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 021 • 1re SESSION • 42e LÉGISLATURE

TÉMOIGNAGES

Le mardi 14 juin 2016

Président

M. Blaine Calkins

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

Le mardi 14 juin 2016

● (0855)

[*Traduction*]

Le président (M. Blaine Calkins (Red Deer—Lacombe, PCC)): Nous reprenons la séance. Merci beaucoup, chers collègues, d'avoir pris soin de ces quelques points importants.

Nous avons maintenant le plaisir de reprendre notre étude de la Loi sur la protection des renseignements personnels. Conformément au sous-alinéa 108(3)h)(i), nous étudions la Loi sur l'accès à l'information.

Nous sommes heureux d'avoir avec nous ce matin les témoins suivants: Teresa Scassa, professeure titulaire de l'Université d'Ottawa et Chaire de recherche du Canada en droit d'information; David Lyon, qui se joint à nous par vidéoconférence et qui est professeur à l'Université Queen's; enfin, Lisa Austin, professeure agrégée, Université de Toronto, Faculté de droit, David Asper Centre for Constitutional Rights.

Merci beaucoup d'avoir pris le temps de vous joindre à nous, et merci d'avoir eu la patience d'attendre que nous finissions de traiter quelques affaires au début de cette réunion du Comité. Nous venons de terminer notre étude de la Loi sur l'accès à l'information, et maintenant nous allons poursuivre notre étude de la Loi sur la protection des renseignements personnels.

Nous allons vous demander à chacun de nous présenter une allocution d'environ 10 minutes. Nous procéderons ensuite à des rondes de questions qui dureront, je l'espère, jusqu'à la fin de cette réunion de deux heures.

En suivant l'ordre dans lequel les témoins sont inscrits sur ma feuille, nous allons commencer par Teresa; à vous la parole.

Mme Teresa Scassa (professeure titulaire, Université d'Ottawa, Chaire de recherche du Canada en droit d'information, à titre personnel): Merci, monsieur le président, et merci de m'avoir offert cette occasion de parler au Comité de la réforme de la Loi sur la protection des renseignements personnels.

J'ai eu l'occasion de lire les recommandations du commissaire sur la réforme de cette Loi, et je suis d'accord avec la majorité de ces propositions. Je vais concentrer mon allocution sur quelques enjeux particuliers liés au thème de la transparence.

Lorsque le gouvernement recueille, utilise et divulgue les renseignements personnels de manière plus transparente, il protège mieux les renseignements personnels en exposant les commentaires et les examens et en favorisant la surveillance et la reddition de comptes. La transparence est également cruciale pour maintenir la confiance du public sur la manière dont le gouvernement traite les renseignements personnels.

L'appel à la transparence doit partir du milieu informatique, qui est en pleine évolution. Non seulement la technologie permet de recueillir et d'emmagasiner un niveau de données inimaginable, mais les nouvelles capacités d'analyse ont aussi considérablement altéré la valeur de l'information dans les secteurs public et privé. Cette valeur améliorée incite à recueillir plus de renseignements personnels qu'il le faut, puis de les transmettre entre ministères et secteurs, de les extraire et de les compiler afin de les analyser et de les conserver plus longtemps que ce qui était requis initialement.

C'est pourquoi je tiens à souligner l'importance de la recommandation du commissaire d'amender la Loi sur la protection des renseignements personnels afin de mieux expliquer la « nécessité » de recueillir des renseignements personnels et de définir clairement le terme « nécessaire ».

Cette recommandation vise à limiter la collecte exagérée de renseignements personnels. Une telle collecte va à l'encontre des attentes du public, qui fournit des renseignements au gouvernement à des fins précises et limitées. Elle rend aussi les Canadiens plus vulnérables à la négligence, à l'inconduite ou même aux cyberattaques dont découle souvent la violation des données.

La minimisation des données est un principe important qu'appuient les autorités chargées de la protection des données dans le monde entier. Ce principe se retrouve dans les lois sur la protection des renseignements personnels. Il devrait figurer explicitement et bien en vue dans la version réformée de notre Loi sur la protection des renseignements personnels.

La minimisation des données améliore aussi la transparence. En fixant des limites claires à la collecte de renseignements personnels, on favorise la transparence des objectifs de la collecte. D'un autre côté, la collecte exagérée favorise la réorientation de l'objectif de la collecte ainsi que l'usage injustifié des renseignements et leur divulgation exagérée.

L'exigence visant à limiter la collecte de renseignements à des fins précises et nécessaires est reliée à celle exhortant le gouvernement à recueillir les renseignements personnels directement de la personne dans la mesure du possible. Ces exigences accroissent très évidemment la transparence puisque la personne est directement au courant de la collecte desdits renseignements.

Cette règle générale comporte cependant de nombreuses exceptions. Citons par exemple les circonstances dans lesquelles des renseignements sont communiqués à des enquêteurs dans le cadre d'une enquête ou de l'application d'une loi; ils peuvent aussi être divulgués à des représentants du gouvernement en vertu d'une ordonnance ou d'une sommation du Tribunal. Bien que ces exceptions s'avèrent souvent nécessaires, il faut en tenir compte dans le contexte de l'évolution des données auquel nous faisons face à l'heure actuelle.

Les entreprises du secteur privé recueillent maintenant de gros volumes de renseignements personnels, qui comprennent souvent de l'information biographique fondamentale. Nous devrions donc nous inquiéter profondément de ce que les exceptions laxistes de la LPRPDE et du Code criminel permettent à un volume massif de renseignements personnels de circuler du secteur privé vers le gouvernement sans que la personne à qui ils appartiennent n'en ait connaissance.

Ces requêtes ou ces ordonnances sont souvent, mais pas toujours, déposées dans le cadre d'enquêtes criminelles ou d'enquêtes liées à la sécurité nationale. Cette collecte n'est aucunement transparente, et les personnes touchées n'en ont pas connaissance; d'ailleurs, ces pratiques générales ne sont pas transparentes; le grand public et le Commissariat à la protection de la vie privée, ou CPVP, n'en sont pas informés.

Nous avons surtout entendu parler de ce problème lorsqu'on demande ou qu'on ordonne régulièrement aux sociétés de télécommunication de fournir des renseignements détaillés à la police ou à d'autres agents du gouvernement. Soulignons cependant que bien d'autres sociétés recueillent sur des individus des renseignements personnels qui révèlent une grande partie de leurs activités et de leurs choix. Il est important de ne pas considérer ce problème comme étant moins important parce que ces individus ont manifesté un comportement antisocial. Les ordonnances des tribunaux et les demandes de renseignements risquent, et le font, d'englober les renseignements personnels d'un grand nombre de Canadiens qui ne sont pas soupçonnés d'inconduite. Par exemple, un plaidoyer devant la Cour suprême de l'Ontario a récemment souligné le problème des vastes ordonnances de production de données relatives à la téléphonie cellulaire, ou mandats de type « tower dump ». Dans cette affaire, le mandat initial exigeait des renseignements personnels extrêmement détaillés sur environ 43 000 personnes; la majorité de ces personnes n'avaient rien fait de mal, que d'utiliser leurs cellulaires dans une région particulière à une heure particulière.

Soulignons que la capacité de mener des analyses complexes incitera toujours plus les enquêteurs à obtenir du secteur privé de gros volumes de données pour trouver un individu qui aurait mené un certain type d'activités.

Si le secteur privé effectue la collecte de renseignements personnels sans transparence, le public ne croira jamais que le secteur privé n'abuse pas de cette autorité. Les améliorations récentes de la transparence — comme les directives de l'ISDE sur la transparence volontaire dans la production de rapports — visent avant tout la transparence dans le secteur privé. Autrement dit, les sociétés de télécommunication ont essayé d'établir un cadre de rapport sur le nombre de demandes qu'elles reçoivent d'organismes gouvernementaux avec le nombre auxquelles elles répondent, etc. Mais ces lignes directrices sont entièrement volontaires, et elles ne s'appliquent qu'au secteur des télécommunications alors qu'il faudrait exiger cette divulgation de toutes les entreprises du secteur privé.

● (0900)

Ces lignes directrices s'appliquent aussi à la transparence de la production de rapports des entreprises elles-mêmes. Aucune loi n'exige que les intervenants gouvernementaux présentent des rapports pertinents au public ou au Commissariat à la protection de la vie privée du Canada sur les renseignements personnels qu'ils recueillent de sociétés privées. Soulignons que l'audit que le CPVP a essayé d'entamer sur les demandes de renseignements que la GRC exige sans mandat sur les données des abonnés a pris fin lorsqu'il a découvert que la GRC ne tient pas de dossiers précis sur ces pratiques.

À mon avis, la modernisation de la Loi sur la protection des renseignements personnels devrait viser directement cette capacité qu'ont maintenant les institutions gouvernementales d'accéder à de vastes sources de renseignements personnels que détient le secteur privé. La loi qui permet d'obtenir des renseignements personnels du secteur privé devrait inclure des exigences sur la transparence des rapports de collecte. De plus, la loi devrait indiquer de quelle façon les intervenants du gouvernement qui obtiennent ces renseignements personnels du secteur privé, en présentant soit une demande de renseignements, soit une ordonnance du Tribunal, devraient traiter ces renseignements. Plus précisément, la loi devrait fixer des limites sur l'usage et sur la période de conservation des renseignements.

Il est vrai que la LPRPDE et le Code criminel autorisent les services de police et les organismes d'enquête qui relèvent des gouvernements fédéral et provinciaux à obtenir des renseignements personnels du secteur privé dans les mêmes conditions et que la réforme de la Loi sur la protection des renseignements personnels n'imposera pas de transparence et de reddition de comptes aux intervenants provinciaux. Ces faits suggèrent que l'on pourrait aussi aborder les questions de transparence et de reddition de comptes dans la LPRPDE et dans le Code criminel — dont votre Comité envisage aussi d'étudier la réforme éventuelle —, mais ce n'est pas une raison pour ne pas aborder ces questions dans la Loi sur la protection des renseignements personnels. Tant que les institutions gouvernementales recueillent des renseignements personnels de manière indirecte, la Loi sur la protection des renseignements personnels devrait imposer la transparence et la reddition de comptes à ces activités.

Le commissaire soulève aussi la question de la transparence du partage de cette information au sein du gouvernement. Grâce aux progrès de la technologie, les ministères et les agences du gouvernement peuvent échanger plus facilement des renseignements personnels, ce qu'ils font « à très grande échelle », comme l'a écrit le commissaire.

La Loi sur la protection des renseignements personnels autorise l'échange d'information entre gouvernements, qu'ils soient nationaux ou étrangers, et cela dans des circonstances particulières comme des enquêtes menées par des services d'application de la loi, par exemple, ou à des fins qui correspondent à celles de la collecte de l'information en question. Le commissaire Therrien recommande des amendements qui exigeraient que tout échange d'information entre gouvernements se fasse dans le cadre d'ententes écrites explicites. On garantirait ainsi que l'échange d'information est conforme à la loi et l'on présenterait aussi au public un certain degré de transparence. En effet, les gens ont le droit de savoir si les renseignements qu'ils fournissent à une agence ou à un ministère seront divulgués et, dans l'affirmative, dans quelles conditions leurs renseignements personnels seront transmis à des gouvernements provinciaux ou étrangers.

Nous avons un autre problème de transparence lié à la déclaration obligatoire des atteintes à la protection des données.

À l'heure actuelle, le Secrétariat du Conseil du Trésor exige que les ministères informent le CPVP de toute atteinte à la protection des données, mais le commissaire a remarqué que tous les ministères ne s'y conforment pas. Il demande donc que l'on amende la loi pour y inclure la déclaration obligatoire de toute atteinte à la protection des données. Le Parlement a récemment amendé la LPRPDE en y ajoutant cette obligation. Lorsque ces dispositions seront en vigueur, le secteur public sera soumis à des normes plus élevées si l'on n'amende pas également la Loi sur la protection des renseignements personnels.

En modifiant la Loi fédérale sur la protection des renseignements personnels pour y ajouter l'obligation de déclarer l'atteinte à la protection des données, il faudra tenir compte de la nécessité d'en avertir le commissaire et les personnes touchées en leur indiquant qu'une infraction ainsi commise pourrait atteindre un certain seuil de préjudice, comme la LPRPDE l'exigera aussi.

Les amendements apportés à la LPRPDE exigeront aussi que l'on tienne des dossiers sur toutes les infractions aux mesures de sécurité, qu'elles atteignent ou non le seuil de préjudice exigeant qu'on les déclare officiellement. Le Parlement devrait exiger que les organismes régis par la Loi sur la protection des renseignements personnels tiennent des dossiers et présentent au CPVP des rapports sur ces événements. Ces rapports serviraient à cerner des pratiques ou des tendances dans chaque ministère ou organisme, ou entre ministères et organismes. Cette capacité de détecter les problèmes proactivement soit là où ils se manifestent, soit dans tout le gouvernement fédéral, ne pourra que renforcer la sécurité des données. Cela devient d'autant plus urgent que nous vivons en une ère de menace à la cybersécurité.

Je vais conclure mon allocution sur ce point.

Merci beaucoup, monsieur le président.

● (0905)

Le président: Merci beaucoup.

Je crois que la conversation que nous aurons avec vous sera très intéressante.

Nous allons maintenant passer la parole à M. Lyon pour 10 minutes.

M. David Lyon (professeur, Queen's University, à titre personnel): Merci beaucoup de m'avoir invité à prendre part à cette initiative très importante. La Loi sur la protection des renseignements personnels est désuète. Les Canadiens ont un besoin urgent d'une nouvelle loi qui réagisse fortement à l'incroyable progrès technologique et aux virages politiques et économiques qui se déroulent depuis les années 1980.

J'appuie les propositions générales du commissaire à la vie privée, et je l'en remercie. Toutefois, je ne suis pas avocat et je ne suis pas expert en droit. Je parle dans l'esprit d'un professeur de sciences sociales. Je dirige le Surveillance Studies Centre de l'Université Queen's.

Le dernier ouvrage que j'ai publié s'intitule *Surveillance after Snowden*. Je dirige à l'heure actuelle une équipe qui mène le projet Big Data Surveillance. J'écris aussi un nouveau livre intitulé *The Culture of Surveillance*. Je vous dis tout cela simplement pour vous indiquer le point de vue à partir duquel je vous parle, c'est-à-dire le contexte général de cet acte, et non les détails.

Tout d'abord, permettez-moi de souligner que notre équipe de recherche a publié, il y a deux ou trois ans, un ouvrage intitulé *Vivre à nu: La surveillance au Canada*. C'est une étude très facile à comprendre sur les tendances de la surveillance à l'heure actuelle. Je recommande au Comité de le consulter. Vous le trouverez dans toute bonne librairie et vous pouvez même le télécharger d'Internet.

[*Français*]

C'est aussi disponible en français, sous le titre *Vivre à nu: La surveillance au Canada*.

[*Traduction*]

Cet ouvrage présente les enjeux clés de la surveillance au XXI^{e} siècle. Les lecteurs intéressés y trouveront une description approfondie du contexte qui nous incite à demander l'amendement de la Loi sur la protection des renseignements personnels.

Les auteurs examinent, en présentant des exemples canadiens, les tendances telles que l'augmentation rapide des niveaux de surveillance, les préoccupations qui déclenchent les activités de surveillance, la confusion des limites entre les secteurs public et privé — les divulgations de Snowden ont établi cela très clairement —, l'ambiguïté des renseignements personnels, le développement de la surveillance mobile et géodépendante, l'intégration de la surveillance dans les milieux quotidiens — appelée souvent « Internet des objets » —, la croissance de la biométrie ainsi que la surveillance sociale qui envahit Facebook, Twitter et les autres médias.

La Loi sur la protection des renseignements personnels repose sur des idées plutôt fixes liées à qui recueille ces renseignements et où ils sont retransmis, le cas échéant. À l'heure actuelle, nous devrions nous concentrer sur leur mobilité et non sur leur fixité. Les termes tels que « bases de données » représentent l'ancien document et suggèrent le cloisonnement au lieu des voies multiples qu'empruntent les données à l'heure actuelle. Dans le passé, l'information se trouvait à des endroits bien précis, et l'on ne pouvait la transmettre que dans des circonstances très particulières.

Il est bien entendu urgent de limiter cette pratique, comme nous venons de l'entendre. Nous devons reconnaître que le partage d'information à l'heure actuelle s'exécute à une échelle dont nous n'aurions pas rêvé dans les années 1980, une échelle qui serait très difficile à quantifier, et encore plus difficile à contrôler.

Ce partage s'exécute aussi à travers des limites qui représentent la distinction entre les activités gouvernementales et commerciales dans les deux lois fédérales principales de 1982 et de 2004. Les auteurs de la loi de 1982 n'avaient jamais imaginé la circulation des données entre ces deux domaines; c'est là le problème clé à aborder dans tout examen mené sur cette question.

En même temps, la surveillance peut s'effectuer, et cela se fait, sans mécanismes indiquant clairement quels renseignements sont personnels. Aujourd'hui, il est difficile de définir la catégorie des renseignements personnels. Il fut un temps où il s'agissait tout simplement du nom, de l'adresse, du numéro de téléphone et peut-être d'une indication officielle comme le numéro d'assurance sociale. Aujourd'hui, une photo de vos plaques d'auto prise sur la route compte aussi et, bien que cela porte à controverse, les adresses IP des ordinateurs.

On peut aussi identifier une personne par reconnaissance faciale. Le logiciel utilisé quotidiennement dans Facebook ne nécessite pas un compte Facebook pour fonctionner. Il est en fait très facile d'identifier les gens sans même disposer de leurs renseignements personnels. Une étude menée récemment à Montréal a indiqué que l'on peut identifier positivement 98 % des gens par leur date de naissance, leur sexe et leur code postal, sans même connaître leurs noms et de leurs adresses.

● (0910)

Nous en avons un autre exemple dans le débat post-Snowden qui cherche à déterminer si les métadonnées des messages téléphoniques et Internet sont aussi des données personnelles. Certains affirment que cela dépend du contexte, pensant à tort qu'il s'agit de renseignements tirés de l'annuaire téléphonique et non du contenu des messages, mais la plupart du temps, ces métadonnées révèlent plus d'information que l'on pense.

Les deux enjeux mentionnés ont trait aux changements socio-techniques et politico-économiques survenus au cours de ces 40 dernières années. Je vais maintenant me concentrer sur des questions de recherche et d'éducation, que le commissaire mentionne également.

D'un côté, il faudra mener beaucoup plus de recherche pour bien comprendre les changements énormes qui ont eu lieu depuis les années 1980. Soulignons qu'il s'agit de changements sociotechniques et politico-économiques que l'on ne peut pas se permettre d'enfermer simplement dans des catégories techniques et juridiques.

Pendant plusieurs années, le commissaire a dirigé un programme efficace d'études de recherche subventionnées. Toutefois, vu l'ampleur des enjeux traités et le fait qu'ils se centrent sur des questions allant de la sécurité nationale à la vie domestique, il faudra mener beaucoup plus de recherche pour mettre à jour la loi qui régit l'usage des données personnelles; en effet, il faudra que cette loi aborde sérieusement la vie de toutes les personnes qui subissent une surveillance quelconque, c'est-à-dire tout le monde.

On pourrait étendre ce programme de recherche pour qu'il constitue l'étude de contexte de la révision de la Loi sur la protection des renseignements personnels. On pourrait aussi l'étendre si les trois Conseils ou si la Société royale du Canada commandait un rapport sur les lois canadiennes qui régissent la surveillance et la protection des renseignements personnels.

Il est aussi clair qu'il y aura beaucoup à faire dans le domaine de l'éducation. On pourrait pour cela étendre le mandat du commissaire à la vie privée pour le charger de coordonner les activités d'éducation à ce sujet.

Dans les années 1980, l'informatique se limitait encore aux ordinateurs centraux et personnels. La popularité des systèmes de diffusion, des appareils mobiles et du nuage ne se manifestait pas encore. En ce temps-là, pour communiquer avec autrui, par exemple, avec ce qui est devenu Internet dans les années 1990, il fallait utiliser un système encombrant où l'on branchait le récepteur du téléphone dans des poches de caoutchouc — je ne sais pas si quelqu'un ici se rappelle, on appelait cela un coupleur acoustique —, pour créer un modem très incertain de transmission des données.

À l'heure actuelle, les appareils et les réseaux informatiques prolifèrent tellement qu'il faut concevoir des méthodes nouvelles de ce qu'on devrait nommer « une citoyenneté numérique adaptée à tous les âges ». Il faut que tous les Canadiens soient au courant de leurs droits, comprennent les problèmes et s'engagent activement et de manière éclairée. Cette obligation ne s'applique pas à une minorité. Ce n'est pas une activité secondaire. Le commissaire pourrait aussi lancer cette éducation. Elle pourrait accompagner la nouvelle loi et s'inspirer du travail de nombreux organismes qui se concentrent sur cette question. Vous trouverez quelques références à ce sujet dans le court mémoire que je vous ai remis.

Je suis convaincu que les faits que je viens de décrire constituent les éléments essentiels de la révision de la Loi sur la protection des renseignements personnels. Toutefois, il me semble que le coeur du débat devrait virer vers un examen approfondi de l'orientation éthique afin d'assurer l'usage le plus juste et équitable des médias numériques et des renseignements personnels. Cela assurerait l'utilisation optimale du potentiel extraordinaire qu'offrent les technologies numériques.

Le concept même de la protection des renseignements personnels, bien sûr, s'est transformé depuis les années 1980. Ces enjeux ne sont ni mineurs, ni secondaires. Nous ne pouvons pas nous permettre de les aborder uniquement en termes techniques et juridiques. Non seulement nous risquons de porter atteinte à la protection des données en abusant de ces puissantes technologies, mais nous avons là une occasion de rehausser la liberté et l'épanouissement des humains en améliorant ou en réduisant la surveillance, qu'elle soit menée par un gouvernement ou par une grande entreprise.

Comme l'a dit Eric Stoddart, nous passons aujourd'hui beaucoup de temps à surveiller et à suivre la surveillance d'autrui. Nous ferions mieux de nous efforcer d'utiliser la surveillance pour favoriser l'épanouissement humain, c'est-à-dire de mener de la surveillance pour autrui.

● (0915)

Merci beaucoup.

Le président: Merci beaucoup, monsieur Lyon.

Nous passons maintenant à notre dernier témoin.

Madame Austin, vous avez la parole pour 10 minutes.

Mme Lisa Austin (professeure agrégée, Université de Toronto, Faculté de Droit, David Asper Centre for Constitutional Rights, à titre personnel): Merci.

Je vous remercie de m'avoir invitée à comparaître ici aujourd'hui. Je me félicite d'en avoir l'occasion. J'ai rédigé un mémoire à l'intention du Comité. Sa traduction est en cours et la version française vous sera transmise par la suite. Mes observations aujourd'hui sont un résumé de ce mémoire. Je serai heureuse de répondre à vos questions.

Le point fondamental que je veux faire ressortir aujourd'hui, c'est que la réforme de la Loi sur la protection des renseignements personnels doit tenir compte de la Charte canadienne des droits et libertés et de ce qu'elle prévoit en matière de protection de la vie privée. Nous ne devons pas assimiler conformité à la Loi sur la protection des renseignements personnels et conformité à la Charte, pas plus que nous devons penser que l'intégration plus poussée des principes équitables en matière d'information dans la Loi sur la protection des renseignements signifie qu'elle sera conforme aux exigences de protection de la vie privée prévues par la Charte.

Il est essentiel de bien le comprendre, parce que nous sommes maintenant à une époque où le gouvernement recueille de grandes quantités d'information sur les particuliers et les communique tant à l'intérieur du gouvernement qu'avec d'autres gouvernements, y compris des gouvernements étrangers. Cela se fait non seulement à des fins de prestation de services sociaux, mais également à des fins d'application de la loi et de sécurité nationale, comme les deux témoins précédents l'ont souligné. En effet, lorsque le précédent gouvernement a déposé le projet de loi C-51 et adopté la nouvelle Loi sur la communication d'information ayant trait à la sécurité du Canada, on a dit aux Canadiens qu'il y avait, du fait que la Loi sur la protection des renseignements personnels s'appliquait et que le commissaire à la protection de la vie privée en surveillerait l'application, un équilibre approprié entre la protection de vie privée des citoyens et les nécessités de la sécurité nationale. Il s'agit d'une illusion, et d'une dangereuse illusion.

Il est vrai que la Loi sur la protection des renseignements personnels est une loi quasi constitutionnelle. La Cour suprême l'a affirmé à de nombreuses reprises. Cependant, il ne faut pas en faire l'équivalent de droits constitutionnels à la protection de la vie privée. La Loi sur la protection des renseignements personnels repose sur ce qui est venu à être connu, au plan international, sous le nom de « principes équitables en matière d'information ». Il s'agit, dans sa forme élémentaire, d'une réaction à l'État administratif et à ses pratiques en matière d'information. Un particulier voulant obtenir des services gouvernementaux dans un État fournisseur de services de bien-être social est intéressé à recevoir ces services. L'administration de ces services exige que des renseignements personnels soient recueillis et traités, si bien que l'intérêt du particulier relativement à ces renseignements personnels n'est pas d'empêcher qu'ils soient recueillis, utilisés ou divulgués, mais d'en empêcher la collecte excessive ou leurs utilisations ou divulgations subséquentes à des fins différentes, ainsi que d'en assurer l'exactitude. Le droit central du particulier est d'avoir accès aux renseignements à son sujet que l'État possède et d'en corriger les inexactitudes. Cette loi n'a jamais vraiment eu pour objet de régir, avec quelque rigueur, les activités d'application de la loi ou de sécurité nationale, et bon nombre de ses exceptions visent de telles utilisations.

Par contraste, la protection constitutionnelle de la vie privée au Canada procède, dans une large mesure, de l'article 8 de la Charte, bien que la vie privée soit aussi protégée par l'article 7. Son paradigme central est le contexte des fouilles, perquisitions et saisies, où l'État cherche à recueillir de l'information dans le cadre d'enquêtes à des fins d'application de la loi. Ici, l'intérêt du particulier est complètement à l'opposé de l'intérêt de l'État. La relation est coercitive. Le droit central du particulier est d'être protégé contre l'accès abusif de l'État par l'exigence d'obtenir un mandat et l'application du critère des motifs raisonnables et probables. Il s'agit de deux structures différentes, mais qui doivent être fusionnées pour peu que nous pensions que la Loi sur la protection des renseignements personnels puisse avoir quelque pertinence dans les pratiques en matière d'information dont le gouvernement fait un recours accru à des fins d'application de la loi et de sécurité nationale. Un examen fondé sur la Charte devrait renforcer l'examen prévu par la Loi sur la protection des renseignements personnels, en particulier dans ce contexte.

À la lumière de ce qui précède, j'ai formulé à votre intention quatre recommandations, qui se retrouvent d'ailleurs dans mon mémoire écrit.

En premier lieu, il y a un principe interprétatif. Nous recommandons d'inclure dans la Loi sur la protection des renseignements personnels un renvoi aux droits à la vie privée protégés par la Charte canadienne des droits et libertés. Il faudrait le faire figurer dans l'article de déclaration de l'objet de la loi afin de permettre des arguments se rapportant à la Charte des droits et libertés.

En deuxième lieu, nous recommandons que les pratiques du gouvernement en matière d'information soient examinées dans l'optique du respect des droits garantis par la Charte. La norme de nécessité préconisée par le Commissariat à la protection de la vie privée du Canada n'est pas suffisante. Elle est mieux que ce qui existe actuellement et elle est utile dans bien des contextes, mais elle n'est pas suffisante.

Pourquoi? Les droits garantis par la Charte peuvent être en cause dans la collecte, l'utilisation ou la divulgation des renseignements personnels. La Charte entre en jeu lorsqu'il y a une attente raisonnable de respect de la vie privée; ce n'est pas simplement quand des renseignements personnels sont recueillis, utilisés ou divulgués, mais quand il y a une attente raisonnable de respect de la vie privée. La Cour suprême du Canada a statué à plusieurs reprises que l'attente raisonnable de respect de la vie privée qui préside à la collecte d'une information par l'État à une fin particulière peut subsister lorsque cette information est utilisée à d'autres fins, notamment sa divulgation à des États étrangers.

● (0920)

L'adoption de quelque chose comme un critère de nécessité, modelé sur celui de l'arrêt Oakes, à l'article 1, ce que préconise le commissaire à la protection de la vie privée, ne suffira pas dans ce contexte. Pourquoi? Le critère des motifs raisonnables et probables établi à l'article 8, qui constitue la norme de base, n'est pas un critère que dit que l'État a accès à l'information si elle est nécessaire à une fin d'application de la loi; c'est un critère qui dit que l'objectif d'application de la loi prime seulement au point marqué par l'efficacité probable dans l'atteinte de cet objectif. Jusqu'à ce jour, cette idée d'efficacité probable ne fait pas partie de la jurisprudence relative à l'article 1.

En réalité, il n'est pas du tout clair quand une atteinte à l'article 7 ou à l'article 8 de la Charte peut être justifiée en vertu de l'article 1 de la Charte. Cela tient au fait qu'il y a un équilibre interne dans l'article 1, de même que dans l'article 7, et que les tribunaux sont réticents à les accepter en vertu de l'article 1. Nous ne devrions donc pas nous presser à régulariser une quelconque analyse fondée sur l'article 1 tant que nous n'aurons pas effectivement incorporé les protections de la vie privée découlant de la Charte, en particulier dans le contexte de l'utilisation par l'État de cette information à des fins d'application de la loi et de sécurité nationale.

Par conséquent, nous recommandons que l'utilisation ou la divulgation de renseignements personnels à des fins d'enquêtes en vue de l'application de la loi ou de sécurité nationale devrait être assujettie à un examen d'après la protection des droits personnels garantis aux articles 7 et 8 de la Charte et non être examinée simplement en fonction d'une norme de nécessité.

En troisième lieu, nous recommandons que le Commissariat à la protection de la vie privée soit habilité à effectuer un examen fondé sur la Charte des pratiques gouvernementales en matière d'information. L'examen fondé sur la Charte de ces pratiques en matière d'information ne devrait pas imposer aux Canadiens ordinaires le fardeau de découvrir les pratiques en matière d'information qui leur sont difficiles de constater et de comprendre — en venir à savoir ce qu'elles sont — et de les contester devant les tribunaux. Les particuliers ne devraient pas avoir le fardeau d'être les premiers à contester ces pratiques devant les tribunaux alors même qu'il y a une crise d'accès à la justice dans ce pays. Ce rôle devrait faire partie des fonctions du Commissariat à la protection de la vie privée.

Cependant, il importe aussi que cet examen judiciaire se fasse en fonction d'une norme du bien-fondé. Il ne devrait pas être incorporé dans un processus administratif de telle sorte que les tribunaux auraient à faire l'examen de plaintes relatives à la Charte en fonction d'une norme de raisonnabilité. Il faudrait que ce soit une norme du bien-fondé.

Nous recommandons en conséquence que les exceptions, en particulier celles prévues aux articles 7 et 8 de la Loi sur la protection des renseignements personnels, visant les utilisations et les divulgations de renseignements personnels sans consentement, fassent l'objet d'un examen fondé sur la Charte par le commissaire à la protection de la vie privée, sous réserve d'un contrôle judiciaire d'après une norme du bien-fondé.

Notre quatrième recommandation porte sur le renforcement de l'obligation d'exactitude sous le régime de la Loi sur la protection des renseignements personnels.

Une information inexacte peut avoir de graves conséquences pour les droits et libertés fondamentaux. C'est l'une des leçons tragiques de l'affaire Arar. À l'heure actuelle, l'obligation d'exactitude, énoncée au paragraphe 6(2) de la Loi, s'applique aux utilisations de renseignements personnels, mais elle devrait s'appliquer également aux divulgations, non seulement aux utilisations. Actuellement confinée à des fins administratives, elle devrait être élargie à toutes les fins auxquelles servent ces renseignements.

Je pense que la Loi devrait également être modernisée afin de tenir compte de ce que les universitaires désignent de plus en plus comme la « responsabilité algorithmique », c'est-à-dire l'idée que le problème ne tient pas seulement à l'exactitude de l'information recueillie, utilisée ou divulguée, mais aussi à l'exactitude des méthodes de traitement de l'information qui sont employées par le gouvernement.

À une époque de grandes banques de données, où d'énormes quantités d'information sont recueillies et analysées de différentes façons, nous devons nous préoccuper de l'exactitude de ces méthodes d'analyse. Nous devons nous soucier de ce que des biais, par exemple, ou d'autres formes d'inexactitude, puissent être introduites. Par conséquent, nous recommandons que le paragraphe 6(2) de la Loi soit modifié de manière à imposer l'obligation d'assurer l'exactitude de tous les renseignements personnels qui sont utilisés ou divulgués à toutes fins par les institutions. L'obligation d'exactitude devrait s'appliquer aussi aux méthodes de traitement de l'information.

Voilà qui met fin à mes observations.

Merci de votre attention.

● (0925)

Le président: Je suis certain que nous aurons une discussion de grande qualité.

Merci, madame Austin.

Nous passons maintenant à la ronde des interventions de sept minutes. Nous avons quatre intervenants, qui disposeront chacun de sept minutes. M. Erskine-Smith, est notre premier intervenant.

M. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Je vous remercie chaleureusement tous les trois.

Madame Austin, je voudrais parler d'abord de quelques-unes de vos recommandations portant sur l'inclusion d'un renvoi explicite à la Charte et sur la mention explicite d'un examen en fonction de la norme du bien-fondé.

D'après ce que j'en comprends, la Charte s'applique de toute façon et tous les examens s'y rapportant se font déjà sur la base de la norme du bien-fondé. Ce que vous proposez revient, au fond, à inscrire ce qui se fait déjà dans le texte même de la Loi sur la protection des renseignements personnels. La modification de fond, si j'ai bien compris votre mémoire, consisterait à charger le commissaire à la protection de la vie privée d'examiner le partage et l'utilisation de l'information pour en déterminer la conformité à la Charte. Tout le reste, c'est de la codification, plutôt qu'une modification de fond de la loi.

Mme Lisa Austin: La tendance en jurisprudence se caractérise actuellement par la grande déférence accordée par les tribunaux aux décideurs administratifs, tels que le Commissariat à la protection de la vie privée, y compris pour des questions relevant de la Charte. C'est une tendance que le David Asper Centre suit de près et qui le préoccupe. Il s'inquiète, lorsqu'il s'agit de questions relevant de la Charte, pour que le dernier mot sur une norme du bien-fondé demeure, dans les faits, aux tribunaux. Il vaut la peine de l'insérer.

Pour le reste, oui, il s'agit d'introduire dès l'étape initiale un examen fondé sur la Charte, parce que des questions touchant la Charte peuvent parfois surgir même s'il y a conformité à la Loi sur la protection des renseignements personnels. Il peut y avoir un partage d'information qui soit parfaitement conforme à la Loi sur la protection des renseignements personnels dans sa version actuelle, ou même à une version modifiée dans le sens recommandé par le commissaire à la protection de la vie privée, qui soulèverait néanmoins des problèmes en regard de la Charte.

Cet examen fondé sur la Charte ne devrait pas venir s'ajouter après le fait, ni être à la charge des citoyens. Il devrait être inclus dès le départ.

M. Nathaniel Erskine-Smith: J'adresse ma prochaine question à nos trois témoins.

Madame Austin, vous avez fait mention de la Loi sur la communication d'information ayant trait à la sécurité du Canada, qui autorise désormais 17 institutions gouvernementales à se communiquer de l'information entre elles, et cette autorisation peut être étendue par le Cabinet à d'autres particuliers, organismes et ministères. Comme nous envisageons de modifier la Loi sur la protection des renseignements personnels afin d'exiger, par exemple, des accords écrits de partage d'information, cette possibilité permettrait-elle de résoudre le problème entourant la Loi sur la communication d'information ayant trait à la sécurité du Canada? Si non, quelles autres modifications de fond devrions-nous apporter à la Loi sur la protection des renseignements personnels en particulier pour dissiper les inquiétudes des Canadiens quant au partage d'information excessivement large prévu en vertu du texte législatif auquel a abouti le projet de loi C-51?

Mme Lisa Austin: Je dirais que des accords écrits seraient un début. De nouveau, je voudrais que l'exigence de conformité à la Charte y soit intégrée, parce qu'une partie de cette information partagée pourrait soulever des problèmes en regard de la Charte et que ceux-ci doivent être relevés tôt dans le processus.

La jurisprudence sur les questions reliées à la Charte est claire: ce n'est pas parce qu'une institution gouvernementale possède de l'information qu'elle a recueillie à une fin qu'elle peut s'en servir par la suite à d'autres fins; il arrive qu'une question reliée à la Charte soit soulevée, et la conformité à la Charte est une exigence incontournable. Cela peut survenir également à l'occasion du partage d'information avec des pays étrangers.

L'article 8 a été appliqué dans l'arrêt Wakeling, quoiqu'il y ait eu désaccord quant au caractère raisonnable des dispositions pertinentes du Code criminel. En fin de compte, ils ont été jugés raisonnables.

Les accords écrits sont donc un début, mais il faut que le partage d'information fasse l'objet d'un examen fondé sur la Charte, parce que certains éléments d'information — pas tous, c'est à espérer — soulèveront des questions reliées à la Charte. C'est pourquoi il est nécessaire de prévoir cet examen au début du processus.

Je dirais également que dès qu'une partie de cette information est partagée, tout particulièrement avec des gouvernements étrangers, la question de son exactitude prend des proportions exceptionnelles. Il est donc important que l'obligation d'exactitude soit énoncée.

Je ne vois pas comment l'actuelle obligation d'exactitude s'applique dans la pratique, puisqu'elle concerne l'utilisation de l'information à des fins administratives. Si elle est communiquée à des fins de sécurité nationale ou d'application transnationale de la loi, il ne me semble pas que cette obligation entre en jeu, mais il est néanmoins impérieux que l'exactitude soit assurée. Il serait possible, par voie réglementaire, de préciser ce que cela peut signifier dans des circonstances particulières, mais je suis d'avis que c'est une modification d'une importance tout à fait cruciale.

M. Nathaniel Erskine-Smith: Les deux autres témoins auraient-ils des observations à faire?

Mme Teresa Scassa: Pour ce qui est des accords écrits — et je pense que le commissaire en fait état comme d'un formulaire prescrit —, c'est dans les détails que surviendront les difficultés. Cela dépendra dans une très large mesure de ce que sera le formulaire prescrit, de son niveau de détail et des exceptions qui seront admises. Je pense qu'il y a toujours le risque, notamment dans les domaines de l'application de la loi et de la sécurité nationale, de créer des exceptions ou des limitations étendues de ce qui pourra être divulgué.

De toute évidence, la tension tiendra, dans ce contexte, à l'équilibre entre le respect de la vie privée et la sécurité, mais je pense que l'efficacité des accords écrits dépendra vraiment de ce qui devra y être consigné, de leur degré de transparence réelle et de la mesure dans laquelle les exemptions en atténueront l'efficacité.

● (0930)

M. Nathaniel Erskine-Smith: Pensez-vous que les accords écrits figureront dans une annexe de la Loi, par exemple, pour servir de modèle ou différeront-ils individuellement selon les ministères concernés et le genre d'information qu'ils partageront?

Le président: Monsieur Lyon, auriez-vous quelque chose à ajouter? Je sais que M. Erskine-Smith a lancé la question à tous et j'ai eu l'impression que vous vouliez y répondre. Je veux m'assurer de vous en donner le choix ou l'occasion.

M. David Lyon: La seule chose que je voulais dire, c'est que je n'ai pas bien saisi la question. Le micro ne semblait pas bien capter la voix de M. Erskine-Smith.

M. Nathaniel Erskine-Smith: Ma question avait trait à la possibilité d'envisager un modèle établi dans une annexe de la Loi ou de différents genres d'accords entre les ministères. Devrions-nous avoir un formulaire type que les ministères pourraient modifier s'ils le souhaitaient, un formulaire type sur lequel ils pourraient se fonder?

M. David Lyon: D'accord. Oui, je pense que les observations de Lisa Austin répondaient directement à cette question et je crois bien que j'aurais répondu sensiblement comme elle.

Mme Lisa Austin: Le seul point concernant les accords écrits sur lequel je suis incertaine ou sur lequel je vous inviterais à réfléchir, est le suivant: quand on établit les pratiques de partage d'information, il ne s'agit pas, il me semble, de simplement rédiger un accord et de l'adopter; il faut prévoir certains outils techniques pour traiter les données, surtout dans les cas où il y a de grandes quantités de données qui seront partagées de différentes façons. Quels seront les mécanismes de surveillance du système technique qui sera mis en place?

L'exigence d'un accord écrit me paraît être un progrès par rapport à la situation actuelle. Sur ce point, je suis d'accord avec le mémoire du Commissariat à la protection de la vie privée, mais ne faudrait-il pas aussi un mécanisme de surveillance de l'infrastructure technique que nous créerons? Comment s'assurer également que les examens seront menés correctement et de manière transparente? C'est une question à laquelle il faut réfléchir.

M. Nathaniel Erskine-Smith: Je pense que mon temps est écoulé.

Madame Scassa, vous avez dit être, pour l'essentiel, en accord avec les recommandations du commissaire à la protection de la vie privée.

Quant aux points sur lesquels l'un ou l'autre d'entre vous sont en désaccord avec les recommandations, auriez-vous l'obligeance de les signaler aujourd'hui au Comité ou plus tard par écrit? Nous l'apprécierions grandement.

Le président: Je suis sûr que nous arriverons à relever les divergences.

Merci beaucoup, monsieur Erskine-Smith.

Monsieur Kelly, la parole est à vous pour sept minutes.

M. Pat Kelly (Calgary Rocky Ridge, PCC): Merci.

Je remercie les témoins de s'être déplacés pour la réunion aujourd'hui. L'information que vous nous avez donnée sera d'une très grande utilité.

J'adresse ma première question à M. Lyon. Je n'ai malheureusement pas eu l'occasion de lire votre livre. Pourriez-vous nous parler, ne serait-ce que de manière anecdotique, des différentes particularités de la façon dont s'exerce sur le terrain de la culture de surveillance, telle que vous l'avez décrite? Quelles sont les préoccupations ou les activités particulières qui contribuent à cette culture et comment se rapportent-elles à la Loi sur la protection des renseignements personnels?

M. David Lyon: C'est une excellente question. Je n'ai pas encore achevé la rédaction du livre, mais nous cherchons des façons de... Nous ne sommes plus dans la même situation que dans les années 1980 où l'on considérait encore ces questions comme étant relativement distinctes, en ce sens qu'elles ne s'appliquaient pas à tous. Dans ce que j'appelle une culture de la surveillance, les gens acquièrent en quelque sorte un imaginaire de la surveillance, une impression de ce qui se passe, et ils adoptent des pratiques en lien avec la surveillance, qu'il s'agisse d'éviter certaines formes de surveillance ou d'y participer activement, ou encore de se conformer aux règles, de recourir à la négociation et que sais-je encore.

Quand je parle de culture de la surveillance, j'essaie d'attirer l'attention sur le fait qu'il ne sert plus à rien de parler d'un État espion ou même d'une société de la surveillance, bien qu'il s'agisse de notions importantes. Nous devons réfléchir aux façons dont les gens, dans la vie de tous les jours, entre en contact avec différentes formes de surveillance, de nombreuses manières différentes et de plus en plus fréquemment.

Évidemment, je parle de la surveillance au sens large et j'englobe ici toute activité ou expérience de collecte et d'analyse de renseignements personnels, que ce soit pour influencer, pour contrôler, pour gérer, etc. Dans mon travail, j'adopte une définition plutôt large, la surveillance que les personnes qui ont rédigé la Loi sur la protection des renseignements personnels dans les années 1980 ne pouvaient pas envisager. Je pense notamment à des situations où des personnes sont présentes dans les médias sociaux tout en étant très au fait des risques qu'elles courent dans certains types de communications, dans leur navigation sur le Web, et ainsi de suite.

La culture de la surveillance qui se développe dans tant d'aspects de la vie courante influe sur la manière dont la surveillance est effectuée et dont la vie privée est préservée, et à cet égard, certains estiment que la vie privée revêt moins d'importance pour les jeunes personnes qui utilisent les médias sociaux. Il semble en fait que leur conception de la vie privée soit très complexe. Cela touche non seulement aux grandes questions relatives à la Charte, par exemple, mais aussi aux questions de moins grande portée, comme lorsqu'il est question de savoir quels intervenants peuvent avoir accès ou non à vos communications.

Je parle donc ici d'un phénomène qui s'installe au Canada et dans d'autres pays et qui influe sur notre conception de ce que signifie le fait de jouir de sa vie privée ou de faire l'objet d'une surveillance. Je parle de la manière dont cette conception et nos pratiques transforment la façon même dont fonctionne la surveillance — son efficacité — et aussi la vie privée.

● (0935)

M. Pat Kelly: Merci de votre réponse. Je vous en suis très reconnaissant. J'aimerais seulement profiter du temps qu'il me reste pour poser quelques questions aux autres témoins.

Madame Austin, juste pour que nous comprenions bien ce dont il est ici question, pourriez-vous me donner un exemple d'une activité précise qui est conforme à la loi, mais qui contrevient à la Charte? Vous avez parlé de la coupure entre la loi et la Charte. Pourriez-vous nous donner des exemples précis d'activités?

Mme Lisa Austin: En vertu de la loi, à des fins d'application, il est permis de divulguer sans consentement préalable des renseignements personnels à la demande d'un organisme énoncé dans les règlements. Si l'on peut raisonnablement présumer que la transmission de ces renseignements peut porter atteinte à la vie privée, on doit alors demander un mandat. Si l'on vous demande de fournir des renseignements personnels et que vous acquiescez à cette demande, cela ne pose pas de problème au regard de la Loi sur la protection des renseignements personnels. Cela dit, en vertu de la Charte, un mandat peut être exigé. Il est donc possible de se conformer à la loi tout en contrevenant à la Charte.

Il en va de même pour les gouvernements de pays étrangers. En vertu de la Loi sur la protection des renseignements personnels, il est possible de communiquer des renseignements à des gouvernements étrangers aux termes d'une entente qui n'a pas à être écrite. Cela ne contrevient pas à la loi, mais peut poser problème au regard de la Charte. Le jugement rendu par la Cour suprême du Canada dans l'affaire *Wakeling c. États-Unis d'Amérique* suggère que l'article 8 de la Charte est concerné quand des renseignements sont transmis à un État étranger. Il s'agissait, dans ce cas, de renseignements recueillis légalement conformément à la législation canadienne en matière d'écoute électronique.

Vous pouvez obtenir des renseignements que le gouvernement a en sa possession et met à la disposition d'un État étranger. Selon la Loi sur la protection des renseignements personnels, cet échange ne pose aucun problème s'il est effectué aux termes d'un accord et à des fins d'application de la loi. Toutefois, selon la Charte, et dans ces circonstances bien précises, il est possible que des mesures de protection additionnelles soient nécessaires. Il peut s'agir ou non d'un mandat; il peut s'agir de mesures de protection additionnelles relatives aux utilisations possibles de ces renseignements. La Cour suprême parle généralement de « garanties », mais cela ne figure actuellement pas dans la loi.

M. Pat Kelly: Madame Scassa, vous avez parlé de la collecte de données par des tiers. Je suppose que vous faisiez allusion aux renseignements recueillis à des fins commerciales par une entreprise privée ou à l'information qui est transmise par un particulier à un autre et qui, à la suite d'un second transfert, aboutit à un organisme gouvernemental.

Pourriez-vous me donner quelques exemples de la manière dont le gouvernement parvient à obtenir des données recueillies par des tiers?

● (0940)

Mme Teresa Scassa: Oui. Il y parvient essentiellement en vertu des dispositions relatives à l'échange de renseignements, dispositions contenues dans le Code criminel et dans la LPRPDE, la loi sur la protection des données du secteur privé, laquelle autorise la divulgation. Dans le Code criminel, la divulgation est autorisée à des fins d'application de la loi. Dans la LPRPDE, elle peut être autorisée à des fins d'application de la loi, à des fins d'enquête ou à des fins d'application de toute loi fédérale ou provinciale. Les possibilités de divulgation à des fins réglementaires sont donc nombreuses.

Ces renseignements peuvent être demandés par une entreprise privée et être fournis sur demande, si l'entreprise en question est disposée à les divulguer, ou faire l'objet d'une ordonnance de divulgation ordonnée par un tribunal. Dans les deux cas, les renseignements seront recueillis par le gouvernement, non pas auprès d'un particulier, mais auprès de l'entreprise privée. Il pourra s'agir de renseignements propres à un particulier, mais aussi — et ce fut le cas récemment dans certaines ordonnances de tribunaux — de données en vrac soumises à une analyse pour en dégager des tendances.

Le président: Merci beaucoup, monsieur Kelly. Vous avez légèrement dépassé le temps qui vous était alloué.

Monsieur Dubé, vous disposez de sept minutes. Allez-y.

[*Français*]

M. Matthew Dubé (Beloeil—Chambly, NPD): Merci, monsieur le président.

Je remercie les témoins d'être avec nous aujourd'hui.

Madame Austin, je crois que c'est vous qui avez parlé de l'importance des agences gouvernementales qui recueillent des données en vue de l'élaboration des programmes sociaux. Cependant, le problème ne porte pas seulement sur la collecte des données, mais aussi sur l'entretien des données collectées, si je peux m'exprimer ainsi. Pensons à des exemples récents, particulièrement celui de l'Agence du revenu du Canada qui a perdu ou laissé fuir, peu importe, des données personnelles.

Que devrait-on faire pour s'assurer non seulement que la collecte des données se fait de façon appropriée, mais aussi qu'on protège comme il se doit les données une fois qu'elles sont collectées?

Je pose cette même question aux autres témoins également.

[*Traduction*]

Mme Lisa Austin: Je crois qu'une des questions importantes à prendre en compte en ce qui a trait au stockage et à la protection des renseignements est le respect de la Charte.

Les jugements rendus récemment par la Cour suprême du Canada étaient très clairs en ce qui a trait à la nécessité de fournir des garanties en matière de renseignements. Par exemple, dans l'analyse du caractère raisonnable d'une loi au regard de la protection de la vie privée garantie par la Charte, nous discutons de plus en plus de la question des garanties et nous prenons conscience que, si nous ne garantissons pas adéquatement les renseignements, il peut y avoir violation de la Charte.

Cette question est cruciale, car il ne s'agit pas simplement d'un élément technique ou administratif de la Loi sur la protection des renseignements personnels. Le fait de ne pas garantir adéquatement les renseignements pose de graves problèmes au regard de la Charte, et les tribunaux commencent à y faire réellement attention.

Personnellement, je crois que nous n'avons pas suffisamment consolidé l'aspect technique du processus d'examen. Il semble que nous suivions encore sensiblement le même raisonnement dont parlait David Lyon. Nous voyons les renseignements personnels comme des données distinctes recueillies dans un environnement tout papier et échangées au moyen de classeurs, quand il s'agit en fait de systèmes d'information. Il est question de systèmes techniques, de logiciels, d'algorithmes. Toute la question des garanties revêt aussi une incroyable dimension technique. Il importe de respecter les normes juridiques, qu'il s'agisse de lois ou de règlements, et d'assurer une supervision adéquate, mais cela comporte aussi tout un côté technique. Je crois que nous ne développons pas suffisamment d'expertise technique dans le processus d'examen.

Pour ce qui est de savoir à quoi cela ressemble exactement dans les faits, je n'ai pas de réponse, malheureusement, mais je crois que nous devons vraiment comprendre la fluidité dont parle David Lyon. En pratique, nous parlons de systèmes logiciels. Nous parlons d'algorithmes. Il ne s'agit pas de numéros d'assurance sociale inscrits sur des documents papier stockés dans un classeur. C'est un milieu très technique.

M. Matthew Dubé: J'aimerais permettre à un autre témoin de s'exprimer sur la question, mais je tiens à poser ma prochaine question juste pour m'assurer qu'il y aura assez de temps pour y répondre.

Le fait de parler de toute cette composante numérique, des logiciels et des serveurs constitue un excellent tremplin. Nous avons parlé des États étrangers et de nos rapports avec eux. Cela concerne le PTP, par exemple.

L'un des principaux problèmes soulevés a trait à la localisation. En d'autres mots, si des Canadiens ont des données les concernant aux États-Unis, ils ont beaucoup moins de recours juridiques dans ce pays qu'au Canada, compte tenu de l'appareil de surveillance américain. Nous savons que les entreprises de Silicon Valley, par exemple, ne sont pas de grands amateurs de la localisation. Cette dernière empêche les médias sociaux et les initiatives du genre de croître d'une manière qui leur est bénéfique.

Que devons-nous faire dans la négociation d'accords comme celui-là, sachant que les données pourraient maintenant être aussi considérées comme des biens, et que nous devons en être conscients? Quand nous nous retrouvons avec un accord imparfait au regard de la vie privée au Canada, devrions-nous en tenir compte dans la loi?

● (0945)

Mme Lisa Austin: Je serais ravie de me prononcer sur les flux transfrontaliers des données.

Je ne crois pas que cela concerne la Loi sur la protection des renseignements personnels en soi, mais je pense que nous devrions réellement examiner la question d'un point de vue constitutionnel. Un Canadien résidant au Canada, mais dont les données se retrouvent aux États-Unis, sera considéré comme un étranger non résident — comme nous sommes au Canada, nous ne sommes pas résidents des États-Unis —, et le quatrième amendement à la Constitution américaine qui garantit la protection de la vie privée, ne s'appliquera pas du tout dans son cas.

Une grande partie de la jurisprudence canadienne confirme que les lois en vigueur dans le pays étranger avec qui on fait affaire s'appliquent dès qu'on traite dans ce pays. Si vous stockez vos renseignements aux États-Unis, vous les jetez pour ainsi dire dans un trou noir constitutionnel. Il n'y a pas de droit constitutionnel là-bas.

Que faire alors? La localisation des données est une solution. Je crois qu'il est irréaliste de penser que c'est une solution à long terme. Une autre solution, par contre, compte tenu de la taille du Canada et de l'envergure de notre économie, consisterait à négocier avec des pays alliés, comme les États-Unis, un accord bilatéral selon lequel, quand des données canadiennes se trouvent en sol américain, les États-Unis protègent les Canadiens dans la même mesure que leurs propres citoyens.

J'irais même plus loin en demandant à ces pays de protéger les Canadiens conformément aux normes de la Charte canadienne relatives à la vie privée, car celles-ci accordent plus de protection que les normes constitutionnelles américaines. Pourquoi? Parce que les Américains croient encore à ce qu'on appelle la « third-party doctrine ». Selon eux, quand on transmet des renseignements à un tiers, comme à un fournisseur de services de télécommunication, on ne peut raisonnablement pas s'attendre à ce que ces renseignements soient protégés aux États-Unis. Ces données font l'objet d'une renonciation.

Cette doctrine est insensée. Nous n'y avons jamais adhéré au Canada. La Cour suprême du Canada la dénonce depuis plus de 20 ans.

Il est crucial, à mon avis, de négocier avec les Américains et de leur dire: « Si vous souhaitez accéder à nos données à des fins d'application de la loi ou d'assurance de la sécurité nationale, c'est la Charte canadienne qui prévaut. » Cela ressemble à ce que le TEJ tente d'accomplir en faisant appliquer les droits constitutionnels du porteur de données, et nous devons trouver un moyen d'y parvenir. Je crois que c'est ce qui nous attend, mais je pense que nous devons négocier ce traité.

M. David Lyon: J'ajouterais que la question laisse sous-entendre l'existence d'une forme de transfert de données à des fins commerciales, d'application de la loi, etc. En réalité, il arrive fréquemment que des données traversent les États-Unis et circulent d'un emplacement à un autre au Canada. Le Système d'acheminement peut envoyer des données aux États-Unis et les retourner au Canada. L'acheminement peut même être effectué entre deux endroits au sein d'une même ville, mais non sans un détour par les États-Unis. Dans ces cas-là, il est possible que les renseignements d'un particulier soient assujettis à la loi américaine et que ce particulier ne bénéficie d'aucune protection. Cela peut se produire occasionnellement lorsque des renseignements sont acheminés aux États-Unis.

Le président: Voilà qui est très intéressant.

Votre temps est écoulé, monsieur Dubé.

Monsieur Lightbound, la parole est à vous.

M. Joël Lightbound (Louis-Hébert, Lib.): Je vous remercie tous d'être ici aujourd'hui. Vos propos sont très intéressants, et je vous en suis reconnaissant.

Ma première question a trait à l'exigence de nécessité énoncée dans l'article 4 de la loi qui stipule qu'une institution peut recueillir des renseignements personnels s'ils ont un lien direct avec ses programmes ou activités.

Quand on entend dire que le gouvernement a fouiné dans les profils des Canadiens sur les médias sociaux et que les données contenues dans des millions de dossiers ont été exploitées, comment, à votre avis, pourrait-on restreindre cette exigence de nécessité? Avez-vous des suggestions à nous faire en ce sens? La proposition de M. Therrien semble assez large. Pourriez-vous nous donner des exemples dont nous pourrions nous inspirer, sur la scène internationale, alors que nous examinons la Loi sur la protection des renseignements personnels.

J'inviterais d'abord Mme Austin à répondre à la question.

● (0950)

Mme Lisa Austin: C'est une excellente question. En ce qui concerne l'exigence de nécessité, je comprends qu'on ait mentionné le cadre de l'article 1. C'est un type bien connu de cadre juridique d'analyse de la proportionnalité. En droit international humanitaire, il y a aussi un critère équivalent nécessaire, et il vaudrait vraiment la peine que nous l'examinions.

Ma seule hésitation au regard de l'exigence de nécessité a trait au fait que le critère prévu à l'article 1, si on l'interprète sous l'angle de la jurisprudence actuelle, a été largement créé dans un contexte de réglementation sociale. Les tribunaux visent réellement le critère d'atteinte minimale. Ils ne se concentrent pas sur l'équilibre plus large que vous trouveriez, par exemple, dans des cas conventionnels relatifs à la vie privée soulevés en vertu de l'article 8 de la Charte. Dans les cas de perquisition et de saisie, l'« attente raisonnable en matière de vie privée » est vue comme une forme de mise en équilibre. Cette disposition trouve un équilibre entre la vie privée et les intérêts de l'État. Encore une fois, le critère des « motifs raisonnables et probables » n'est pas un critère d'atteinte minimale; ce genre de mise en équilibre offre une meilleure protection de la vie privée.

Ma seule hésitation ne concerne pas... Je crois que le critère de nécessité et le cadre de l'article 1 constituent une amélioration par rapport aux dispositions actuelles de la Loi sur la protection des renseignements personnels, mais je crains que cela ne devienne un sceau d'approbation pour la collecte, l'utilisation et la divulgation des données, particulièrement quand on parle d'application de la loi ou de sécurité nationale, car il y a une vision plus robuste de la proportionnalité, je pense, dans les articles 7 et 8 de la Charte, qui n'est pas exprimée dans la loi. C'est comme si vous en veniez immédiatement à une justification au titre de l'article 1 sans avoir fait d'analyse plus approfondie au préalable. Je crois que cela pose problème dans de tels contextes.

Mme Teresa Scassa: Le problème que pose directement la norme actuelle est qu'elle est trop souple et qu'elle peut être interprétée de nombreuses façons. Établir une norme de nécessité vise à affirmer plus fermement la notion de réduction des données, qui est un important principe de protection des données, puisqu'il sous-entend une réduction de la quantité de renseignements recueillis en premier lieu. La question est réellement de savoir si ces renseignements sont nécessaires au programme ou au service concerné. Si ce n'est pas le cas, alors les renseignements en question ne devraient pas être recueillis.

Évidemment, quel que soit le mot choisi, il y aura du jeu, il y aura matière à interprétation et matière à débat: « Eh bien, c'est en fait nécessaire, car ce que nous faisons nécessite... » Je crois que c'est une partie du problème dans la sphère des mégadonnées: nous commençons à dire que ce que nous essayons de faire est de recueillir suffisamment de renseignements afin que nous puissions effectuer ces autres tâches d'analyse et de profilage, ce qui nous permettra de mener ces autres activités, et par conséquent, cela devient nécessaire.

Selon moi, il y a des risques quel que soit le vocabulaire employé. L'objectif ici est de réduire au minimum la collecte de données. En combinaison avec les autres mesures recommandées, comme les études d'impact sur la vie privée, entre autres, cela pourrait offrir des moyens d'imposer plus de supervision.

M. Joël Lightbound: Je veux maintenant aborder un autre sujet. Madame Austin, vous avez mentionné, avec justesse d'ailleurs, les risques que pose l'échange d'informations, surtout quand on songe à la saga Maher Arar. Le projet de loi C-51 précise que l'échange d'informations doit être effectué conformément aux lois en vigueur au Canada. L'article 8 de la Loi sur la protection des renseignements personnels prévoie une interdiction générale de l'échange d'informations, laquelle est modérée par de nombreuses exceptions notamment énoncées au paragraphe 8(2). Par exemple, l'alinéa 8(2)b) stipule qu'il peut y avoir échange d'informations si cet échange est effectué conformément à une autre loi ou mesure législative, ce qui constitue pour ainsi dire une impasse.

J'aimerais connaître vos impressions au regard de l'article 8 et savoir si vous avez une idée de la manière dont nous pourrions restreindre plus encore l'échange d'informations dans le cadre de la Loi sur la protection des renseignements personnels.

Mme Lisa Austin: L'un des gros problèmes serait de penser que le projet de loi C-51 permettra de protéger la vie privée parce que la Loi sur la protection des renseignements personnels s'applique. La disposition autorisant un large partage de l'information en vertu de la Loi sur la communication d'information ayant trait à la sécurité du Canada reprend en grande partie celles de l'article 8. Je n'ai pas la loi sous les yeux, mais toute analyse doit partir de l'idée que conformité avec l'article 8 ne signifie pas conformité avec la Charte. De nombreuses modalités de partage de l'information pourraient être compatibles avec les dispositions en matière de divulgation ou d'utilisation énoncées à l'article 7 ou à l'article 8 de la Loi sur la protection des renseignements personnels, dans sa rédaction actuelle, sans être pour autant conformes à la Charte.

Je ne sais pas trop, pour ce qui est de la rédaction du texte législatif, si vous voulez modifier ces dispositions ou seulement signaler que, dans certains cas, cela risque de poser un problème de compatibilité avec la Charte, parce que ça ne sera pas nécessairement toujours le cas. La Loi sur la protection des renseignements personnels réglemente la collecte, l'utilisation et la divulgation des informations personnelles. Elle ne répond pas nécessairement dans chacun de ses détails aux exigences constitutionnelles en matière de protection de la vie privée. C'est le hic. Lorsqu'il est question de partage d'information, en particulier dans les cas où l'individu est soumis à l'autorité de l'État, un soin méticuleux doit être apporté aux aspects relatifs à la Charte. Comment intégrer cela au texte?

C'est pourquoi nous avons dit qu'il faut un principe d'interprétation pour préciser ce qui est compatible avec la Charte et insérer dans le texte une disposition d'examen de la Charte. Il faut peut-être préciser à l'article 8 que la compatibilité avec la Charte doit également être assurée. Il faut un mécanisme permettant à des spécialistes en matière de jurisprudence de trancher les questions relatives à l'utilisation et la divulgation de l'information. Que se passe-t-il, lorsque des mesures contreviennent aux dispositions de la Charte? Est-il nécessaire d'obtenir une autorisation préalable? Y a-t-il une question de garantie qui se pose? En quoi consistent ces garanties? Il faut concevoir des processus en matière de renseignements personnels qui soient d'emblée conformes à la Charte pour éviter que quelqu'un ne se rende compte 10 ans plus tard que le processus n'est pas conforme et soit traduit en justice. La conformité à la Charte doit être assurée au stade de la conception.

● (0955)

M. Joël Lightbound: Puisque le président ne m'interrompt pas...

Le président: Si vous avez une question complémentaire rapidement...

M. Joël Lightbound: Non, c'est sur un autre sujet.

Le président: Pouvons-nous attendre le tour suivant?

M. Joël Lightbound: Oui, bien sûr.

Le président: Cela conclut notre tour de parole de sept minutes.

Nous passons à M. Strahl, je vous en prie, monsieur, vous avez cinq minutes.

M. Mark Strahl (Chilliwack—Hope, PCC): Merci, monsieur le président et merci aux témoins.

Sujet fascinant et fascinante époque. Monsieur Lyon, les gens sont de plus en plus préoccupés par la protection de leur vie privée et en même temps ils révèlent volontairement de plus en plus de choses sur leur propre compte, en ligne, sur des médias de moins en moins sûrs. Et malgré tout, vous dites qu'ils sont informés de leurs droits et s'attendent que l'on respecte leur vie privée.

Je voudrais parler plus précisément d'une des recommandations du commissaire à la protection de la vie privée. Elle concerne l'obligation légale de déclarer les atteintes graves à la vie privée dans le cadre de la Loi sur la protection des renseignements personnels.

Monsieur Lyon, pensez-vous que c'est une bonne recommandation et pensez-vous qu'elle puisse être appliquée dans le cadre de la Loi sur la protection des renseignements personnels?

M. David Lyon: Il est difficile de répondre à la deuxième partie concernant la possibilité de faire respecter la loi. Pour ce qui est de la déclaration des infractions, il me semble essentiel que le public sache ce qui se passe et quand se produisent des atteintes à la vie privée.

Il en est fait état dans certaines circonstances, mais elles peuvent également être tenues sous le boisseau. Elles peuvent être dissimulées de sorte qu'on n'en sache jamais rien. Il me semble essentiel qu'on en soit informé, qu'elles soient rendues publiques et que la loi rende leur déclaration obligatoire.

Quant à la façon de s'y prendre, comme je l'ai dit, je m'en remets aux autres.

M. Mark Strahl: En parlant des autres, monsieur Austin ou madame Scassa, êtes-vous d'accord avec cette recommandation et selon quelles modalités, et dans quels délais, ces infractions devraient être déclarées?

Mme Teresa Scassa: Pour ma part, la procédure de déclaration devrait comporter deux étapes, un peu comme ce qui se fait avec la LPRPDE.

Avec l'entrée en vigueur des amendements à la LPRPDE, il y aura un premier niveau de déclaration en fonction du préjudice causé, assorti de l'obligation de notifier à la fois le commissaire à la protection de la vie privée et les individus exposés au préjudice. C'est le premier niveau et il est très important, parce qu'il ne s'agit pas simplement de déclarer l'infraction, mais également d'essayer d'atténuer le préjudice et de notifier les individus qui peuvent être affectés.

La deuxième étape prévue par la LPRPDE, et que je trouve assez intéressante, c'est l'obligation pour l'organisation de faire rapport sur les infractions, quel que soit le préjudice potentiel, autrement dit, sur toutes les infractions quand bien même en fin de compte l'information ne tombe pas dans de mauvaises mains. Je pense que les registres d'infraction et les rapports au commissaire à la vie privée ne doivent pas nécessairement être mis à la disposition du public — la décision reste à prendre — et pourraient faire simplement l'objet d'un rapport au commissaire à la vie privée.

Cela est important, je pense, parce que ça amène à autre chose, à savoir l'identification des pratiques de sécurité présentant des faiblesses et devant être améliorées de l'intérieur. Si le commissaire à la vie privée a accès à cette information, il a la possibilité de déterminer s'il s'agit d'un problème commun à tout le gouvernement et auquel il faut s'intéresser ou s'il ne concerne qu'un département particulier qui n'a pas suffisamment bien formé son personnel à certaines mesures de protection de la vie privée. Cela rend possible une démarche plus proactive visant à s'attaquer aux problèmes de sécurité mis en évidence à ce niveau de la procédure de présentation des rapports.

Je suis partisan d'un tel mécanisme à deux niveaux où le préjudice n'est pas le seul élément qui déclenche la notification, la présentation de rapports étant rendue obligatoire sitôt qu'il y a infraction afin de pouvoir diagnostiquer le problème et s'y attaquer avant qu'il n'empire.

● (1000)

M. Mark Strahl: Merci beaucoup.

Le commissaire à la vie privée a également signalé que le modèle à suivre pour moderniser la Loi fédérale sur la protection des renseignements personnels est celui de Terre-Neuve-et-Labrador. Êtes-vous d'accord avec lui et, si oui, pourquoi? Pensez-vous qu'il existe de meilleurs modèles, au Canada ou dans le monde, que l'on puisse adopter pour améliorer notre loi?

Je commencerai peut-être avec Mme Austin.

Mme Lisa Austin: J'ai cru comprendre que la recommandation concernait avant tout la question des pouvoirs d'exécution. Le modèle de Terre-Neuve était un modèle hybride, lequel semblait présenter de nombreux avantages par rapport au modèle reposant sur le pouvoir de rendre des ordonnances.

Je n'ai pas d'idée bien arrêtée sur cette question spécifique, mais je penche fortement du côté du pouvoir de rendre des ordonnances. Je vous invite, dans votre réflexion, à vous placer du point de vue du titulaire de droits individuels qui garantissent sa vie privée et à vous demander lequel de ces deux modèles vaut mieux pour lui, celui qui le pousse à saisir les tribunaux pour faire valoir ses droits, ou celui qui suit l'autre approche. Nous faisons face à une crise en matière d'accès à la justice ici et contraindre les individus à faire appel aux tribunaux alors qu'ils sont censés jouir de droits solides, me semble peu réaliste. Par le passé, les recommandations favorisant le recours aux tribunaux ne prenaient pas ce facteur en compte. C'est un premier point.

L'autre, c'est que le débat semble faire une large part aux gesticulations et aux détails anecdotiques. Au Canada nous avons différentes juridictions qui ont chacune leur façon de faire. L'Ontario privilégie le pouvoir de rendre des ordonnances. La Colombie-Britannique aussi. Si l'on se demande dans quelle mesure cela infléchit la dynamique au détriment du modèle reposant sur un ombudsman en encourageant le recours plus systématique aux tribunaux contre le gouvernement, il n'est sans doute pas difficile de s'informer auprès des différentes juridictions. L'enquête consisterait davantage à documenter les faits. On peut examiner ce qui se passe dans ces juridictions et trouver la réponse.

La seule autre chose que je voudrais ajouter, c'est que dans ces contextes faisant intervenir la Charte, qui me préoccupent beaucoup, il est bon d'avoir un gros bâton, parce que l'individu est dans un rapport conflictuel avec l'État, alors que dans un contexte davantage administratif, où l'État administre un programme social, la tension conflictuelle est moindre. Elle existe, mais le conflit n'est pas aussi radical.

Dans cette perspective, le modèle axé sur le pouvoir de rendre des ordonnances me semble plus avantageux, mais mon point de vue n'est pas arrêté.

Le président: Voilà une réponse très longue. Elle a fait d'un tour de parole de cinq minutes, un tour de sept minutes.

Nous en venons à M. Saini, je vous en prie, j'essaierai d'être aussi généreux envers vous.

M. Raj Saini (Kitchener-Centre, Lib.): Bonjour. Merci d'être venus.

Une question plus générale d'abord, puis une plus spécifique.

Ma première question d'ordre général, c'est que, comme vous le savez, le gouvernement met en place, dans 17 départements, un système informatique qui s'appelle GCDocs. Si un département collecte de l'information dont il a besoin, comment empêcher que les autres départements aient accès à cette information sur des Canadiens lorsque 17 ministères auront la possibilité de la consulter en ligne? Auriez-vous une recommandation à faire?

Mme Teresa Scassa: Je n'en sais pas suffisamment sur le système en ce qui concerne les méthodes d'accès prévues, mais les moyens techniques existent, même dans une grande base de données partagées, de créer différents niveaux d'accès pour différentes personnes ou parties qui ont accès à cette base de données. Je ne sais pas si l'une des mesures envisagées est précisément de créer ces différents niveaux d'accès pour gérer l'accès à la base de données.

● (1005)

Mme Lisa Austin: Je reviendrai sur certaines de mes remarques antérieures: on ne peut penser à protéger la vie privée simplement en ayant en vue les processus administratifs de partage de l'information; il faut également examiner les systèmes techniques que l'on met en place. C'est à ce niveau qu'il faut y réfléchir pour savoir comment concevoir ces systèmes et les munir des garanties que la loi vous impose de fournir. Il est difficile de les greffer sur le système après coup. C'est possible, mais en général ça coûte cher et c'est difficile.

Il faut y réfléchir d'emblée. Lorsqu'on élabore des processus, il faut avoir présent à l'esprit les exigences en matière de protection de la vie privée. La mise en conformité avec la Charte doit être votre premier souci et vous en tenez compte dans la mise au point de votre appareil technique.

M. Raj Saini: Ma seconde question concerne la sécurité nationale.

Comme vous le savez, le Canada est membre de nombreuses alliances dans le monde, que ce soit celle du Groupe des cinq ou celle concernant le partage de renseignements avec nos partenaires européens. Je me demande si vous pourriez me donner une idée, parce que je ne suis pas sûr de bien comprendre comment cela fonctionne.

Un gouvernement étranger peut vous adresser deux types de demandes. Une demande immédiate en présence d'un événement particulier dans un pays étranger qui a besoin de renseignements sur un Canadien, ou une demande à long terme de renseignements à propos d'un Canadien donné, qui n'est mêlé à rien de spécial dans l'immédiat mais qui pourrait l'être à l'avenir. Comment analysez-vous cette demande? Et surtout, comment protège-t-on cette information? Une fois qu'elle a franchi la frontière, elle est consignée dans un dossier d'un gouvernement étranger.

Nous avons notre Loi sur la protection des renseignements personnels et jouissons de certaines garanties. Comment nous assurer que ces mêmes garanties seront maintenues dans un pays étranger, ou que l'information ne sera pas partagée avec d'autres ministères de ce pays ou envoyée vers un pays tiers?

Mme Lisa Austin: C'est une grande question. Je voudrais souligner le besoin de garanties, c'est une question qui est soulevée dans la jurisprudence entourant la Charte. C'est pourquoi nous sommes partisans d'une obligation plus stricte de précision dans la Loi sur la protection des renseignements personnels, en vue d'imposer ces garanties.

Je pense que dans ces alliances et ces contextes internationaux, chaque pays doit chercher à protéger ses propres citoyens au moyen de traités garantissant les mêmes droits aux citoyens de tous les pays signataires. Des mécanismes de vérification sont également prévus qui permettent aux individus d'examiner les pratiques en matière d'information. Je ne pense pas qu'une loi sur la protection des renseignements personnels puisse résoudre ces problèmes.

M. Raj Saini: Il faudrait une espèce de traité supranational parce que le problème, c'est que chaque pays a un régime différent. On peut faire une demande en vertu de notre régime, mais un autre pays peut avoir un régime offrant de meilleures garanties. Il faudrait créer un cadre auquel chaque pays adhérerait. C'est ce que vous suggérez?

Mme Lisa Austin: Ce pourrait être la réponse. Il se pourrait, du moins entre alliés, qu'il faille créer une sorte de régime international pour cela. Je sais que l'on s'intéresse beaucoup aux modalités de fonctionnement du Traité d'entraide juridique en matière pénale dans un monde en mutation.

Il y a différents modèles. Je ne sais pas lequel est le bon, mais, d'après moi, c'est une espèce d'accord international, ou du moins un régime supranational. Dans le cadre de la réforme de la Loi sur la protection des renseignements personnels, on peut faire des retouches pour reformuler ces obligations et définir un accord, mais il faut quelque chose de plus robuste que cela.

M. Raj Saini: Monsieur le président, ai-je encore un peu de temps?

Le président: Je serai obligeant. Allez-y, je vous en prie.

M. Raj Saini: Permettez-moi de poser cette question à M. Lyon qui est là à attendre patiemment et je souhaite l'associer à la conversation.

Vous avez parlé de surveillance. Si un pays étranger nous demande des informations, nous demande de surveiller l'un de nos citoyens, comment cela fonctionne-t-il? Pouvez-vous nous donner des précisions sur ce processus, sur ce que l'on doit permettre et ce que l'on doit empêcher? Comment faut-il protéger les droits des citoyens canadiens tout en restant partenaire d'un pays étranger, et nous assurer que les règles de diffusion de cette information sont respectées.

M. David Lyon: Est-ce que vous pensez à un régime de sécurité ou d'application de la loi au niveau national? C'est ce que vous avez en tête?

M. Raj Saini: Non.

Disons qu'un pays étranger nous demande de surveiller l'un de nos citoyens, pour une raison ou une autre, qu'il s'agisse d'une question de sécurité nationale ou d'autre chose. Comment répondre à cette demande? Quels sont nos paramètres?

Je sais que Mme Austin a parlé du processus de délivrance de mandat, mais comment fait-on, surtout s'il s'agit d'une demande exigeant une réponse immédiate?

● (1010)

M. David Lyon: C'est un domaine dont je ne m'occupe pas spécialement, mais il semblerait nécessaire d'assurer une supervision plus étroite des agences concernées par la réception et le partage de ces informations. Il me semble que c'est là une question critique.

Je ne sais pas comment fonctionnerait un tel mécanisme. Mais il me semble que l'on a besoin d'une supervision plus étroite de ces agences chargées de l'application de la loi et des questions de sécurité, parce que c'est là que se posent les questions et que les choses s'embrouillent considérablement.

Le président: Merci, Raj. Nous apprécions vivement.

Nous passons maintenant à M. Kelly pour cinq minutes, je vous en prie.

M. Pat Kelly: Merci.

Professeur Lyon, vous avez parlé plus tôt d'un manque de compréhension des problèmes relatifs à la protection des renseignements personnels et des modalités de leur résolution, si j'ai bien interprété vos remarques. Nous ne serions pas prêts, selon vous, pour une refonte totale de la loi et une étude approfondie de ces problèmes reste encore à faire. Vous préconisez même, me semble-t-il, quelque chose comme la création d'une commission royale ou une étude à grande échelle.

Pourriez-vous nous dire quelles sont ces choses que nous ne connaissons pas? Quelles sont, selon vous, les recherches qui s'imposent et dans quel domaine, avant de reformuler la loi?

M. David Lyon: Nous avons déjà parlé de certaines de ces choses.

On pourrait, dans un sens, dire qu'il s'agit de changements technologiques et des nouvelles méthodes de recherche de l'information sur les individus à diverses fins. J'ai également fait allusion à l'usage croissant des données biométriques, à l'emploi des capteurs dans les bâtiments, les rues, les véhicules, etc. Il s'agit en grande partie de prendre en compte les changements technologiques déjà en cours. Cela me semble crucial.

Par ailleurs, j'ai voulu mettre l'accent sur l'évolution de la notion même de vie privée depuis les années 1980, à l'époque où la loi a été conçue. Nous devons garder cela présent à l'esprit également. Cela me semble essentiel. Et cela s'inscrit dans le droit fil de ce que dit Lisa Austin sur la nécessité de se conformer à la Charte.

La notion de vie privée et renseignements personnels était conçue de façon très atomistique et individuelle, me semble-t-il autrefois, et était étroitement associée à des préjudices déterminés. Dans la situation d'aujourd'hui, il nous faut songer à un ensemble beaucoup plus vaste de questions touchant à la participation démocratique et aux droits de la personne, de sorte que la notion même de vie privée doit être comprise dans un sens plus large.

C'est les deux choses: la capacité de prendre en compte les changements technologiques réels — et là encore la question des grosses bases de données revêt une importance majeure — d'une part, et la compréhension de la notion de vie privée qui s'est métamorphosée avec ses nouvelles dimensions sociale et participative, par rapport à ce qu'elle était dans la loi originelle.

M. Pat Kelly: Je vous remercie.

Dans une veine complètement différente, Mme Austin pourrait peut-être répondre à cette question.

Quelles seraient les implications de l'élargissement des motifs de recours devant la Cour prévus à l'article 41 de la loi que le commissaire a recommandés? La mise en oeuvre de cette recommandation se traduira-t-elle par une augmentation ou une diminution des dépenses des tribunaux liées aux besoins en personnel? Quel effet aurait-elle sur le montant des dépenses du Trésor au titre de la responsabilité civile et des dédommagements? Quel serait l'effet net de cette recommandation?

Mme Lisa Austin: Vous voulez un bilan chiffré. Vous ne devriez jamais poser ce genre de questions à des universitaires.

M. Pat Kelly: Je pourrais l'avoir fait exprès.

Mme Lisa Austin: L'augmentation des voies de recours judiciaires vise à compenser l'un des gros défauts de la Loi sur la protection des renseignements personnels que le commissaire souligne, à savoir l'impossibilité de saisir les tribunaux en cas de différend sur les dispositions touchant la collecte, l'utilisation et la divulgation. Il n'y a pas de recours en la matière bien qu'elles soient vitales pour la protection de l'information dans les contextes les plus divers, administration, sécurité nationale ou application de la loi.

Il est absolument vital d'avoir quelque chose en place. Est-ce que ça va coûter plus cher? Probablement, mais je dirais, encore une fois, que la possibilité de recours constitue un aspect important de la protection des droits de la vie privée. Sans cela, la Loi sur la protection des renseignements personnels ne pourra donner les résultats que l'on en attend.

● (1015)

M. Pat Kelly: Je ne suggère pas que le coût soit un motif pour ne pas le faire. Je voulais simplement une idée...

Mme Lisa Austin: ... de quels seraient ces coûts. Désolé, je ne saurais le dire.

Le président: Monsieur Long, vous avez jusqu'à cinq minutes, allez-y.

M. Wayne Long (Saint John—Rothesay, Lib.): Merci, monsieur le président.

Merci à nos témoins invités ce matin.

Je veux commencer par Mme Scassa. Vous avez participé, évidemment, dans la décision de la Cour suprême de l'Ontario. Je pense que c'était en janvier.

Mme Teresa Scassa: Voulez-vous dire celle liée au « tower dump »?

M. Wayne Long: Exactement.

Mme Teresa Scassa: Eh bien, j'ai écrit un commentaire sur ce sujet.

M. Wayne Long: Je vais le lire dans une seconde.

Je dirai ceci à l'intention du Comité. Je pense qu'il y a toujours un équilibre — et nous en avons parlé des mois durant — entre la liberté et la sécurité. La liberté a un coût, mais on ne doit jamais y renoncer pour la sécurité, sauf en toute dernière extrémité.

J'ai lu hier un article qui vous cite et dit en gros que le juge précise clairement que l'information recherchée par la police doit se limiter aux fins de l'enquête. La police ne peut se lancer dans une partie de pêche.

Compte tenu de l'équilibre qu'il convient évidemment de respecter entre ce que la police a besoin de savoir et la vie privée d'une personne, pourriez-vous élaborer sur le cas en question et ses dessous?

Mme Teresa Scassa: Il s'agit d'une affaire intéressante. Les tribunaux ont été saisis dans le cadre d'un recours en vertu de la Charte intenté par les sociétés de télécommunications concernées, pas par les accusés cherchant à défendre leurs droits.

À la base, les policiers enquêtaient sur le cambriolage d'une bijouterie. Ils étaient à la recherche de suspects. Soupçonnant qu'un téléphone portable avait été utilisé lors du crime, ils ont demandé des mandats pour avoir accès au « tower dump », qui est une sorte de cliché des données des antennes téléphoniques à proximité. Rogers et Telus ont dit qu'à elles deux cela signifierait la remise des données de 43 000 personnes qui avaient utilisé leur téléphone dans le créneau horaire précisé par la police, qui demandait en outre quantité d'autres informations.

M. Wayne Long: Pour un novice comme moi, quand vous dites un cliché des données, ça revient à dire chaque bit d'information transitant par les téléphones des gens, que l'antenne a capté?

Mme Teresa Scassa: Eh bien, c'était plus que ça. La police voulait connaître chaque transmission de téléphone portable relayée par l'antenne. En outre, elle voulait que les deux compagnies fournissent les informations d'abonnement liées à ces numéros de téléphone, les informations de paiement et de carte de crédit et l'identité des destinataires des appels passés dans cette partie de la ville par ces 43 000 personnes.

Devant la résistance de Rogers et Telus, la police a restreint la portée du mandat recherché, disant « On oublie ça. Voilà tout ce qu'on veut. Mais pas de procès, s'il vous plaît. » Elle a même cherché à faire annuler le procès au motif qu'elle avait restreint la portée du mandat demandé et qu'il n'y avait plus lieu par conséquent d'invoquer la Charte. La Cour cependant a décidé d'entendre l'affaire.

Sa décision est très robuste. Elle dit en gros que les juges appelés à délivrer ces mandats ont besoin de nouvelles lignes directrices. La police doit soigneusement circonscrire l'information recherchée. On ne peut l'autoriser à partir à la pêche. L'information recherchée allait bien au-delà de ce qui était nécessaire. Une nouvelle approche s'impose.

Dans sa conclusion, le juge disait aussi, en réponse à une question soulevée par Telus et Rogers, que ni le Code criminel ni la LPRPDE ni aucune autre loi ne dit ce qu'il convient de faire de cette information, une fois le mandat délivré et l'information remise à la police. Est-elle gardée pour toujours? Est-elle utilisée à d'autres fins? Est-elle juste stockée dans une base de données quelque part, où il pourrait y avoir une fuite de données concernant les informations de carte de crédit et d'autres données?

Le juge a dit que la décision ne relève pas de lui. C'est au Parlement de se prononcer. La Cour n'est pas habilitée à créer des lignes directrices en la matière.

La question se pose dans les cas où la police entend recueillir de gros volumes d'information. Qu'en advient-il? Quelle est la marche à suivre pour en disposer lorsque le motif pour lequel elle a été collectée a cessé d'exister?

M. Wayne Long: Madame Austin, monsieur Lyon ou madame Scassa, vous pouvez tous faire vos commentaires sur ce point si vous le souhaitez.

Le commissaire Therrien a récemment critiqué les appels du commissaire de la GRC Bob Paulson et de l'Association canadienne des chefs de police en faveur, essentiellement, d'une nouvelle loi qui élargirait le droit pour la police d'accéder à l'information sans mandat.

Monsieur Lyon, pouvez-vous me dire ce que vous en pensez?

● (1020)

M. David Lyon: Cela fait des années que le mandat est exigé, et cette exigence a semblé indispensable pour préserver l'intégrité de la vie privée des personnes.

Il me semble que l'accès sans mandat aux renseignements personnels des gens aux fins de l'application de la loi ou à toute autre fin est tout simplement inacceptable. C'est quelque chose qui doit être inscrit dans notre système juridique. Nous avons besoin de savoir qu'il existe un mandat clair pour chaque demande d'accès aux renseignements personnels.

Le président: Cela nous amène aux cinq minutes.

Nous allons avoir un peu de temps à la fin de la réunion, si quelqu'un a encore une question. Je sais que M. Lightbound avait encore une question.

Pour finir, nous avons M. Dubé pendant trois minutes.

[*Français*]

M. Matthew Dubé: Merci, monsieur le président.

J'aimerais revenir sur la façon de punir les délinquants. Je regarde les recommandations et, à moins que je ne me trompe, je n'en vois qu'une seule qui traite réellement du genre de conséquences possibles dans un cas d'atteinte à la vie privée, soit celle-ci: « Accroître les motifs de recours devant la cour prévus à l'article 41 de la *Loi* ».

Également, on parle beaucoup de transparence. C'est essentiel, je ne dis pas le contraire. Il est question de rendre obligatoire la déclaration des atteintes à la vie privée et d'éduquer le public. Tous ces points sont essentiels, je ne prétends pas le contraire.

Selon vous, quelles conséquences doit-on imposer aux délinquants, si je peux m'exprimer ainsi? On parle des compagnies de télécommunications, voire du gouvernement à certains moments ou des corps policiers. En fait, les citoyens peuvent être bien outillés et bien informés, mais si ces gens ne risquent pas vraiment de subir des conséquences, la loi manque un peu de mordant.

[*Traduction*]

Mme Teresa Scassa: Le défi est complexe. En ce moment, il y a des recours collectifs déjà en cours contre le gouvernement fédéral pour négligence dans le traitement des renseignements personnels, pour infractions aux règles de confidentialité. Les recours civils et recours collectifs se feront plus fréquents, c'est un moyen pour les gens de faire reconnaître leurs droits.

Le professeur Austin a parlé de recours en vertu de la Charte, et ils existent. Dans certains cas, le recours peut être exercé par les personnes concernées. Nous venons de parler d'une affaire dans laquelle il a été intenté par les sociétés de télécommunications qui estimaient qu'on leur demandait trop d'information, et ce n'est pas le seul cas dans lequel les entreprises ont réagi. Il existe d'autres recours en dehors de la Loi sur la protection des renseignements personnels.

Pour ce qui est de la Loi elle-même, le risque serait d'exposer le gouvernement à des poursuites en responsabilité. Si vous créez des obligations ou des normes strictement définies dans la législation, cela peut accroître ce risque.

Le modèle suivi consistait en partie à tenter d'améliorer la conformité et les pratiques en matière de renseignements personnels au sein du gouvernement. À un certain niveau, c'est le modèle de l'ombudsman. Maintenant, le commissaire cherche un recours supplémentaire, un moyen supplémentaire pour les citoyens de faire respecter leurs droits.

Que cela implique simplement d'obtenir une ordonnance du tribunal exigeant l'application des recommandations et la modification des pratiques ou ouvre également le droit à des dommages et intérêts n'est pas tout à fait clair, parce qu'on peut disposer du premier recours, sans pouvoir réclamer des dommages-intérêts. La question est de savoir s'il faudrait l'exiger.

[*Français*]

M. Matthew Dubé: Permettez-moi d'aiguiller votre réponse, car je dispose de peu de temps.

En ce qui a trait au gouvernement, je comprends. Cependant, en ce qui concerne les compagnies de télécommunications ou les banques, par exemple, on a moins besoin d'avoir cette préoccupation, puisqu'elles doivent se soumettre à la loi à 100 %. Pour ce qui est du gouvernement, je conçois bien qu'il y a une nuance à apporter.

Mme Teresa Scassa: En ce qui a trait aux banques et aux compagnies de télécommunications, elles sont soumises à la Loi sur la protection des renseignements personnels dans le secteur privé. Dans ces circonstances, je crois qu'il y a moyen d'améliorer les recours en vertu de cette loi.

Un des problèmes a été soulevé par Mme Austin: il s'agit du fardeau que doit porter l'individu. En effet, le coût pour aller en cour est très élevé. On voit que très peu de personnes s'adressent à la Cour fédérale pour tenter d'obtenir des dommages-intérêts en vertu de la Loi sur la protection des renseignements personnels dans le secteur privé. Je crois même que les gens se représentent eux-mêmes devant la cour, parce qu'avoir recours aux services d'un avocat coûte trop cher. C'est un autre problème.

● (1025)

M. Matthew Dubé: Je comprends.

Merci.

[*Traduction*]

Le président: On pourrait peut-être en parler dans le cadre d'une révision de la législation de la LPRPDE, mais je comprends votre sentiment.

Chers collègues, j'aime toujours faire en sorte que chaque député à la table ait la possibilité de poser des questions. Deux des députés ici présents n'ont pas encore été en mesure de participer à la conversation.

Monsieur Scarpaleggia ou monsieur Picard, avez-vous une question?

M. Francis Scarpaleggia (Lac-Saint-Louis, Lib.): Oui, mais je vais...

[*Français*]

M. Michel Picard (Montarville, Lib.): Merci, monsieur le président.

Je remercie les témoins.

Je vais vous soumettre ceci et j'aimerais obtenir vos commentaires. Je vais me limiter à une seule question.

L'information en général évolue. La qualité de l'information qu'on recueille change selon le contexte dans lequel elle est reçue et appliquée. Bien souvent, le contenu lui-même est plus ou moins important, mis à part des exceptions comme le numéro d'assurance sociale, bien sûr.

Si je donne mon nom et ma date de naissance, par exemple, je m'expose à une certaine vulnérabilité dans certains dossiers. En même temps, si je m'inscris à un club d'anniversaire afin de recevoir une lettre chaque année, je dois aussi fournir mon nom et ma date d'anniversaire. Je viens encore de dévoiler au grand public de l'information qu'il aurait pu être dangereux de dévoiler dans un autre contexte.

Compte tenu de l'évolution dont a parlé M. Lyon, qui va décider dans quelles situations on recueille trop d'information?

[*Traduction*]

M. David Lyon: Tout dépend vraiment de l'utilisation faite par ailleurs de cette information.

La question des gros volumes de données a déjà été soulevée à plusieurs reprises, et elle me semble être cruciale ici, car il y a beaucoup de fragments d'information nous concernant ayant un air beaucoup plus trivial que nos dates de naissance, et qui peuvent être utilisés, une fois concaténés avec d'autres données, pour créer un profil de nous de sorte que nous nous retrouvons avec des profils qui sont aux mains des sociétés et des agences nationales de sécurité et d'application de la loi, profils qui sont des fictions, en un sens, parce qu'ils sont un collage de minuscules fragments de données recueillies à droite, à gauche.

C'est une question qui me semble incontournable dans toute tentative de réviser ces lois.

M. Michel Picard: Je suis entièrement d'accord sur la question de l'utilisation.

Madame Austin, vous avez dit quelque chose sur la nécessité de faire que les organismes limitent leur collecte d'information à celle qui correspond à leurs besoins spécifiques, ni plus ni moins. Avec l'évolution de l'information, comment puis-je évaluer ce qui semble relever de mon mandat?

Mme Lisa Austin: Vous voulez dire afin de réduire au minimum les volumes de données?

M. Michel Picard: Je viens de la communauté du renseignement, et le plaisir d'analyser des informations n'est pas de les obtenir, mais de les mettre en contexte.

Tout d'un coup, je peux lancer une recherche sur les gens qui n'ont pas de cheveux, sans aucune raison. Ça ne veut rien dire. Pourquoi devrais-je savoir ça? Je ne sais pas. Peut-être que dans un autre contexte, je vais lier ça à autre chose, et oh, voilà qui est intéressant. J'ai un profil d'une personne qui correspond à cette image. Tout d'un coup, la calvitie revêt un intérêt brûlant, qui peut à un moment donné déborder le cadre du mandat que j'ai dans mon agence.

Qui sera la personne chargée de décider où je dois arrêter la collecte d'informations et s'il faut que je m'arrête?

Mme Lisa Austin: Voilà une grande question. Je suppose que je voudrais juste ajouter une autre façon de l'aborder.

On peut le faire dès le début, mais peut-être devons-nous aussi commencer à réfléchir à la façon d'examiner les pratiques des différents départements. Je suppose qu'ils ont leurs propres normes. Les vôtres sont sans doute très différentes de celles d'autres organismes gouvernementaux. Quelle est l'efficacité de ces pratiques *ex post?*

Nous ne savons pas toujours dès le début, et peut-être nous faut-il accorder le bénéfice du doute dans certaines circonstances. Voilà une autre question. Certes, nous devons tirer parti des résultats des examens *ex post*: « Eh bien, qu'avez-vous fait? Qu'est-ce que ça a donné en termes d'efficacité? » Si ce n'est pas efficace, peut-être nous faut-il revenir en arrière et changer ces pratiques plutôt que de les perpétuer.

Quand il est difficile de savoir à l'avance, il faut peut-être commencer à réfléchir à certains modèles qui offrent une certaine latitude au départ assortie d'une obligation de rendre des comptes, et d'un mécanisme de contrôle.

● (1030)

Le président: Afin que tout le monde puisse intervenir, nous sommes à environ cinq minutes de la fin, je dois prendre une dizaine de minutes du temps du Comité pour discuter de nos travaux futurs.

Francis, une question, rapidement?

M. Francis Scarpaleggia: Je cherche juste à savoir si j'ai bien compris.

Nous avons une Loi sur l'accès à l'information, qui était probablement très prescriptive. Le gouvernement ne pouvait avoir accès qu'à certaines informations. Pour les informations fiscales, par exemple, c'était le numéro d'assurance sociale et l'adresse. Avec les progrès de la technologie, d'autres informations sont devenues disponibles — les adresses IP, par exemple. Même la technologie préexistante a tout d'un coup pris une nouvelle pertinence. Les relevés de compteurs d'électricité, par exemple, en rapport avec les cultures de marijuana et ainsi de suite.

Est-ce que je comprends bien en disant, en substance, que la loi est obsolète car elle ne prend pas en compte toute cette nouvelle information qui est disponible, et que, d'une certaine manière, nous devons codifier ce que nous devrions être autorisés à recueillir? En fait, nous serons toujours en retard d'une étape, parce que la technologie ne cessera pas d'avancer. Pour combler ces lacunes, nous devrons compter sur les décisions de justice jusqu'à ce que nous ayons suffisamment d'informations pour modifier à nouveau la loi et faire face à des choses comme les métadonnées et ainsi de suite. Est-ce une bonne façon de voir le processus qui nous occupe ici?

Mme Teresa Scassa: Je serais tenté de dire que la loi est obsolète parce que c'est la loi. Dans un sens, dans notre conversation aujourd'hui, nous sommes passés de la législation du secteur privé, à la sécurité nationale, à la Charte et à la Loi sur la protection des renseignements personnels et l'on a dit aussi que tout ce paradigme a changé. L'approche consistant à aborder ces questions en les enfermant dans leur contexte propre — cela relève de la vie privée, cela du Code criminel, cela de la sécurité nationale, cela de l'accès à l'information — est peut-être tout simplement surannée.

M. Francis Scarpaleggia: Nous essayons vraiment d'identifier ce qui devrait être ou ne pas être acceptable, mais nous aurons toujours un temps de retard à ce sujet. Est-ce correct? On peut voir les choses comme ça?

Mme Teresa Scassa: Je le crois. Cela change constamment, mais c'est peut-être juste notre paradigme d'analyse qu'il nous faut réélaborer et repenser.

M. Francis Scarpaleggia: Les règles que nous utilisons pour prendre ces décisions peuvent être...

Mme Teresa Scassa: Ce sont les règles, et c'est aussi notre façon de séparer les questions et de dire voici une question de tel genre, et une autre de tel autre. Les questions de gouvernance algorithmique abordées par le professeur Austin soulèvent aussi d'intéressantes questions qui vont au-delà de la protection des renseignements personnels et touchent les droits de la personne de façon plus générale. Cela fait partie du défi aussi.

M. Francis Scarpaleggia: Nous devrons toujours compter sur la jurisprudence, dans une certaine mesure, pour décider ce qui est acceptable et ce qui ne l'est pas. La loi ne peut jamais être à jour à cet égard. Est-ce exact?

Mme Teresa Scassa: C'est tout à fait juste, je pense.

Le président: Je ne suis pas si pessimiste. On peut toujours la rédiger de manière à permettre un ajustement dynamique du système.

Je sais que M. Long et M. Lightbound ont chacun une question. Nous commencerons par M. Lightbound.

M. Joël Lightbound: Je serai très rapide, et on peut plus ou moins répondre par un oui ou un non. Ma question est pour Mmes Scassa et Austin.

Autant que je sache, les métadonnées ne sont définies nulle part dans la législation canadienne. Corrigez-moi si je me trompe, mais je ne pense pas que ce soit le cas. Pensez-vous qu'il faille les inclure dans notre définition des renseignements personnels dans la Loi sur la protection des renseignements personnels, pour qu'elles soient protégées, ou qu'il devrait y avoir quelque chose par rapport à ça dans la Loi sur la protection des renseignements personnels?

Mme Teresa Scassa: Je voulais simplement demander ce que vous entendez par métadonnées, donc évidemment la réponse est oui. C'est en fait un terme assez large.

M. Joël Lightbound: Oui. C'est vrai.

Mme Teresa Scassa: C'est de l'information à propos d'information, en gros. En tout état de cause, oui, je pense que ce serait probablement le cas.

Mme Lisa Austin: Je pense que ce serait utile dans la définition des renseignements personnels, qui est assez large pour y faire place. C'est de l'information identifiable, donc dans de nombreux contextes les métadonnées trouveraient parfaitement leur place comme information identifiable. Il serait utile de préciser en disant, « par exemple, cela comprend... », et quand vous avez la liste non exhaustive, y ajouter cela. C'est utile pour l'interprétation.

La réserve porte sur la façon de définir les métadonnées. Si vous utilisez une formule générale, comme « cela inclut des informations sur l'information », ou quelque chose comme ça...

● (1035)

M. Joël Lightbound: C'est tout.

Je vous remercie.

Le président: Merci beaucoup.

Monsieur Long, avez-vous une brève question supplémentaire?

M. Wayne Long: Elle n'est pas vraiment brève, donc je vais juste la garder pour plus tard.

Le président: J'ai une question rapide pour Mme Scassa.

Dans votre présentation, vous avez parlé de la collecte indirecte des données du secteur privé par le gouvernement, à notre insu à tous. Mes renseignements personnels, qui seraient normalement régis par la LPRPDE dans mes rapports avec une entreprise du secteur privé, pourraient alors, par le biais d'un rapport que la société entretient avec le gouvernement... Vous ai-je bien entendu?

Mme Teresa Scassa: C'est juste que la LPRPDE permet aux entreprises, à l'insu et sans le consentement de l'individu, de communiquer des renseignements aux organismes d'enquête, à la police, aux agences d'application de la loi, de la sécurité nationale, ou d'autres organismes de réglementation, à leur demande. Une société peut refuser de le faire sans une ordonnance du tribunal, mais elle peut divulguer ces renseignements volontairement. C'est un problème important qui s'est posé dans le cadre de la LPRPDE, qui permet de divulguer volontairement des renseignements, sans mandat, aux organes gouvernementaux, essentiellement.

Le président: D'accord.

J'ai une question pour vous, madame Austin. Au sujet de la jurisprudence.

Nous avons parlé de questions de souveraineté qui se rapportent aux données. M. Saini avait en fait une série de questions à ce sujet. Les tribunaux ont décidé il y a quelques années que toute personne entrant sur le territoire du Canada se voit accorder tous les privilèges et protections d'un citoyen canadien. Existe-t-il une jurisprudence en la matière? Les tribunaux ont-ils eu à se prononcer sur la question de savoir si un individu entrant au Canada bénéficie effectivement des garanties offertes par la Charte des droits et libertés en ce qui concerne la protection de ses informations ou données personnelles?

Mme Lisa Austin: À ma connaissance, cette question n'a pas été portée devant les tribunaux.

Le président: Elle n'a pas encore été testée.

Mme Lisa Austin: Pas à ma connaissance; quand votre corps est dans un endroit et vos données sont dans une autre, vous êtes en quelque sorte dans une zone inconnue.

Le président: D'accord. Merci beaucoup.

Monsieur Lyon, ma question pour vous vient de l'exemple que vous me donniez, comme ancien professionnel de l'informatique, quand nous parlions d'informations passant d'une plaque tournante du Canada à une autre aux États-Unis, avant de revenir éventuellement à la même ville au Canada. Les paquets de données, c'est de cela, je suppose, que vous parliez dans le cadre d'un transfert de réseau, pourraient transiter par une juridiction hors du Canada, afin de se rendre à destination. Cela soulève quelques questions.

Auriez-vous des témoins à proposer à ce Comité qui pourraient traiter des aspects informatiques de cette question? Il s'agit d'une problématique assez technique qu'il nous faut bien comprendre. Je serais ravi d'avoir un expert qui puisse répondre à une série de questions très techniques.

M. David Lyon: Il est extrêmement important que vous puissiez le faire. La personne que je vous suggère serait Andrew Clement à l'Université de Toronto.

Le président: D'accord. Merci beaucoup.

Au nom de mes collègues, je vous remercie tous pour votre témoignage aujourd'hui. Si vous souhaitez apporter un complément d'information sur quoi que ce soit, veuillez le communiquer au greffier du Comité. Il se peut que nous ayons des éclaircissements à vous demander dans le cours de notre examen de la Loi sur la protection des renseignements personnels. Merci beaucoup de nous avoir consacré votre temps.

Avant de partir, chers collègues, je veux discuter un peu des affaires du Comité. Voulez-vous le faire en réunion publique ou à huis clos? Nous pouvons passer à huis clos en un instant si vous voulez. À vous de voir. Je veux discuter de l'horaire et de la liste des témoins attendus ces deux prochaines semaines.

Un député: Je dirais à huis clos.

Le président: Nous passons à huis clos? D'accord. Nous allons suspendre la séance et passer à huis clos.

Merci encore, mesdames et messieurs.

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