de sécurité du programme Mon dossier, aucune mesure ne permettrait de dédommager les citoyens dont on aurait volé les données?

M. Maxime Guénette: C'est ce que je comprends.

Mme Marie-Claude Juneau (directrice, Accès à l'information et protection des renseignements personnels, Agence du revenu du Canada): En effet, il n'y a pas à l'heure actuelle de mesures comme celle-là. Il n'y a rien à cet égard dans la Loi sur la protection des renseignements personnels.

Si nous perdions de l'information ou si de l'information était compromise, nous agirions de façon conforme à la loi actuelle. Si les recommandations à cet égard sont différentes, il faudrait voir comment l'Agence réagirait à ce genre de situations.

M. Pierre-Luc Dusseault: Merci.

Je vais aborder un autre sujet.

Une autre recommandation du commissaire est d'élargir la portée de la Loi sur la protection des renseignements personnels à d'autres institutions fédérales, et ce, idéalement à toutes les institutions fédérales. On parle également d'inclure le cabinet du premier ministre et ceux des ministres en ce qui a trait à la portée de la Loi.

Lors de notre dernière réunion, nous avons entendu des représentants de la Colombie-Britannique, de la Nouvelle-Écosse et de Terre-Neuve-et-Labrador. À ma grande surprise, quand je leur ai demandé si les cabinets des ministres et du premier ministre étaient soumis à la Loi, les trois m'ont répondu de façon affirmative. Je me demande si ce serait idéal et si ce serait faisable. Mme Bernier pourra répondre à cette question.

En arrivant sur plusieurs sites gouvernementaux, et même sur le site du premier ministre, on demande aux citoyens leur adresse courriel afin de les informer au sujet des nouveautés gouvernementales. Ce n'est rien de partisan, mais c'est quand même de la cueillette de données. Serait-il pertinent que cela soit soumis à la Loi sur la protection des renseignements personnels?

Mme Chantal Bernier: Tout à fait, et ce, pour plusieurs raisons.

Premièrement, il y a en ce moment un vide juridique en ce qui concerne ce genre de renseignements personnels détenus par les cabinets politiques et par les partis politiques.

J'ai lu les travaux antérieurs du Comité. Vous avez discuté de la question quant à savoir si les partis politiques devraient être assujettis à la Loi sur la protection des renseignements personnels. Je ne parlerai pas de cela parce que ce n'est pas le but de votre question.

Pour répondre à votre question, je dirais qu'effectivement, on viendrait combler une lacune juridique si les bureaux des ministres étaient assujettis à la Loi. Lorsqu'un parti est au pouvoir, il devient le gestionnaire de l'État et il exerce les pouvoirs de l'État. Il doit donc rendre des comptes quant au respect des droits fondamentaux et à la constitutionnalité des gestes de l'État.

Si l'on étendait l'application de la Loi sur la protection des renseignements personnels aux cabinets des ministres et à celui du premier ministre, ce serait effectivement un développement positif.

Le vice-président (M. Joël Lightbound): Monsieur Dusseault, malheureusement, votre temps est écoulé, mais nous allons revenir à vous plus tard.

Je cède maintenant la parole à M. Saini.

• (1145)

[Traduction]

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

La question que j'ai est pour Mme McCulloch, et M. Guénette et Mme Juneau, car vous représentez deux institutions, et en raison de la quantité et du volume d'information que vous avez à nous présenter.

Madame McCulloch, vous avez mentionné que Services partagés dessert 43 ministères. Avez-vous une sorte d'entente écrite avec les ministères et les organismes gouvernementaux? Parce que maintenant que nous sommes passés du support papier aux dossiers numériques, nous avons parfois tendance à recueillir trop de données. Comment faites-vous pour éviter cela?

Mme Monique McCulloch: La Loi sur Services partagés Canada a été rédigée de manière très explicite lorsqu'elle est appliquée en lien avec la Loi sur l'accès à l'information et la Loi sur la protection des renseignements personnels. Services partagés Canada est responsable de la gestion de l'infrastructure de TI, donc de la gestion de la coquille, mais le contenu — toutes les données de nos centres de données, même le contenu des courriels au sein de nos réseaux — appartiennent aux organismes partenaires et sont toujours sous leurs contrôles. Services partagés Canada, aux fins de la Loi sur l'accès à l'information et de la Loi sur la protection des renseignements personnels, n'a aucun contrôle sur les données contenues dans l'infrastructure de TI.

Cependant, nous sommes entièrement responsables et imputables, et nous travaillons en étroite collaboration avec les organismes partenaires en veillant à ce que la protection des renseignements personnels nécessaire et les contrôles de sécurité soient en place dans la gestion de l'infrastructure de TI, et lorsqu'il faut gérer les violations en matière de protection des renseignements personnels. Bien que les données puissent être sous le contrôle d'organismes partenaires — en d'autres termes, ils répondraient aux demandes d'accès, parce qu'il s'agit de leurs données — s'il y a une violation causée par un malheureux incident venant de l'infrastructure de TI, Services partagés Canada travaillera côte à côte avec les organismes partenaires pour s'assurer que la violation n'a plus cours, qu'elle est gérée et que des mesures correctives ont été mises en place. C'est une responsabilité partagée.

M. Raj Saini: Vous avez dit qu'il y a 23 000 serveurs desservis par Services partagés Canada. Si une personne travaillait dans un ministère ou une agence, y aurait-elle accès? Aurait-elle un accès complet à ces renseignements, indépendamment du fait qu'ils soient pertinents à leur ministère ou à leur agence?

Mme Monique McCulloch: Non. Les organismes partenaires ont uniquement accès aux données qui font partie des activités de programme pour lesquelles ils ont été mandatés, qui sont les renseignements personnels, de même que tous les renseignements gouvernementaux qui sont spécifiques aux activités du programme de leur ministère.

L'Agence du revenu du Canada, par exemple, n'a pas accès aux données personnelles du Programme canadien de prêts aux étudiants, qui est géré par une autre institution fédérale. De ce point de vue, c'est un environnement cloisonné.

M. Raj Saini: D'accord.

M. Maxime Guénette: Monsieur le président, si vous me permettez d'ajouter, en réponse à la question qui s'adressait plus particulièrement pour l'Agence du revenu du Canada, les contrôles vont même plus loin que cela. Deux fois par an, nous avons un mécanisme nous permettant d'évaluer les accès de nos employés à des applications pertinentes et à des parties du service. Même pour les employés des Services partagés, ils sont visés par cette mesure, et ce, depuis la mise sur pied de SPC en 2011. Ils s'y sont conformés depuis.

Nous évaluons les fonctions deux fois par an afin de voir si les fonctions ont changé et si les accès à certains serveurs ou bases de données sont encore nécessaires pour certains employés. Cela est réglé en temps réel.

M. Raj Saini: Vous êtes un organisme très important ici au Canada et vous devez recevoir des demandes de renseignements de l'extérieur. Une fois que ces renseignements quittent le Canada, comment peut-on éviter la diffusion et la divulgation de ces renseignements dans un autre pays où nous n'avons pas nécessairement le contrôle? Est-ce que vous avez des accords de services partagés écrits avec d'autres pays, et dans quelle mesure sont-ils exécutoires ou pertinents?

M. Maxime Guénette: Cette question comporte deux volets. Nous avons environ 350 accords de partage de renseignements. Environ 160 d'entre eux ont été conclus avec 46 organismes fédéraux, et ce sont des accords de partage de renseignements entre les ministères, tandis que 186 d'entre eux ont été conclus avec des ministères provinciaux ou territoriaux. Quelques dispositions ont été clairement établies dans ces accords de partage de renseignements qui établissent les objectifs pour lesquels les renseignements sont partagés et les raisons justifiant leur utilisation.

Quant à la mesure dans laquelle ces accords sont juridiquement exécutoires, je crois comprendre qu'ils ont plutôt une portée similaire au protocole d'entente, si vous voulez. J'hésite à aller plus loin là-dessus, à moins que Mme Bernier ait des commentaires sur l'applicabilité de ces types d'accords de partage de renseignements.

• (1150)

Mme Chantal Bernier: Oui, je peux certainement conclure en disant qu'il existe des lois sur la façon de transmettre les renseignements d'un pays à l'autre. Les lois fiscales, comme vous le savez, sont pour l'essentiel internationales, car il existe des accords entre les pays pour assurer le recouvrement des impôts. Ces accords se reflètent habituellement dans la loi, la FATCA étant l'exemple le plus récent et le plus médiatisé.

C'est définitivement exécutoire. C'est certainement accompagné de restrictions, et ces restrictions découlent de la loi sur la protection des renseignements personnels. En d'autres termes, le gouvernement fédéral enverrait-il des renseignements fiscaux, par le biais d'une demande du gouvernement français, par exemple? Tout doit être conforme aux lois sur la protection des renseignements personnels d'ici et aux lois sur la protection des renseignements de la France.

Le vice-président (M. Joël Lightbound): D'accord.

M. Raj Saini: Je vais utiliser les 30 secondes. J'ai une question pour vous, madame Bernier.

En vertu de la LPRPDE, lorsque vous avez la différence entre le modèle privé et le modèle public, vous avez le consentement éclairé par lequel vous avez la possibilité d'accepter ou de refuser. Pensez-vous que c'est quelque chose sur lequel nous devrions enquêter du côté public, également? En 30 secondes ou moins...

Mme Chantal Bernier: Non, cela me ramène à la réponse que j'ai donnée à Mme Rempel. La notion essentielle de légitimité dans le secteur public est la nécessité. La notion essentielle de légitimité dans le secteur privé est le consentement.

[Français]

Le vice-président (M. Joël Lightbound): Merci beaucoup.

Nous passons maintenant à la deuxième ronde de questions. Cette fois, elle sera d'une durée maximale de cinq minutes.

Monsieur Kelly, vous avez la parole.

[Traduction]

M. Pat Kelly (Calgary Rocky Ridge, PCC): Je vous remercie, monsieur le président.

Avec Services partagés, j'ai été un peu surpris par le faible nombre de demandes que le ministère a reçues, soit 123 en vertu de la Loi sur la protection des renseignements personnels, dont 120 ont été traitées avant la fin de la période couverte par le rapport. Ce n'est pas clair pour moi exactement combien de temps cela représente, mais il semble que c'est au moins dans la période de temps dans laquelle vous êtes censés les traiter.

Au cours de notre étude sur l'accès aux renseignements, nous avons entendu à la fois votre ministère et d'autres ministères — nous n'avons peut-être pas entendu parler du vôtre — qui a reçu des demandes d'accès. Nous avons entendu dire à maintes reprises que la conformité posait problème, compte tenu des ressources offertes, et que les arriérés étaient liés à l'insuffisance des ressources et à d'autres problèmes du système auxquels nous avons essayé de résoudre en apportant des améliorations.

Pourquoi pensez-vous que vous avez si peu de demandes en vertu de la Loi sur la protection des renseignements personnels? La première chose la plus évidente qui m'est venue à l'esprit était de savoir si les gens connaissent et comprennent votre ministère et l'énorme volume de renseignements qui y sont traités. Je ne pense pas avoir déjà entendu parler de Services partagés jusqu'à ce que je devienne député? Y a-t-il des gens qui ne savent pas qu'ils devraient faire des demandes adressées à votre ministère?

Mme Monique McCulloch: Cela rejoint bien ma réponse à la question précédente.

Il a été clairement précisé dans la Loi sur les Services partagés Canada, qu'aux fins de l'exercice des droits d'accès en vertu de la Loi sur l'accès à l'information et de la Loi sur la protection des renseignements personnels, les données qui se trouvent dans l'infrastructure de la TI de SPC — que ce soit les centres de données, les solutions de messagerie, les réseaux — ne sont pas sous

le contrôle de Services partagés Canada, mais sous le contrôle d'organismes partenaires. Les demandes d'accès, en vertu des deux lois, doivent être déposées par l'organisme gouvernemental qui a le mandat de réaliser l'activité de programme et qui, par conséquent, assume l'entière responsabilité de gérer ces renseignements et de les rendre disponibles.

Services partagés Canada ne dispose pas d'un volume très élevé de demandes en vertu de la Loi sur la protection des renseignements personnels, contrairement, par exemple, à l'Agence du revenu du Canada, à Immigration Canada à Emploi et Développement social Canada (EDSC), ou à d'autres ministères. Leur travail quotidien consiste à traiter les renseignements personnels utilisés dans la prestation de programmes et de services, tels que l'administration fiscale et l'assurance-emploi, mais Services partagés Canada n'exécute pas les activités du programme de cette ampleur lorsque nous traitons les renseignements sur la personne.

Nous aurons quelques renseignements personnels sur l'authentification des courriels, les adresses IP, ce type d'administration, mais nous n'administrons pas les activités de programme qui détiennent...

• (1155)

M. Pat Kelly: Je comprends, mais vous êtes le canal par lequel 43 ministères, 50 réseaux, 485 centres de données, et 23 000 serveurs fonctionnent.

De nombreux Canadiens ont des préoccupations au sujet de la protection des renseignements personnels. Les Canadiens s'inquiètent au sujet de la protection de leurs renseignements personnels pour diverses raisons, allant d'une utilisation imprudente par un individu dans un ministère à des cyberattaques, des menaces, des erreurs, de la négligence ou pour toute autre chose qui pourrait se produire dans tous ces réseaux et ces serveurs.

Parmi les demandes qui vous ont été faites, y a-t-il des gens préoccupés par la perte non déclarée de données ou ce genre de chose?

Mme Monique McCulloch: La majorité des demandes en vertu de la Loi sur la protection des renseignements personnels que nous recevons portent sur des questions de ressources humaines. Il s'agit d'employés ou d'anciens employés de Services partagés Canada qui sont à la recherche de leurs renseignements.

Je pense que le gouvernement, grâce à divers moyens, a fait savoir que Services partagés Canada gère l'infrastructure de la TI, mais que le contrôle des données aux fins de l'exercice des droits d'accès des individus... L'outil en ligne, par exemple, stipule très clairement que les individus doivent adresser leurs demandes en vertu de la Loi sur l'accès à l'information et de la Loi sur la protection des renseignements personnels à l'organisme gouvernemental responsable de l'administration de ce programme.

Nous recevons un certain nombre de ce que nous appelons des demandes mal dirigées, mais nos chiffres ne sont pas très élevés du côté de la Loi sur la protection des renseignements personnels. Vous avez tout à fait raison.

[Français]

Le vice-président (M. Joël Lightbound): Merci beaucoup.

[Traduction]

M. Pat Kelly: C'est ça? D'accord.

[Français]

Le vice-président (M. Joël Lightbound): Nous passons maintenant à M. Bratina.

[Traduction]

M. Bob Bratina (Hamilton-Est—Stoney Creek, Lib.): Je vous remercie.

J'ai été distrait tout à l'heure de certains des témoignages, parce qu'une vieille connaissance, un architecte qui travaille sur des projets à travers le monde, a répondu à ma demande à son courriel, « C'est de l'hameçonnage. Tu dois t'en débarrasser. » J'ai dû changer mon mot de passe.

À la lumière de cela, madame Bernier, la technologie est en constante évolution. Vous faites partie d'un organisme vraiment énorme. Il s'agit d'organisme de taille gouvernementale, je dirais.

Mme Chantal Bernier: C'est le plus grand cabinet d'avocats au monde.

M. Bob Bratina: Êtes-vous en mesure de comparer le genre de sécurité que votre entreprise doit offrir avec ce que vous savez du gouvernement canadien?

Mme Chantal Bernier: Je dirais que nous devons être encore plus prudents, et nous sommes encore plus prudents, d'abord parce que nos renseignements sont protégés par le secret professionnel. Ils sont donc non seulement protégés comme des renseignements personnels, mais aussi par l'obligation de confidentialité envers nos clients.

Deuxièmement, parce que nous avons une présence mondiale, nous devons nous assurer que nous avons une protection mondiale. En même temps, l'avantage d'être présent dans le monde est que nous avons la même empreinte que nos clients. Nos clients apprécient le fait qu'ils n'ont qu'à venir me voir, pourtant je peux me connecter au monde entier pour répondre à leurs questions à mesure qu'elles se produisent dans le monde entier. Nous avons donc besoin de l'interopérabilité et cette interopérabilité doit être sécurisée.

Il est évident que nous sommes fiers d'avoir cet environnement extrêmement sécurisé qui est régi par une architecture de gouvernance très complexe, comme vous l'imaginerez, qui nous permet d'être vraiment bien coordonnés tout en étant complètement sécurisés.

• (1200)

M. Bob Bratina: Pourquoi ne serions-nous pas en mesure de fournir le même niveau de confiance aux gens qui font affaire avec le gouvernement?

Mme Chantal Bernier: Après avoir examiné les organismes gouvernementaux pendant six ans, j'avoue avoir beaucoup de sympathie. En fait, c'est intéressant, parce que la vérification à laquelle M. Guénette faisait référence est une vérification que j'ai supervisée. Nous avons fait des recommandations pour des améliorations, mais nous étions très conscients de leurs défis.

Il y a 400 000 employés, ai-je raison?

M. Maxime Guénette: Non, c'est 40 000.

Mme Chantal Bernier: Vous voyez? Dans mon empathie, j'ai rendu le nombre plus grand.

Voix: Oh, oh!

Mme Chantal Bernier: Il y a 40 000 employés de différents niveaux qui ont besoin de répondre à des gens qui appellent de partout, comme M. Dusseault a dit. Ils ont besoin de répondre, donc ils ont besoin d'avoir accès aux fichiers, mais cet accès doit être contrôlé. Ça ne peut pas sortir. Il s'agit de renseignements sensibles. C'est la première difficulté, le fait que ce soit opérationnel avec tant de gens et à tant de niveaux.

La deuxième difficulté réside dans le fait que le gouvernement veut avoir accès à une partie des renseignements. Par exemple, nous savons que « suivre la trace de l'argent » est la clé de la découverte des activités illégales. Cela signifie qu'il doit y avoir certains accès autorisés en dépit de toutes les protections. C'est là une autre difficulté.

Puis, avec 400 000 personnes dans la fonction publique — ce nombre est exact — cela fait beaucoup de personnes à surveiller. C'est beaucoup de personnes qui pourraient avoir de la rancune ou des intentions malveillantes. J'en ai vu beaucoup. Je ne les ai pas vues seulement au gouvernement. Je les ai vues dans le secteur privé. Si vous regardez les menaces internes à la sécurité des données et les menaces extérieures à la sécurité des données, vous vous rendez compte que le risque est très élevé.

L'un des avantages que nous avons dans notre cabinet, puisque vous avez fait la comparaison, c'est que nous sommes tous des avocats. Nous sommes tous des avocats ayant un intérêt direct dans ce domaine florissant, et donc nous avons une culture qui favorise, qui aide, la sécurité des données. Dans le gouvernement, toutefois, vous pouvez avoir un employé mécontent. Vous n'avez pas un employé qui a en même temps investi personnellement dans l'entreprise. Vous avez différentes contingences avec lesquelles composer.

Je peux vous parler d'un organisme pour lequel j'ai beaucoup de sympathie. Cet organisme fonctionnait bien. Leur principale difficulté concernait le désengagement du personnel. Parce que le personnel était désengagé, le personnel n'a pas exercé la discipline appropriée qu'ils auraient dû exercer.

M. Bob Bratina: Est-ce qu'il y a plus de temps?

Le vice-président (M. Joël Lightbound): Non. Nous aurons probablement plus de temps à la fin.

Nous retournons maintenant à M. Kelly.

M. Pat Kelly: Merci, monsieur le président.

Nous avons eu toute une discussion lors de notre réunion précédente au sujet de la déclaration obligatoire des atteintes à la vie privée. Je donnerai à chacun de vous une minute pour commenter sur ce que vous croyez être des seuils, sur ce qui constitue le type de violation substantielle qui exigerait une déclaration obligatoire au commissaire et sur la façon d'atténuer les dommages supplémentaires chez un individu victime d'un reportage.

Mme Chantal Bernier: Cela est un cas où la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) est un bon modèle à suivre. Je crois que le gouvernement a eu raison avec cette loi sur la déclaration obligatoire des atteintes à la vie privée. Cela signifie d'abord qu'il y a une déclaration seulement s'il y a un risque réel de dommage significatif. Vous ne voulez pas alarmer les gens pour rien.

M. Pat Kelly: En effet.

Mme Chantal Bernier: Le dommage peut être moral ou financier. Ce pourrait être un dommage à la réputation ou à des relations, mais vous devez tenir compte de dommages significatifs.

L'obligation de déclaration ne prévoit pas d'échéancier précis. Cela doit être fait le plus vite possible, ce qui, à mon avis, relève de diligence, mais cette obligation ne contraint pas une organisation à respecter des délais prévus par la technologie qui pourraient être distincts de ce que prescrit la loi. En outre, les personnes concernées et le Commissariat à la protection de la vie privée doivent tous être informés de la déclaration.

Pour revenir sur votre dernier point, je soulignerais que c'est lorsque vous avisez les individus que vous leur donnez les moyens de prendre des mesures pour protéger leur information personnelle.

• (1205)

M. Pat Kelly: Madame McCulloch.

Mme Monique McCulloch: Définir ce qu'est une violation substantielle de la vie privée peut parfois constituer un défi pour les institutions. Une institution considérera qu'il y a violation substantielle lorsqu'une autre institution en juge autrement. Je sais que partout au gouvernement des efforts continus sont déployés pour assurer une normalisation additionnelle.

Le degré de sensibilité étant discrétionnaire, vous pourriez avoir un cas de nature extrêmement délicate, mais qui n'implique qu'une seule personne ou un cas de nature peu délicate impliquant des centaines, voire des milliers de personnes. Il incombe à chaque institution de déterminer s'il y a bel et bien atteinte à la vie privée et, le cas échéant, elle doit en aviser le Commissariat à la protection de la vie privée et le Secrétariat du Conseil du Trésor.

M. Pat Kelly: Avez-vous besoin de plus d'éclaircissements?

Mme Monique McCulloch: Parfois, pour la normalisation au sein du gouvernement, à mon avis, oui. Il pourrait y avoir une certaine valeur ajoutée, plus d'évaluations comparatives et plus de critères.

M. Pat Kelly: Merci.

M. Maxime Guénette: De toute évidence, l'Agence du revenu du Canada tient compte de la nature délicate de l'information divulguée lors de l'évaluation de la gravité d'une violation. Nous avons des renseignements médicaux et financiers et des identificateurs personnels comme les numéros d'assurance sociale. Ce genre de choses ou tout autre élément pouvant mener au vol d'identité ou à la fraude déclencherait évidemment la déclaration d'une violation.

Cependant, pour donner suite au point que vous avez soulevé et à ce à quoi faisait allusion Mme McCulloch, il y a plusieurs types d'atteintes à la vie privée. L'une d'entre elle que nous observons souvent à l'ARC concerne le courrier mal acheminé. Le volume peut paraître élevé en nombre absolu, mais j'aimerais souligner qu'en terme de pourcentage, si l'on tient compte des 110 millions d'envois postaux que nous transmettons chaque année, cela fait moins de 0,001 %. Par contre, un envoi postal acheminé à la mauvaise adresse, qui n'a pas été ouvert et qui nous a été renvoyé est consigné à l'interne comme une atteinte à la sécurité. Cela n'est pas quelque chose qui vaudrait la peine d'être signalé au Commissariat à la protection de la vie privée.

Une violation de la sécurité ayant trait à un employé qui accède volontairement à des renseignements sur les contribuables en dehors de ses fonctions normales sera traitée très différemment. Si je ne me trompe pas, les 20 ou les 21 cas qui ont été signalés au Commissariat à la protection de la vie privée concernaient l'accès illicite d'un employé à des renseignements sur les contribuables. Il y en a toute une gamme, et les activités des différents ministères seraient bien évidemment tout à fait différentes. Il y a un certain degré de flexibilité qui se révèle utile dans le cadre actuel.

[Français]

Le vice-président (M. Joël Lightbound): Merci

Madame Dzerowicz, vous avez la parole pour une période de cinq minutes.

Mme Julie Dzerowicz (Davenport, Lib.): Je vous remercie, monsieur le président.

[Traduction]

Je vous suis grandement reconnaissant pour ces présentations informatives.

Je n'avais pas l'intention de vous poser cette question, mais M. Long a soulevé d'excellents points qui m'incitent à vous la poser. Dans ma circonscription, lorsque je fais du porte-à-porte et que je parle aux gens, je remarque qu'ils croient que le gouvernement recueille des données sur les activités sur le Web et les cellulaires. Au début, je croyais qu'ils étaient simplement inquiets au sujet du projet de loi C-51, du type d'information qui était recueillie et du fait que celle-ci était échangée entre la GRC et la sécurité, mais je crois qu'il y a une croyance populaire. Je ne peux vous dire que des centaines de personnes m'en ont parlé, mais cette croyance existe.

Je sais que vous avez mentionné que le gouvernement ne peut pas utiliser les renseignements personnels recueillis, sauf s'ils répondent au critère de la nécessité. Mais recueille-t-il vraiment ces renseignements? Je veux simplement me faire une idée de ce que je dois répondre aux gens, tel que: « Non, vous lisez trop de trucs sur la théorie de conspiration. » Quelqu'un peut-il me répondre à ce sujet? J'aimerais pouvoir fournir une réponse honnête aux personnes.

• (1210)

Mme Chantal Bernier: Je peux certainement essayer de vous répondre.

Je crois qu'il y a beaucoup de désinformation. C'est la raison pour laquelle je souhaite revenir sur le rapport du 28 janvier 2014, parce que nous nous sommes tellement concentrés là-dessus. Nous avons fait 10 recommandations qui, je l'espère vraiment, ne seront pas oubliées, parce qu'elles abordent des questions très pratiques. L'une d'entre elles porte sur la transparence. Le gouvernement peut-il nous dire plus précisément ce qu'il fait?

Comme j'ai travaillé à Sécurité publique Canada où j'ai été sous-ministre adjointe, et au Commissariat à la protection de la vie privée, je peux vous assurer que ce n'est vraiment pas si mal. Il n'y a pas de Big Brother. Le gouvernement n'a pas les moyens, il n'a pas l'intérêt, et franchement, il est beaucoup plus stratégique et éthique que la croyance populaire le suggère.

Cependant, les commentaires que vous entendez — et je sais que vous les entendez, car je les entends — soulignent vraiment le besoin d'une plus grande transparence. On souligne en particulier le besoin de rapports annuels pour toutes les agences qui recueillent de l'information sur la sécurité publique ou qui reçoivent un signal d'information. Il faudrait que les dirigeants de ces organismes soient régulièrement présents aux comités de la Chambre des communes, comme celui-ci ou celui de la sécurité publique, etc. Tenez compte d'eux et demandez-leur ceci: « Une fois par an, nous voulons un rapport de votre part dans lequel vous précisez ce qui selon vous constitue une menace, quelles sont les activités relatives à cette menace et la façon dont ils respectent les droits fondamentaux. »

Mme Julie Dzerowicz: Vous avez commencé votre présentation en parlant d'entente sur l'échange de renseignements entre les États et les organismes. Qui le fait bien? Quel pays le fait bien? Est-ce que les ententes finissent par être créées pour déterminer la durée de conservation des données? S'il y a des données erronées qui sont envoyées, s'il y a une certaine désinformation qui va du Canada en Autriche et que nous la corrigeons soudainement, y a-t-il une sorte de mécanisme pour effectuer la correction en Autriche également? Jusqu'à quel point pouvons-nous réellement informer? Si les données d'une personne sont transportées, jusqu'à quel point pouvons-nous informer la personne que son information a été partagée avec d'autres États et organismes?

Mme Chantal Bernier: Personne ne le fait, idéalement. Les recours que vous proposez sont très fragmentés. Par exemple, le programme de protection des passagers a des recours si vous êtes arrêté parce que votre nom figure sur la liste de non-embarquement. Nous avons tous entendu parler du garçon de sept ans qui s'est fait refuser son embarquement parce que son nom correspondait au nom d'une personne qui était sur la liste. Il y a un recours possible. Cela prend beaucoup de temps, mais le ministre Goodale a déjà annoncé que des efforts sont déployés pour résoudre ce problème. En fait, cela fait partie du livre vert « Notre sécurité, nos droits », lequel fait actuellement l'objet d'une consultation.

Malheureusement, je dois vous dire que je ne peux vous répondre, puisque le niveau de transparence requis pour connaître la réponse à votre question n'existe pas. Chaque pays doit faire sa part.

Mme Julie Dzerowicz: Combien de temps me reste-t-il?

Le vice-président (M. Joël Lightbound): Aucun...

[Français]

Mme Julie Dzerowicz: D'accord.

Merci.

[Traduction]

Le vice-président (M. Joël Lightbound): ... mais nous aurons plus de temps à la fin.

[Français]

Monsieur Dusseault, vous avez la parole et vous disposez de trois minutes.

M. Pierre-Luc Dusseault: Merci, monsieur le président.

Ma question s'adresse aux représentants de l'Agence du revenu du Canada et concerne les mesures prises dans les cas d'atteinte à la vie privée.

Récemment, une clé USB ou un ordinateur portable — je ne me rappelle plus lequel entre les deux — a été laissé dans un autobus. Des gens malveillants ont eu accès à des données de l'Agence du revenu du Canada. La faille qui leur a permis de le faire est surnommée *Heartbleed*.

Dans un autre cas, Radio-Canada a obtenu, en réponse à une demande d'accès à l'information, un fichier qui était là par erreur. Radio-Canada s'est donc retrouvé avec des informations très sensibles entre ses mains et a évidemment rapporté le tout dans un reportage.

J'aimerais savoir quelles mesures sont prises exactement à ce sujet. Plus tôt, on a parlé des dommages et intérêts possibles, mais vous ne semblez pas les envisager pour l'instant, étant donné que ce n'est pas obligatoire. Que faites-vous pour informer et rassurer les contribuables dans de tels cas? Prenez-vous des mesures pour atténuer les impacts subis par les personnes victimes d'une atteinte à leur vie privée, par exemple en vous assurant que leur cote de crédit est encore bonne? Lorsque des données se retrouvent entre de mauvaises mains, que faites-vous? Comment réagissez-vous?

• (1215)

M. Maxime Guénette: Comme il s'agit de quelque chose qui s'est produit à un très haut niveau, je vais demander à Mme Juneau de vous expliquer les détails de la procédure à ce sujet.

Il y a en effet une procédure qui existe au sein de l'Agence. Nous travaillons avec l'agent de sécurité de l'Agence, qui est notre premier point de contact. Les incidents doivent être rapportés à cette personne, qui doit pour sa part remplir un rapport.

Nous avons parlé un peu plus tôt des critères que nous utilisons pour évaluer à quel point le manquement est grave. Une consultation a lieu avec Mme Juneau pour déterminer s'il y a atteinte à la vie privée et, le cas échéant, quelles mesures doivent être prises. Si c'est désigné selon la matrice d'évaluation du risque, nous communiquons avec le contribuable. Cela fait partie des étapes à suivre.

Madame Juneau, voudriez-vous ajouter quelque chose à ce sujet?

Mme Marie-Claude Juneau: Oui, tout à fait.

Comme M. Guénette vient de le mentionner, l'Agence suit un processus bien établi pour rapporter un incident, quel qu'il soit. À la suite d'un incident, la Direction de la sécurité et des affaires internes fait une enquête et nous fait parvenir sa conclusion. Il s'agit de déterminer si, oui ou non, il y a eu un bris de sécurité. Si c'est le cas, nous rapportons ce bris au Commissariat à la protection de la vie privée. Nous avons aussi un cadre de discipline à l'Agence. Selon ce dernier, on vérifie la façon dont le bris a été rapporté et si une mesure disciplinaire s'applique dans un tel cas.

Quant à ce que nous faisons pour atténuer l'impact des bris de sécurité, je vais revenir à l'exemple que vous avez donné concernant la CBC. Lorsque cet incident s'est produit, les mesures que nous avons prises en matière d'accès à l'information et à la protection des renseignements personnels consistaient à vérifier les processus mis en oeuvre à l'Agence et à déterminer à quel endroit la surveillance ou la révision pouvait être accrue pour éviter que ce genre de situations ne se reproduise.

En outre, un autre processus a été élaboré. Une firme privée a vérifié si nos processus étaient bel et bien adéquats et s'il y avait encore des lacunes. En fin de compte, cette firme nous a fait quelques recommandations. Les mesures qu'elle nous a recommandées concernaient davantage l'accès aux systèmes, la vérification de ceux-ci et l'assurance de la qualité. Nous avons mis en oeuvre ces procédures pour éviter que ce genre de situations ne se reproduise.

M. Pierre-Luc Dusseault: Je vous remercie.

En fait, vous avez déjà répondu à ma deuxième question, qui portait sur les procédures mises en place pour faire en sorte que ce genre d'incidents ne se reproduise pas.

De toute façon, je pense que le temps dont je disposais est écoulé.

Le vice-président (M. Joël Lightbound): En effet, votre temps est écoulé.

Toutefois, nous avons terminé les séries de questions officielles et nous sommes en avance sur notre horaire. J'invite donc ceux qui ont des questions et qui ne sont pas encore intervenus à le faire. Il y a déjà M. Massé qui veut intervenir et, si vous avez d'autres questions, Monsieur Dusseault, vous pourrez les poser un peu plus tard. La même suggestion s'applique à Mme Rempel et à M. Kelly. Vous avez simplement à nous faire signe si vous avez d'autres questions à poser.

Monsieur Massé, vous avez la parole.

M. Rémi Massé (Avignon—La Mitis—Matane—Matapédia, Lib.): Merci, monsieur le président.

Je remercie les témoins de participer à cette rencontre du Comité. C'est fort apprécié.

Ma question s'adresse à M. Guénette.

En 2013, le Commissariat à la protection de la vie privée avait fait une vérification et avait souligné les piètres pratiques de l'Agence en matière de sécurité. Il disait également que l'ARC, à cause de ses pratiques moins qu'excellentes, avait contribué à l'accès inapproprié, de la part d'employés, à des milliers de documents durant plusieurs années.

Vous avez fait référence à ces recommandations formulées en 2013. Parlez-nous des mesures que vous avez mises en place pour vous assurer que ce type de situations ne se produise plus.

• (1220)

M. Maxime Guénette: Merci beaucoup de la question.

Monsieur le président, je mentionnerais deux types de gestes qui ont été posés à ce sujet. L'un est d'aspect plus technique et l'autre touche l'éducation auprès des employés.

Du point de vue technique, il y a des mesures que nous sommes toujours en train de mettre en oeuvre. J'y ai d'ailleurs fait allusion dans mes remarques préliminaires. Elles ont été mises en place et continuent de l'être afin de mieux documenter et de contrôler l'accès des employés aux bases de données et aux applications que nous avons au sein de l'Agence. Comme je le mentionnais, des révisions sont faites deux fois par année pour s'assurer que, s'il y a des changements dans les fonctions de certains employés et qu'il y a des accès qui doivent être revus, cela soit fait.

Des améliorations ont également été apportées pour permettre de créer, dans le cadre du Système national de piste de vérification, ce que nous appelons une « piste de vérification » pour être en mesure de détecter les accès qui ne sont pas liés à certaines fonctions et d'en aviser les gestionnaires. Des mesures ont donc été mises en place pour permettre aux gestionnaires de recevoir de façon automatique une indication en ce sens. Par exemple, je pourrais devoir aller parler à Mme Juneau parce que j'ai reçu une indication comme quoi elle est allée chercher de l'information qui ne semble pas cadrer avec l'ensemble de ses fonctions. Plusieurs applications sont soumises à cette vérification.

M. Rémi Massé: Est-ce qu'elles fonctionnent présentement?

M. Maxime Guénette: Oui, elles fonctionnent, mais elles continuent d'être bonifiées. Nous prévoyons que le travail sera terminé en 2017, donc d'ici la fin de l'année prochaine. Ce sont les éléments qui sont plus techniques.

Cependant, depuis cette vérification en 2009, beaucoup d'accent a été mis sur la sensibilisation auprès des employés. Nous possédons certaines données qui nous permettent de constater les cas où le plus d'atteintes à la vie privée ont été rapportées. Cela vient du fait que ce qui doit être rapporté est maintenant clair pour les employés, comparativement à la situation d'il y a cinq ans, comme vous l'avez mentionné. Il y a le Code d'intégrité auquel j'ai fait référence. Il y a aussi le Cadre d'intégrité. Il y a de plus des initiatives de communication qui ont été mises de l'avant et de la formation obligatoire. Dans notre sorte de tableau de bord de gestion de la performance, il y a plusieurs indicateurs. En tant que chef de la protection des renseignements personnels, je dois vérifier à quel point les employés suivent la formation et à quel point ils consultent les renseignements disponibles. Par exemple, nous avons une vidéo qui a été rendue disponible récemment. Selon les dernières données disponibles, elle a été visionnée au-delà de 12 000 fois par les employés. Il s'agit d'une vidéo qui explique le genre d'atteintes à la vie privée qui peut se produire par inadvertance.

Il y a donc un gros effort de communication qui a été fait à cet égard et qui doit absolument continuer. Nous constatons — et je

crois que nous avons des données qui le démontrent — qu'il y a présentement une meilleure compréhension de l'importance de la protection des renseignements personnels, de ce qui peut constituer une atteinte aux renseignements personnels et de la procédure à suivre en vue d'identifier ces manquements lorsqu'ils surviennent.

M. Rémi Massé: Est-ce qu'il me reste 30 secondes?

Le vice-président (M. Joël Lightbound): Oui. Vous avez 30 secondes.

M. Rémi Massé: Madame Bernier, j'ai cru comprendre que vous aviez contribué à l'établissement de ce processus de vérification. Avez-vous eu la chance de vérifier par la suite les mesures qui avaient été mises en place par l'Agence du revenu du Canada? M. Guénette a donné des explications sur ces mesures. Avec ce que vous avez constaté, avez-vous l'impression que les mesures mises en place sont suffisantes? Doit-on plutôt aller encore plus loin dans cette démarche par rapport à l'Agence?

Mme Chantal Bernier: Évidemment, c'est mon successeur qui fait maintenant le suivi à ce sujet et c'est lui qui pourrait répondre à cette question. Je ne peux parler que de la situation jusqu'à juin 2014. À ce moment-là, j'étais très convaincue que l'Agence prenait très au sérieux les recommandations que nous avons faites. Ces recommandations avaient révélé des lacunes, mais elles ont été prises au sérieux. Je ne peux pas parler de la situation actuelle, mais lorsque j'étais en fonction, je voyais un réel effort de la part de l'Agence.

• (1225)

Le vice-président (M. Joël Lightbound): Merci.

Je vous remercie, monsieur Massé.

Je cède maintenant la parole à M. Dusseault.

M. Pierre-Luc Dusseault: Merci, monsieur le président.

J'ai quelques brèves questions à poser.

Madame Bernier, je veux revenir sur ce que vous avez dit au sujet des partis politiques et que vous n'avez pas eu le temps de développer davantage.

J'ai aussi posé cette question cette semaine au représentant de la Colombie-Britannique. Il m'a dit que les partis politiques de cette province, incluant ceux des paliers provincial et municipal, étaient couverts par la loi, mais je voudrais aborder celle qui s'applique au secteur privé.

Selon vous, quelle serait la meilleure solution à envisager? Est-ce que la loi qui vise le secteur privé pourrait techniquement s'appliquer aux partis politiques? Est-ce que ce serait envisageable de faire en sorte que ce soit le cas?

Mme Chantal Bernier: Il faudrait que la Loi sur la protection des renseignements personnels et les documents électroniques soit amendée pour créer une section particulière étant donné que cette loi s'applique au secteur privé et est fondée sur le paradigme du consentement, c'est-à-dire dans le cadre d'une activité commerciale. Autrement dit, je donne mes renseignements personnels en retour d'un bien ou d'un service. Cependant, ce n'est pas du tout le cas quand on donne des renseignements à un parti politique.

La Loi sur la protection des renseignements personnels et les documents électroniques devrait être élargie pour viser toutes les relations non gouvernementales. Elle devrait comporter une section sur les activités commerciales, comme c'est le cas présentement, où les renseignements personnels sont livrés dans un contexte transactionnel. Il faudrait une section qui s'appliquerait spécifiquement aux partis politiques.

M. Pierre-Luc Dusseault: Nous allons certainement prendre cela en considération pour la suite des choses.

Dans le rapport remis au Parlement par l'Agence du revenu du Canada sur l'application de la Loi sur la protection des renseignements personnels, il est question d'un cas où une information avait été demandée, mais où on avait refusé de la traduire de l'anglais vers le français. On ne donne pas beaucoup d'explications; ce n'est qu'un petit paragraphe du rapport qui parle de cette question. De plus, dans les tableaux en annexe, on voit qu'il y a un cas de refus.

Si vous avez l'information à cet égard, pouvez-vous me fournir plus de détails? Pourquoi une telle information n'a-t-elle pas été traduite afin que la personne concernée puisse l'avoir dans la langue de son choix?

Mme Marie-Claude Juneau: Je vous remercie de cette très bonne question, mais malheureusement, je n'ai pas la réponse à ce sujet. Je vais faire une recherche et m'assurer que la réponse sera transmise au Comité dans les jours à venir. Je suis désolée.

M. Pierre-Luc Dusseault: Il n'y a pas de problème. On ne peut pas connaître tous les détails de chacune des 3 000 demandes qui ont été faites.

Mme Marie-Claude Juneau: Effectivement.

M. Pierre-Luc Dusseault: Il serait toutefois utile que le Comité obtienne cette information.

Mme Marie-Claude Juneau: Tout à fait.

M. Pierre-Luc Dusseault: J'ai une dernière question à poser, monsieur le président.

Au sujet de la sous-traitance de la gestion des données, il y a un cas qui a été relevé. Il y a eu une enquête du commissaire à la protection de la vie privée mettant en cause Shred-it, une compagnie qui fait de l'entreposage de données, particulièrement sur papier, je suppose. Il y a un volume important de documents en format papier à l'Agence du revenu du Canada étant donné qu'elle conserve des données pendant des dizaines d'années.

Prenez-vous des mesures supplémentaires dans le cas d'un sous-traitant ou d'une compagnie privée qui gère les données des contribuables canadiens? Pourquoi ne faites-vous pas cela à l'interne? Pourquoi n'est-ce pas géré par votre ministère? Pourquoi utiliser la sous-traitance alors que cela pourrait être fait directement par le ministère?

Mme Marie-Claude Juneau: Je ne pourrai pas dire pourquoi on a recours à la sous-traitance plutôt que de le faire à l'interne. Je peux toutefois dire qu'un processus a été établi pour que les firmes — j'ai oublié le terme exact en ce qui concerne les contrats — répondent à nos exigences et à tout ce que nous voulions en matière de protection des renseignements personnels.

Vous avez fait référence au rapport du commissaire à la protection de la vie privée. Nous avons communiqué avec le commissaire et nous l'avons rencontré à quelques reprises lors de ce processus, afin de lui expliquer ce à quoi nous nous attendions de la compagnie à ce moment-là. La plainte qui a été déposée au Commissariat à la protection de la vie privée était en lien avec le fait que l'information était gérée par une compagnie qui était aux États-Unis. Finalement, le commissaire a fait enquête et a vérifié certaines choses. Il en est venu à la conclusion que la plainte n'était pas fondée.

• (1230)

M. Pierre-Luc Dusseault: C'était la conclusion du commissaire.

Qui pourrait répondre à la question par rapport à la politique prévoyant d'utiliser la sous-traitance pour l'entreposage des données? Cela relève-t-il davantage d'une décision politique?

M. Maxime Guénette: Non, je ne le crois pas. Si je comprends bien, c'est purement pour des raisons opérationnelles.

J'aimerais clarifier que ce sont strictement des documents en format papier qui sont traités par la compagnie Recall. Je pourrais faire des vérifications et vous revenir avec une réponse plus détaillée à cet égard.

D'après ce que je comprends, l'Agence a recours à la sous-traitance pour réaliser des économies d'échelle. L'Agence a plus d'une centaine de lieux au Canada où des documents peuvent être conservés. La conservation de tous ces documents au sein d'une seule organisation nécessite des méthodes technologiques assez impressionnantes pour la gestion des dossiers et le repérage des documents dans des boîtes au moyen de codes-barres. Plutôt que d'investir dans ce genre de technologies dans ses multiples centres, je soupçonne que l'Agence a recours à la sous-traitance surtout pour des raisons d'efficacité et d'économies d'échelle.

Mme Marie-Claude Juneau: Monsieur le président, puis-je ajouter quelque chose à ce sujet?

Le vice-président (M. Joël Lightbound): Allez-y, madame Juneau.

Mme Marie-Claude Juneau: J'aimerais ajouter ce qui suit par rapport à ce que M. Guénette vient de dire.

Avant qu'on opte pour utiliser les services de cette compagnie, la gestion des documents se faisait par Bibliothèque et Archives Canada. Elle ne s'est pas vraiment désistée de cette fonction. C'est plutôt que cela ne fait plus nécessairement partie de son nouveau mandat. On a donc dû trouver une solution pour s'assurer de conserver la gestion de ces documents. Auparavant, cela se faisait à l'interne par le gouvernement.

M. Pierre-Luc Dusseault: Je vous remercie de votre réponse.

Le vice-président (M. Joël Lightbound): Merci beaucoup.

M. Kelly a maintenant quelques questions à poser.

[Traduction]

M. Pat Kelly: Merci, monsieur le président.

Le commissaire Therrien avait recommandé quelque chose au départ, puisqu'il n'avait pas le pouvoir pour prendre des décisions, mais il a récemment changé sa recommandation pour que son bureau puisse exercer ce pouvoir, qu'il puisse avoir le pouvoir de prendre des décisions, qu'il puisse fonctionner selon ce modèle.

J'aimerais que Mme McCulloch et M. Guénette fassent part de ce qu'ils pensent des conséquences possibles sur leur organisation.

Mme Monique McCulloch: Comme j'ai travaillé au bureau du commissaire pendant plusieurs années, je m'attends à ce que le commissaire continue d'agir en tant qu'ombudsman, puisque le but ultime du bureau du commissaire et de l'institution est de résoudre des problèmes le plus rapidement possible, et ce, à la satisfaction du plaignant. Je pense que les cas où les commandes doivent être émises seront rares, et je ne pense pas que cela aura une incidence énorme.

Les cas seront traités de façon très similaire à ceux des situations actuelles. Si les commissaires ont déjà recommandé de prendre une résolution particulière pour une plainte, la question sera traitée à un niveau très élevé de l'organisation. Mais ces cas ne se produisent pas souvent; la majorité des questions sont normalement résolues à un niveau opérationnel. Donc, je ne m'attends pas à une énorme incidence à cet égard.

Le gouvernement aura toujours la possibilité d'aller devant le tribunal s'il y a une réelle divergence d'opinions en ce qui a trait aux risques. Si nous recevons l'ordre de publier des documents, mais que nous avons des raisons de croire qu'il pourrait y avoir une grave atteinte à la vie privée, la question pourrait être traitée à la prochaine étape. Mais ces cas devraient être très limités.

• (1235)

M. Maxime Guénette: Je vous remercie de votre question.

Tout comme Mme McCulloch, je crois que nous devons traiter nos relations avec le Commissariat à la protection de la vie privée avec l'intention de trouver un terrain d'entente, et si nous entrons dans un cadre législatif différent où il y a un ordre, nous tenterons de résoudre la situation avant que ça n'arrive à cela.

En ce qui concerne ce que pourrait impliquer ce changement particulier pour notre travail, il est difficile de spéculer sur ce à quoi ça pourrait ressembler, sans avoir plus de détails sur le fonctionnement. Dans un endroit comme l'ARC, avec le volume de travail que nous avons, et dépendamment du déroulement, il pourrait y avoir des conséquences sur les processus et les ressources. Il nous faudrait y faire face, mais nous serions en conformité avec le cadre de travail mis en place par le gouvernement.

Oui, je crois que je suis d'accord avec Mme McCulloch que nous tentons d'arriver à un terrain d'entente. Et puis, dans la plupart des cas, nous avons du succès dans ce domaine.

M. Pat Kelly: Êtes-vous d'accord avec la recommandation d'aller de l'avant avec un modèle exécutoire?

Certaines critiques de notre étude sur l'accès à l'information ont fait valoir que lorsqu'il y a un pouvoir de rendre des décisions, l'ombudsman cesse de jouer son rôle et il devient arbitre. Au lieu d'être un défenseur de la vie privée, vous devenez une personne qui fait un jugement sur un cas particulier, plutôt que de défendre simplement la vie privée.

Partagez-vous ces préoccupations ou pensez-vous que le modèle exécutoire est la voie à suivre en ce qui a trait à la vie privée?

M. Maxime Guénette: J'hésite à exprimer une opinion pour dire si c'est la voie à suivre. Je crois que mon rôle au sein de l'agence serait de mettre en oeuvre toute décision rendue en matière de législation. Certes, comme je l'ai dit, avec ou sans pouvoir de rendre des décisions, nous devons essayer de nous conformer à la lettre et à l'esprit de la Loi, dans la mesure du possible, quel que soit le cadre de travail.

[Français]

Le vice-président (M. Joël Lightbound): Merci beaucoup, monsieur Kelly.

Je cède maintenant la parole à M. Long.

[Traduction]

M. Wayne Long: Merci, monsieur le président

Madame Bernier, dans un autre article vous avez fourni des commentaires au sujet de la Loi anti-pourriel. De toute évidence, il y a des entreprises et des commerçants qui la jugent restrictive, et d'un

point de vue évidemment personnel, je comprends qu'elle vise à ce que nous ne soyons pas trop bombardés.

Pourriez-vous me donner vos commentaires? Pensez-vous qu'il y a un équilibre ou que la législation est assez forte?

Mme Chantal Bernier: D'abord, je dois dire que j'écris trop, vraiment.

La Loi canadienne anti-pourriel (LCAP) est un sujet complètement différent, et comme vous le savez, il est aussi très controversé dans l'industrie. De plus, le Commissariat à la protection de la vie privée a publié sa première enquête sur cette loi, et je crois que les consommateurs seront heureux de constater les restrictions qui s'appliquent maintenant à l'industrie.

Pour répondre à votre question en ce qui a trait à l'atteinte d'un juste équilibre, je suggère que nous attendions encore quelques années. Ce que je veux dire par là, c'est que nous devons acquérir plus d'expérience sur le moyen d'évaluer la façon dont les entreprises estiment pouvoir répondre à un véritable désir d'annonces promotionnelles ou d'information, en plus de répondre à leurs propres besoins.

Il y a consentement. Vous pouvez obtenir le droit d'obtenir des informations promotionnelles. En effet, en ce qui a trait à la comparaison qu'a faite M. Saini il y a un instant relativement à la participation ou à la non-participation, ce sujet relève de la Loi sur la protection des renseignements, mais il comprend une structure de contrôle qui permet d'envoyer des messages économiques promotionnels (et commerciaux, de surcroît) aux destinataires consentants et de créer une définition selon laquelle vous voulez tout ou vous ne voulez pas tout. Nous pouvons ainsi trouver un juste équilibre entre les droits du consommateur de ne pas être bombardé, comme vous le dites, et les besoins ou la volonté de l'organisation d'aider ses initiatives de marketing grâce à ce processus.

• (1240)

M. Wayne Long: Jusqu'à quel point devrions-nous être concernés par les applications de consommation exigeant trop d'autorisations? Je ne sais pas si c'était votre bureau ou l'un des bureaux du Commissariat à la protection de la vie privée qui a fait un balayage. Je crois qu'il y avait 1 211 applications, dont 75 % demandaient l'emplacement, l'accès à une pièce d'identité, à la caméra et aux contacts. Jusqu'à quel point cela devrait-il nous inquiéter?

Mme Chantal Bernier: Nous devrions être très inquiets, et heureusement que nous le sommes. Le sondage de janvier 2015 du Commissariat à la protection de la vie privée du Canada révèle que les Canadiens ne sont pas seulement et justement inquiets, mais ils prennent des mesures, et ils vont de plus en plus refuser de télécharger des applications qui sont trop intrusives. Je pense que la prise de conscience donne maintenant lieu à une action, et c'est la façon de voter. Je suppose que, dans ce cas, nous votons avec nos doigts. Nous n'appuyons pas sur Envoyer. Nous ne leur envoyons pas d'information. Nous ne téléchargeons pas.

Nous devons être conscients de cela. Nous devons nous assurer que les développeurs et les entreprises minimisent l'information qu'ils cherchent au moyen des applications. Comme vous parlez tout à l'heure, monsieur Saini, s'ils veulent recueillir beaucoup d'information pour développer une intelligence d'affaires et adapter leurs services aux clients, alors ils doivent obtenir un consentement spécifique pour cela.

M. Wayne Long: D'accord, merci.

[Français]

Le vice-président (M. Joël Lightbound): Nous passons maintenant à M. Bratina.

[Traduction]

M. Bob Bratina: Merci.

Madame Bernier, je crois que vous avez dit un peu plus tôt que vous avez regardé les recommandations d'un oeil favorable. Je ne sais pas si vous êtes en mesure d'analyser soigneusement l'ensemble du rapport, mais permettez-moi de vous poser une question précise. Dans la recommandation 15, le commissaire à la vie privée suggère de modifier la loi pour appliquer la couverture à toutes les institutions gouvernementales, y compris les cabinets des ministres et le bureau du premier ministre. Comment voyez-vous cette recommandation?

Mme Chantal Bernier: Comme mentionné à M. Dusseault, je vois cela favorablement, parce que nous avons un vide juridique en ce moment à cet égard. En d'autres termes, il y a des renseignements personnels détenus ou qui pourraient être détenus par ces bureaux qui ne sont pas actuellement protégés. On observe le fait que le gouvernement au pouvoir, les ministres et le premier ministre disposent du pouvoir du gouvernement. Ainsi, ils devraient être tenus de respecter les normes de la Loi sur la protection des renseignements personnels pour recueillir, utiliser ou divulguer cette information.

M. Bob Bratina: Dans la recommandation 11, la suggestion modifie l'article 64 pour permettre au commissaire de faire, s'il le souhaite, un rapport public sur les questions de protection des renseignements personnels du gouvernement qu'il estime d'intérêt public. Le Commissariat à la protection de la vie privée a déjà le pouvoir de publier des rapports spéciaux et des rapports annuels, et ainsi de suite. À votre avis, est-ce que l'expansion à cet égard est utile?

Mme Chantal Bernier: Elle l'est, absolument. J'ai été confrontée à cette question lorsque nous avons terminé l'enquête sur l'organisme appelé auparavant Emploi et Développement social Canada. Vous vous souviendrez de la perte d'un disque dur contenant l'information financière de 583 000 Canadiens. J'ai senti que c'était une question tout simplement trop importante pour la laisser dans le rapport annuel. Je pensais que le public canadien méritait de recevoir les résultats de notre enquête plus rapidement et c'est ainsi que nous avons déposé un rapport spécial.

Mais il était rédigé dans un style assez guindé et il a coûté cher. Il manquait de flexibilité. Je voulais bien servir le public canadien en leur présentant les résultats de notre enquête, mais je ne pouvais que le faire par le moyen de notre procédure de rapport spécial.

Je crois que cette recommandation est très cohérente et respecte le thème de transparence des recommandations du commissaire.

• (1245)

M. Bob Bratina: Comment croyez-vous que cela fonctionnera dans le cas de certaines violations majeures ou autres? Est-ce que le commissaire à la protection de la vie privée conseillerait le gouvernement qu'il a l'intention de lui en parler? Selon vous, comment cela peut-il fonctionner?

Mme Chantal Bernier: Comme je l'ai mentionné lorsque j'ai décrit le rôle du commissaire à la vie privée en tant qu'agent du Parlement, ce dernier n'a pas besoin d'informer le gouvernement. Il fait des sorties et des déclarations et communique ce qu'il a

découvert et ce sur quoi il fait des rapports. Selon cette façon de faire, cela aurait lieu à la fin d'une enquête ou nous pourrions procéder comme nous l'avons fait pour EDSC.

Lorsque la nouvelle a été divulguée, j'ai immédiatement annoncé que je déposais une plainte, parce que le commissaire peut soit déposer une plainte, soit répondre aux plaintes déposées par un demandeur ou plusieurs plaignants. C'était vraiment trop grave pour ne rien faire, alors j'ai choisi de porter plainte. Ensuite, j'ai décidé de publier le rapport en marge du rapport annuel, mais la contrainte artificielle que j'avais et qui m'obligeait à déposer un rapport spécial, n'était pas vraiment justifiée. C'était vraiment un obstacle à la transparence, sans motif valable.

M. Bob Bratina: Y a-t-il quelque chose dans l'examen qui devrait être mis en lumière et que vous pensiez peut-être aborder dans les recommandations?

Mme Chantal Bernier: L'exception que j'aimerais faire est celle que j'ai soulignée et qui a rapport à la recommandation sur la nécessité. Il s'agit de la recommandation 4, où le commissaire dit qu'un élément devrait être prouvé comme étant nécessaire au programme ou à l'activité du gouvernement. Je juge ce critère inhérent comme étant insuffisant. Il devrait y avoir un test externe intégré à la charte.

M. Bob Bratina: Oui. Ce sont de bons commentaires. Merci.

Le vice-président (M. Joël Lightbound): Merci, monsieur Bratina.

Il y a encore Mme Dzerowicz et M. Saini qui aimeraient poser quelques questions. Je vous demanderais d'être bref parce qu'il ne nous reste que 10 minutes.

Nous commencerons avec vous, madame Dzerowicz.

Mme Julie Dzerowicz: Merci beaucoup.

Je sais que la Loi sur la protection des renseignements personnels est différente de la LPRPDE. Google recueille beaucoup d'informations sur moi. Devrait-il y avoir un meilleur lien entre les deux, entre la LPRPDE et la Loi sur la protection des renseignements personnels? Ma question est d'ordre général.

De plus, la technologie change assez rapidement maintenant. Comment faire en sorte que notre législation soit appropriée et actuelle?

Ensuite, j'aurai une autre question pour Mme Culloch et M. Guénette.

Mme Chantal Bernier: C'est une question pertinente.

Tout d'abord, pour mettre les choses en perspective, l'Europe ne dispose pas d'une législation distincte pour les secteurs public et privé, et je me suis souvent demandé si nous devrions suivre leur exemple. Mais nous avons une législation distincte, et nous avons un excellent système. La raison pour laquelle nous avons une législation distincte est facilement du fait de la différence dans les paradigmes juridiques qui forment l'ensemble des secteurs public et privé. Ici encore, cela renvoie à ma réponse à Mme Rempel qui concerne la relation entre l'État et le citoyen en vertu de la Loi sur la protection des renseignements personnels, qui est strictement fondée sur la nécessité. L'État ne peut pas empiéter sur votre vie privée à moins que l'on puisse le justifier pleinement dans une société libre et démocratique.

La relation que vous avez avec d'autres détenteurs de données, comme Google, Facebook ou toute entreprise auprès de laquelle vous achetez quelque chose est fondée sur votre relation, votre relation libre avec eux; ce qui signifie qu'elle est basée sur le consentement.

Je crois que la façon dont nous avons construit notre système fonctionne très bien. Cependant, le lien que vous soulignez est extrêmement important et il l'est de plus en plus. Nous l'avons vu avec l'attribution de fonctions au secteur privé. De toute évidence, la grande épreuve de force d'Apple et du FBI en est un bon exemple aux États-Unis. Ils détiennent un trésor d'informations au sein du secteur privé auxquelles les organismes chargés d'appliquer la loi, c'est-à-dire le secteur public, veulent avoir accès. Comment réglémentons-nous ce lien?

Des éclaircissements ont été apportés au Canada. L'un d'entre eux concerne *R. v. Spencer*, comme je l'ai mentionné plus tôt. Un autre apporté plus récemment et qui se rapporte directement votre question est l'arrêt *R. c. Rogers Communications Partnership*. C'était en janvier 2016. Il était question d'un mandat judiciaire pour un dépotier de tours qui aurait donné à la police toutes les communications ayant eu lieu à proximité d'une tour cellulaire précise, ce qui lui aurait permis d'obtenir les communications de 43 000 personnes ayant eu lieu entre, environ, 15 heures et 17 heures cette journée-là. Pourquoi? Parce qu'il y avait eu un vol de bijouterie à ce moment-là, cette journée-là. Rogers a refusé et s'est opposé au mandat judiciaire, et la police a abandonné ses démarches. Toutefois, Rogers est tout de même allé en cour et a dit que le mandat était invalide puisqu'il était beaucoup trop large. La police a répondu par l'intermédiaire de la vérificatrice générale que Rogers n'avait pas la qualité pour agir dans cet enjeu, alors que la cour (et cela est très important pour votre question) a dit que Rogers était en droit de refuser de se conformer à ce mandat judiciaire, puisque celui-ci était trop large pour être constitutionnel, mais Rogers avait l'obligation de s'opposer au mandat en raison de son obligation contractuelle envers ses clients.

Je crois que cela illustre le lien que vous faites entre le secteur public et le secteur privé.

• (1250)

Le vice-président (M. Joël Lightbound): M. Saini aura maintenant la parole pendant trois minutes.

M. Raj Saini: J'ai une dernière question, madame Bernier. Vous avez soulevé un point que je trouve très curieux. Vous avez parlé du fait que Dentons est une entreprise internationale. De toute évidence, si vous avez des bureaux partout dans le monde, vous avez différents systèmes de protection des renseignements personnels dans les différentes juridictions. En effet, quel que soit le système en place

dans un pays, il y a une demande de ressources, qu'elle soit humaine ou financière. Si vous avez des clients qui font des affaires dans plusieurs juridictions, comment établissez-vous un équilibre dans tout cela pour avoir une seule norme?

Appliquez-vous des normes multiples ou y a-t-il un transfert des responsabilités là où les affaires ont lieu, ou là où le cas est jugé ou entendu? Comment trouvez-vous un équilibre dans tout cela?

Mme Chantal Bernier: Nous devons suivre la loi partout où nous opérons, et chaque pays a ses propres lois.

J'étais dans notre bureau de Singapour récemment et nous avons discuté plus particulièrement de la façon de gérer le droit à la vie privée à Singapour, mais dans ce cas il s'agissait d'une entreprise canadienne désireuse d'aller s'installer là-bas. Les règles en matière de compétence qui encadrent la loi sur la protection des renseignements personnels sont telles que là où nous effectuons une opération et là où nous recueillons l'information, nous devons toujours respecter les lois qui ont été adoptées dans ce pays.

Toutefois, les lois transfrontalières diffèrent. Certains pays ne permettent pas les transferts transfrontaliers de renseignements personnels de leurs citoyens, s'ils ne sont pas régis par des règles, des conditions très strictes, et ainsi de suite. D'autres pays exigent avant tout une diligence raisonnable, en disant que vous pouvez effectuer des transferts transfrontaliers de renseignements personnels, mais en veillant à ce que, lors d'un transfert, l'information soit protégée dans le respect des lois canadiennes. Ils le font en choisissant d'abord des entrepreneurs très fiables, puis en adoptant des clauses contractuelles selon lesquelles l'entrepreneur protégera l'information aussi rigoureusement, que le client ayant recours à l'entrepreneur pour transférer l'information sera lié à l'entrepreneur et qu'il fera des vérifications à son sujet. Des règles de conformité comme celles-là ont été mises en place.

Oui, ces lois conflictuelles constituent définitivement un défi, un défi qu'il faut relever dans le respect des règles.

Le vice-président (M. Joël Lightbound): Merci beaucoup. J'aurais eu quelques questions pour Mme Bernier, mais je suppose que nous allons devoir vous réinviter. Comme je présidais, cela a été un sacrifice pour moi de ne pas pouvoir poser mes questions. Ce sera pour une autre fois.

Merci à tous d'avoir été avec nous aujourd'hui. Nous vous en sommes reconnaissants et je souhaite à tous les membres une joyeuse Action de grâce. Nous nous reverrons dans deux semaines.

[Français]

Merci à toutes et à tous et bonne journée.

La séance est levée.

Publié en conformité de l'autorité
du Président de la Chambre des communes

PERMISSION DU PRÉSIDENT

Les délibérations de la Chambre des communes et de ses comités sont mises à la disposition du public pour mieux le renseigner. La Chambre conserve néanmoins son privilège parlementaire de contrôler la publication et la diffusion des délibérations et elle possède tous les droits d'auteur sur celles-ci.

Il est permis de reproduire les délibérations de la Chambre et de ses comités, en tout ou en partie, sur n'importe quel support, pourvu que la reproduction soit exacte et qu'elle ne soit pas présentée comme version officielle. Il n'est toutefois pas permis de reproduire, de distribuer ou d'utiliser les délibérations à des fins commerciales visant la réalisation d'un profit financier. Toute reproduction ou utilisation non permise ou non formellement autorisée peut être considérée comme une violation du droit d'auteur aux termes de la *Loi sur le droit d'auteur*. Une autorisation formelle peut être obtenue sur présentation d'une demande écrite au Bureau du Président de la Chambre.

La reproduction conforme à la présente permission ne constitue pas une publication sous l'autorité de la Chambre. Le privilège absolu qui s'applique aux délibérations de la Chambre ne s'étend pas aux reproductions permises. Lorsqu'une reproduction comprend des mémoires présentés à un comité de la Chambre, il peut être nécessaire d'obtenir de leurs auteurs l'autorisation de les reproduire, conformément à la *Loi sur le droit d'auteur*.

La présente permission ne porte pas atteinte aux privilèges, pouvoirs, immunités et droits de la Chambre et de ses comités. Il est entendu que cette permission ne touche pas l'interdiction de contester ou de mettre en cause les délibérations de la Chambre devant les tribunaux ou autrement. La Chambre conserve le droit et le privilège de déclarer l'utilisateur coupable d'outrage au Parlement lorsque la reproduction ou l'utilisation n'est pas conforme à la présente permission.

Aussi disponible sur le site Web de la Chambre des communes à l'adresse suivante : <http://www.noscommunes.ca>

Published under the authority of the Speaker of
the House of Commons

SPEAKER'S PERMISSION

The proceedings of the House of Commons and its Committees are hereby made available to provide greater public access. The parliamentary privilege of the House of Commons to control the publication and broadcast of the proceedings of the House of Commons and its Committees is nonetheless reserved. All copyrights therein are also reserved.

Reproduction of the proceedings of the House of Commons and its Committees, in whole or in part and in any medium, is hereby permitted provided that the reproduction is accurate and is not presented as official. This permission does not extend to reproduction, distribution or use for commercial purpose of financial gain. Reproduction or use outside this permission or without authorization may be treated as copyright infringement in accordance with the *Copyright Act*. Authorization may be obtained on written application to the Office of the Speaker of the House of Commons.

Reproduction in accordance with this permission does not constitute publication under the authority of the House of Commons. The absolute privilege that applies to the proceedings of the House of Commons does not extend to these permitted reproductions. Where a reproduction includes briefs to a Committee of the House of Commons, authorization for reproduction may be required from the authors in accordance with the *Copyright Act*.

Nothing in this permission abrogates or derogates from the privileges, powers, immunities and rights of the House of Commons and its Committees. For greater certainty, this permission does not affect the prohibition against impeaching or questioning the proceedings of the House of Commons in courts or otherwise. The House of Commons retains the right and privilege to find users in contempt of Parliament if a reproduction or use is not in accordance with this permission.

Also available on the House of Commons website at the following address: <http://www.ourcommons.ca>