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 046 • 1re SESSION • 42e LÉGISLATURE

TÉMOIGNAGES

Le mardi 14 février 2017

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 février 2017

● (1545)

[*Traduction*]

Le président (M. Blaine Calkins (Red Deer—Lacombe, PCC)): Chers collègues, je vous souhaite la bienvenue dans notre nouvelle salle de réunion.

Nous allons commencer tout de suite les témoignages.

Il s'agit de nos premières audiences dans le cadre de notre nouvelle étude de la LPRPDE, soit la Loi sur la protection des renseignements personnels et les documents électroniques. Je ne vous le lis même pas, je le sais tout simplement, ce qui vous montre que je suis ici depuis bien trop longtemps.

Je vous souhaite la bienvenue dans notre nouvelle salle de comité.

Nous recevons aujourd'hui des témoins très prestigieux, dont beaucoup ont déjà comparu devant des comités. Accueillons Chantal Bernier, qui travaille maintenant chez Dentons Canada et qui a une connaissance et une expérience approfondies du domaine. Je vous remercie beaucoup d'être ici.

Nous recevons également Alysia Lau et John Lawford, qui représentent le Centre pour la défense de l'intérêt public. Je vous remercie d'être ici.

Enfin, nous accueillons Éloïse Gratton et R. Gary Dickson, qui ont déjà comparu devant nous. Nous sommes heureux de vous revoir tous les deux.

Nous commencerons par vos exposés de 10 minutes, dans la langue officielle de votre choix, selon l'ordre dans lequel je vous ai présentés. C'est également l'ordre selon lequel vous apparaissez dans la liste. Vous savez tous comment le Comité fonctionne. Nous nous arrêterons à 17 h 30 exactement, parce que certaines personnes ont des déplacements de prévus.

Madame Bernier, la parole est à vous.

[*Français*]

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

Je vous remercie de me donner l'occasion de contribuer à vos travaux sur la révision de la Loi sur la protection des renseignements personnels et les documents électroniques.

Je ferai ma présentation dans les deux langues et je serai heureuse de répondre à vos questions dans les deux langues également.

Dans le cadre de ma présentation, j'utiliserai le terme « la Loi » pour désigner la Loi sur la protection des renseignements personnels et les documents électroniques.

Mon point de départ est la lettre que vous a adressée le commissaire à la protection de la vie privée du Canada le 2 décembre 2016 et dans laquelle il portait à votre attention quatre domaines d'intervention possibles. J'y ajouterai mon éclairage personnel en m'appuyant sur mon ancien rôle au sein de l'organisme de réglementation de la vie privée et sur la fonction que j'occupe présentement, soit avocate dans le secteur privé.

Le premier point porte sur le consentement valable.

L'été dernier, j'ai soumis un mémoire dans le cadre de la consultation du commissaire sur le consentement. J'y ai conclu que, dans sa forme actuelle, la Loi est adéquate en ce sens, et ce, pour deux raisons essentielles. D'abord, elle a la rigueur nécessaire pour assurer la validité du consentement. Deuxièmement, elle a la souplesse nécessaire pour que ce consentement s'applique aux diverses applications qui ont maintenant cours dans Internet.

Je vous donne comme exemple l'article 6.1, dans lequel on dit ceci:

> [...] le consentement de l'intéressé n'est valable que s'il est raisonnable de s'attendre à ce qu'un individu visé par les activités de l'organisation comprenne la nature, les fins et les conséquences de la collecte, de l'utilisation ou de la communication des renseignements personnels auxquelles il a consenti.

C'est donc dire qu'on prend vraiment en compte la complexité d'Internet, sans toutefois prescrire de modalités, de sorte qu'il est possible d'adapter ce principe à toutes les applications qui se présentent.

Par ailleurs, la Loi reconnaît le consentement implicite. À l'annexe 1 de la Loi, plus particulièrement au point 4.3.6, vous verrez en effet que le consentement implicite est acceptable dans certaines circonstances.

Dans mon mémoire, je souligne que l'accroissement de la valeur du consentement passe par les politiques de confidentialité. À mon avis, celles-ci doivent satisfaire à trois critères précis. Premièrement, elles doivent être énoncées dans un langage accessible. Deuxièmement, elles doivent être adaptées à l'organisation. Troisièmement, elles doivent être facilement navigables. Aucune modification législative n'est nécessaire pour apporter cette amélioration.

Par ailleurs, il y a une amélioration qui n'exige pas de modification législative, mais pour laquelle une telle modification pourrait être utile. Il s'agit d'une précision qui existe en droit européen et selon laquelle l'anonymisation constitue une façon de soustraire les renseignements personnels à l'application de la loi.

Je vous fais cette suggestion parce que je vois très souvent dans des politiques de confidentialité un paragraphe qui dit au lecteur et au consommateur que les renseignements personnels dépersonnalisés serviront à tel ou tel usage. Or c'est inutile. En effet, lorsque les identifiants sont séparés des renseignements pour que l'individu ne puisse plus être identifié, la loi ne s'applique pas. Je pense qu'il serait utile de le clarifier, comme le fait le droit européen.

● (1550)

[*Traduction*]

La deuxième préoccupation portée à votre attention par le commissaire en est une largement partagée: la protection de la réputation en ligne. Cependant, la question ne relève que partiellement de la loi fédérale. La majorité des atteintes à la réputation surviennent non pas dans le cadre de transactions commerciales, mais dans celui de relations personnelles, elles sont donc du ressort de lois provinciales.

Je vais vous donner l'exemple des cinq lois provinciales pertinentes à cet égard et d'une loi fédérale.

Pour ce qui est des lois provinciales, la Colombie-Britannique, le Manitoba, la Saskatchewan et Terre-Neuve-et-Labrador ont adopté des lois particulières qui reconnaissent la violation de la vie privée comme un droit de recours en responsabilité civile. Au Québec, un juge peut prescrire des mesures visant à faire cesser une atteinte à la réputation en ligne.

Au fédéral, la Loi sur la protection des Canadiens en ligne criminalise la transmission non consensuelle d'images intimes, comme vous le savez.

Il y a donc un cadre qui donne des outils pour faire cesser les atteintes à la réputation en ligne, mais il reste tout de même un vide juridique. Ce vide juridique pourrait peut-être être comblé par une loi fédérale. Il faudrait alors créer un droit à l'oubli, c'est-à-dire le droit d'effacement de certains renseignements, selon le modèle du droit européen, comme le commissaire l'a exposé dans sa lettre.

Une telle disposition réduirait la dissémination de renseignements personnels nuisibles à la réputation et ajouterait, donc, une certaine protection. Afin de bien maîtriser sa portée, cependant, le cadre législatif canadien devrait servir de balise: le droit à l'effacement pourrait s'appliquer à tout affichage de données personnelles déclaré par un tribunal comme une violation du droit à la vie privée, avec la possibilité d'injonctions afin d'interdire la dissémination de données pendant le procès. Quoi qu'il en soit, il me semble important de lui donner une certaine solidité plutôt que de conserver le pouvoir discrétionnaire et que cela reste un fardeau pour les plateformes.

Devant la gravité de l'atteinte à la réputation en ligne, et malgré le caractère restreint de la compétence fédérale en la matière, je vous encourage à explorer la création dans la loi d'un droit à l'effacement dans le but de réduire les dommages de l'atteinte à la réputation en ligne.

La troisième question portée à votre attention par le commissaire concerne ses pouvoirs d'exécution. De par ma pratique chez Dentons, qui est le plus grand cabinet d'avocats au monde et qui m'amène à travailler dans le contexte mondial de la protection de la vie privée, je me préoccupe de la disparité croissante entre les pouvoirs de notre commissaire et ceux de ses homologues.

Je ne peux qu'observer la différence d'emprise des autres commissaires sur les entreprises parce qu'ils peuvent imposer des amendes de millions de dollars. La Federal Trade Commission, par exemple, lorsqu'elle mène des enquêtes comparables à celles de notre commissaire, peut imposer des millions de dollars en amendes, alors que notre commissaire ne peut que faire des recommandations.

La France peut imposer des amendes de 300 000 euros, et il est intéressant de souligner que le 7 février dernier, la Russie a multiplié par 10 l'amende maximale imposable selon ses lois de protection de la vie privée. Ce n'est toujours pas un montant très élevé. Le plafond est passé de 10 000 roubles à 35 000 roubles, ce qui correspond à environ 1 600 $ CAD, mais cela montre une tendance vers le renforcement des pouvoirs d'exécution. Le commissaire à la vie privée de la Nouvelle-Zélande, lui, vient de recommander à son gouvernement des amendes d'un million de dollars pour les atteintes à la vie privée.

Comme vous l'avez peut-être entendu, le règlement européen qui entrera en vigueur le 25 mai 2018, prévoit des amendes pouvant aller jusqu'à 4 % des revenus totaux d'une entreprise.

Pourtant, le Commissariat canadien obtient de bons résultats, surtout grâce à son pouvoir de nommer les entreprise, parce que la réputation revêt une importance cruciale. Il faut donc soupeser, d'une part, l'avantage d'un modèle ombudsman qui, selon le secteur privé, favorise la collaboration entre les entreprises et le Commissariat, et d'autre part, la singularité mondiale d'un commissariat canadien dépourvu de pouvoirs d'exécution, si je puis dire.

Cependant, je dois vous dire, selon mon expérience en matière de réglementation et comme conseillère juridique en protection de la vie privée auprès des entreprises, que je ne considère pas les pouvoirs d'exécution comme le facteur déterminant de la collaboration. Ce serait plutôt la bonne foi de part et d'autre. C'est ce qui compte vraiment.

● (1555)

De même, l'imposition de sanctions n'est pas nécessairement néfaste pour le secteur privé, puisqu'en fait, elle peut rétablir l'équité entre les organisations diligentes qui affectent, elles, en amont, les ressources nécessaires à la protection des renseignements, et celles négligentes qui, ne l'ayant pas fait, payent l'amende en aval. Beaucoup de représentants d'organisations diligentes vous diront: « Merci. Vous venez d'équilibrer les règles du jeu. »

Cela dit, quand on compare les pouvoirs d'exécution du commissariat canadien avec ceux des autres commissariats dans le monde, une mise à niveau semble s'imposer, mais selon certains paramètres.

Je vous encourage à explorer l'option de créer un pouvoir d'imposer des amendes, mais rigoureusement encadré de la façon suivante. Premièrement, je crois qu'une amende ne devrait être imposée que s'il y a preuve de négligence. Dans un contexte de cyber-attaques incessantes, on ne peut pas exiger des organisations de parer à tous les coups. Ce ne serait pas juste.

Deuxièmement, l'amende devrait être payable au receveur général, évidemment. Il existe des autorités de protection des données qui imposent des amendes qui leur sont directement payables. Cela crée un conflit d'intérêts. Cela devrait passer par la Cour fédérale. Évidemment, et cela a une énorme incidence, il doit y avoir un droit d'appel.

Troisièmement, comme dans le cas du règlement européen, je serais favorable à ce que l'amende soit calculée selon un pourcentage des revenus annuels, parce que l'utilisation de renseignements personnels fait partie des profits. Du coup, une mauvaise utilisation des renseignements personnels devrait faire partie des pertes financières. Il y a là une logique, selon moi, à reconnaître la valeur financière des renseignements personnels. Ensuite, cela permet un arrimage avec l'investissement nécessaire en amont. Enfin, cela laisserait la question des dommages-intérêts aux recours civils, comme il se doit.

[*Français*]

Finalement, le quatrième point que le commissaire porte à votre attention est, à mon avis, de la plus grande urgence. Pourquoi? C'est parce que cela concerne le nouveau règlement européen sur la protection des données, qui entrera en vigueur le 25 mai 2018. Ce règlement modifie de façon considérable la loi européenne sur la protection des renseignements personnels, et cela comporte un risque pour notre statut d'adéquation. Je m'explique.

L'enjeu est économique. Le Canada jouit du statut d'adéquation avec l'Europe, ce qui permet aux compagnies canadiennes de recevoir des données européennes sans autre autorisation. C'est un avantage concurrentiel crucial. Nous pourrions perdre ce statut d'adéquation, et ce, pour deux raisons. Premièrement, le nouveau règlement établit que le statut d'adéquation sera maintenant révisé tous les quatre ans. Notre statut sera donc remis en cause. Deuxièmement, nous serons évalués selon les normes du nouveau règlement. Or celles-ci sont très différentes de celles de la loi fédérale actuelle. Il y a donc un problème de concordance.

Bref, nous pourrions perdre un avantage concurrentiel considérable. Le Canada est en effet le seul État nord-américain à bénéficier de cette adéquation. Je vous encourage donc à porter votre attention sur ce sujet.

Sur ce, je serai heureuse de répondre à toutes vos questions.

● (1600)

[*Traduction*]

Le président: Merci beaucoup, madame Bernier.

Vous avez un peu dépassé les 10 minutes imparties, mais compte tenu de votre qualité d'ex-commissaire, j'ai pensé que nous pouvions vous accommoder.

Monsieur Lawford, est-ce vous qui allez prononcer l'exposé de votre organisation?

M. John Lawford (directeur exécutif et avocat général, Centre pour la défense de l'intérêt public): Je vais commencer.

Le président: Très bien.

Monsieur Lawford, la parole est à vous.

M. John Lawford: Merci, monsieur le président.

Le Centre pour la défense de l'intérêt public est une organisation nationale de bienfaisance enregistrée, à but non lucratif qui offre des services juridiques et de recherche pour défendre les intérêts des consommateurs, en particulier des consommateurs vulnérables concernant la prestation de services publics importants. Nous sommes intervenus activement dans le processus d'établissement de la LPRPDE, même avant qu'elle ne soit adoptée.

Il y a cinq ans, nous sommes venus devant ce Comité parler de la protection de la vie privée et des réseaux sociaux. Aujourd'hui, nous venons discuter avec vous dans le cadre de votre étude de la LPRPDE. Nous parlerons encore des médias sociaux, mais cette fois-ci, ils s'accompagnent de leurs amies, les mégadonnées.

Les réseaux sociaux et la plupart des applications pour téléphones intelligents recueillent systématiquement des renseignements personnels au sens de la LPRPDE et les conservent sur des serveurs centraux. L'information est ensuite utilisée, comme le permet la LPRPDE, afin de cibler les publicités qui apparaîtront dans les médias sociaux de cette personne, de ses amis, des membres de sa famille et de ses collègues.

On parle alors de « publicité comportementale » ou de marketing, puisque d'énormes quantités de données très personnelles, dont les préférences d'une personne concernant une pléthore de produits, ses achats, l'endroit où elle habite, son âge, son genre, son ethnicité et bien d'autres choses, permettent aux publicitaires de lui envoyer des publicités ciblées en fonction de ses comportements et de son profil présumés.

C'est ce qu'on appelle les « mégadonnées » quand les publicitaires et d'autres entreprises combinent des ensembles de données de diverses applications et sites Web, ou d'un même site sur une longue période. Il y a ensuite de l'exploration de données, à l'aide d'algorithmes, pour dégager des tendances et prévoir quelles annonces ciblées pourraient porter fruit ou même essayer de trouver des façons présumées de connaître ou d'influencer ses comportements futurs.

Les entreprises qui le font vous diront aujourd'hui qu'elles respectent la LPRPDE, qu'elles ont des politiques sur la protection de la vie privée, qu'elles ont votre consentement et qu'elles suivent toutes les règles sur la communication et le traitement de données. Le fait est, toutefois, qu'elles n'ont bien souvent pas votre consentement éclairé. Le consentement éclairé, qui sous-entend que vous comprenez les conséquences de la divulgation de vos renseignements, ce à quoi ils serviront et comment ils seront communiqués, est la norme pour la collecte, l'utilisation et la communication de données en vertu de la LPRPDE.

Les entreprises commencent maintenant à demander à ce qu'on modifie la norme sur le consentement, essentiellement parce qu'elle empêche la collecte de données et de mégadonnées. Elles vous demanderont d'abandonner la norme du consentement éclairé qui protège les consommateurs, ainsi que les attentes raisonnables et l'interprétation actuelle du concept de la vie privée. Elles vous demanderont de les remplacer par un modèle fondé sur le risque ou sur un consentement plus implicite. Il faut leur résister. En fait, la LPRPDE doit privilégier la norme du consentement éclairé, et tout ce qu'il faut, ce sont de nouvelles règles pour protéger cette norme et les consommateurs.

Pour ce qui est de l'application de la loi, si nous voulons régler les problèmes liés à la protection de la vie privée et aux mégadonnées en ligne, le commissaire à la protection de la vie privée du Canada doit jouir de véritables pouvoirs d'application de la loi, y compris du pouvoir de rendre des ordonnances obligatoires et d'imposer des amendes ou des sanctions administratives pécuniaires.

Le CDIP réclame ces pouvoirs depuis le premier examen de la LPRPDE, qui a eu lieu en 2008. À l'époque, le Commissariat à la protection de la vie privée n'en voulait pas. Puis, il a croisé les armes avec Facebook après une plainte déposée en 2010. Par la suite, Jennifer Stoddart et le gouvernement ont commencé à vous demander haut et fort, à répétition, le pouvoir de rendre des ordonnances et d'imposer des amendes. Son raisonnement était que son commissariat ne pouvait pas obliger les grands médias sociaux à se conformer seulement à coup de recommandations non contraignantes, par la honte et en nommant les entreprises fautives.

M. Therrien, l'actuel commissaire à la protection de la vie privée, est plus prudent et il pourrait ne vous demander qu'un pouvoir d'ordonnance. Ce sera difficile à appliquer en cour. Vous devriez aussi lui conférer le pouvoir d'imposer des amendes.

Quoi qu'il en soit, si le ou la commissaire à la protection de la vie privée dit qu'il ou elle a besoin de ces outils pour faire son travail, pourquoi ne lui donneriez-vous pas? Le Commissariat se bat contre les plus grandes entreprises au monde en ce moment et a besoin d'outils pour ce faire. Il est franchement embarrassant que les commissaires provinciaux à la protection de la vie privée aient ce pouvoir, mais pas le Commissariat canadien. Ce n'est qu'en faisant respecter les normes déjà prescrites par la LPRPDE qu'on verra si elles sont efficaces ou s'il y a lieu de les modifier. Il serait injuste de juger de l'efficacité de la loi alors qu'elle n'est pas mise en application.

Pour ce qui est des enfants, nous avons besoin de nouvelles règles sur le traitement des renseignements personnels des enfants. J'ai lu une lettre ouverte extraordinaire à ce sujet la semaine dernière. Owen Charters, président-directeur général des Repères jeunesse du Canada, disait ce qui suit:

> Selon le *Wall Street Journal*, les sites Web pour enfants aux États-Unis installent plus de logiciels de pistage que les sites destinés aux adultes. Ces outils suivent nos enfants lorsqu'ils naviguent sur le Web, recueillant des données sur leurs comportements et leurs intérêts. Ces renseignements sont souvent vendus à des sociétés de marketing.
>
> Il y a constamment des campagnes de sensibilisation publiques sur la cyberintimidation. Il y a des changements qui s'observent, mais compte tenu de toute l'attention que ces discussions attirent, les droits à la protection de la vie privée des enfants au Canada sont mis en veilleuse.

Le fait qu'une simple organisation de bienfaisance générale défendant le bien-être des enfants souligne la question de la protection de la vie privée en ligne est révélateur. Sa lettre se conclut par une exhortation à l'endroit du gouvernement canadien à adopter une loi spéciale sur la protection de la vie privée des enfants.

● (1605)

Nous partageons ses sentiments, mais nous croyons que cette protection pourrait être ajoutée à la LPRPDE. Nous constatons le problème de visu. En 2011, le CDIP a porté plainte pour atteinte à la vie privée contre Nexopia.com, un réseau social de l'Alberta, qui vise principalement les adolescents. Le Commissariat à la protection de la vie privée a retenu toutes nos plaintes, qui ne portaient pas tant sur la sécurité en ligne que sur le marketing ciblé à l'intention de mineurs.

Malheureusement, outre des lignes directrices volontaires publiées par le Commissariat à la protection de la vie privée, nous n'avons observé aucune amélioration dans la protection de la vie privée des enfants au Canada depuis. Nous avons une proposition détaillée à vous présenter pour remédier au problème, et l'on voit que l'Europe adopte également des règlements — mais compte tenu du temps dont nous disposons, nous vous invitons à nous interroger sur ces solutions dans vos questions.

Mlle Alysia Lau (conseillère juridique, Centre pour la défense de l'intérêt public): Bonjour.

Nous aurions également besoin de nouvelles règles sur la rétention et la destruction de données. Les consommateurs peuvent-ils être certains que l'information qu'ils ont fournie ou qui a été extraite de leurs habitudes sera vraiment détruite ou qu'elle ne sera plus utilisée lorsque les raisons pour lesquelles ils ont donné leur consentement ne seront plus valides? Ont-ils un quelconque contrôle? Certaines des personnes ici présentes aujourd'hui vous diront que non.

Nous vous disons qu'il est d'ores et déjà le temps de les effacer. La LPRPDE dicte qu'on ne peut conserver de renseignements personnels que le temps nécessaire pour la réalisation des fins déterminées par l'organisation. Cependant, la loi exige seulement que les organisations élaborent des lignes directrices et appliquent des procédures pour la conservation des renseignements personnels. Elle dicte qu'on devrait — et non doit — détruire, effacer ou dépersonnaliser les renseignements personnels dont on n'a plus besoin aux fins précisées. Cela ne suffit pas.

Les seuls constats du CPVP que Nexopia a refusé de suivre, au point où le Commissariat s'est adressé aux tribunaux, étaient ceux qui lui demandaient d'effacer les renseignements personnels d'adolescents qui n'utilisaient plus leurs services. Comme les Canadiens peuvent maintenant passer des années, des dizaines d'années, et dans le cas des enfants, peut-être même toute leur vie à utiliser des services en ligne comme ceux d'un réseau social, la quantité de renseignements personnels recueillis sur un utilisateur peut donner le vertige. Plus une organisation a d'information sur une personne, plus elle la conservera longtemps et plus le risque d'atteinte à la protection des données est grand.

Les Canadiens doivent avoir le choix et pouvoir exercer un contrôle sur la façon dont leurs données personnelles sont utilisées, y compris par le consentement, la rectification d'information et particulièrement la suppression ou l'effacement de renseignements les concernant.

L'Union européenne a reconnu, dans son récent Règlement général sur la protection des données, qui entrera en vigueur en 2018, un droit à l'effacement. Le nouveau RGPD codifie ce qu'on appelle le « droit à l'effacement ». Il confère aux personnes le droit à l'effacement de leurs données personnelles afin de prévenir le traitement de leurs données notamment lorsque la personne retire son consentement, s'oppose au traitement de ces données ou qu'il n'y a pas de raison légitime supérieure justifiant qu'elles soient conservées.

Les organisations sont également tenues de faire particulièrement attention lorsqu'elles recueillent des données personnelles partagées par des enfants sur un réseau social, par exemple. Elles ne peuvent refuser que dans certaines circonstances d'effacer des données personnelles lorsqu'on leur demande, notamment pour se conformer à leurs obligations juridiques ou exercer leur liberté d'expression.

Le CDIP estime que le Comité devrait envisager de recommander des règles similaires pour la LPRPDE, pour accorder le même genre de protection que le RGPD. Par exemple, les organisations devraient divulguer d'emblée aux utilisateurs combien de temps elles comptent conserver leurs données personnelles et pour quelles raisons. Elles devraient également être tenues d'effacer ou de détruire les renseignements personnels dont on n'a plus besoin aux fins précisées ou si la personne a retiré son consentement.

● (1610)

M. John Lawford: Dans notre mémoire de 2012, nous recommandions un suivi des parties liées et la déclaration des flux de données, l'établissement d'une liste nationale d'interdiction du suivi des télécommunications ainsi que des évaluations des facteurs relatifs à la vie privée pour les réseaux sociaux et les autres entreprises avant le lancement de grands services utilisant des renseignements personnels. Dans notre soumission récente au Commissariat sur l'interprétation du consentement dans un contexte numérique, nous avons recommandé la mise en oeuvre de normes sur les préférences relatives à la protection de la vie privée et d'un système de marques de confiance.

Nous sommons le Comité de se pencher sur ces propositions avant-gardistes sur la façon de renforcer la norme du consentement éclairé qu'on trouve dans l'actuelle LPRPDE, puisque les Canadiens sont confrontés chaque jour aux conséquences du marketing ciblé et des mégadonnées.

Nous vous remercions de votre attention et nous avons hâte de répondre à vos questions.

Le président: Merci infiniment, monsieur Lawford et madame Lau. C'est très apprécié.

Nous allons maintenant entendre Mme Gratton, s'il vous plaît. Vous avez jusqu'à 10 minutes.

[*Français*]

Me Éloïse Gratton (associée et cochef nationale, Groupe de pratique Respect de la vie privée et protection des renseignements personnels, Borden Ladner Gervais, à titre personnel): Je vous remercie de m'avoir invitée. Je suis heureuse d'être ici aujourd'hui et d'avoir ainsi l'occasion de vous faire part de mes réflexions sur des sujets importants pour les Canadiens en matière de protection de la vie privée.

Je suis associée chez Borden Ladner Gervais et j'enseigne également à la Faculté de droit de I'Université de Montréal. C'est à titre personnel que je comparais aujourd'hui devant votre comité.

Je traiterai de deux sujets qui ont fait l'objet de consultations de la part du Commissariat à la protection de la vie privée au cours de la dernière année, soit les enjeux touchant le consentement valable ainsi que la réputation et le respect de la vie privée. De plus, je dirai quelques mots sur les pouvoirs d'exécution. Je témoignerai en anglais, mais je répondrai aux questions en français ou en anglais.

[*Traduction*]

La LPRPDE se fonde sur les principes de pratiques justes en matière de renseignements personnels qui ont été établis au début des années 1970. Il ne faut pas oublier que ces principes avaient pour principal objectif de répondre aux inquiétudes entourant les bases de données informatisées et le fait que différentes organisations du secteur privé pouvaient s'échanger plus facilement des renseignements personnels sans le consentement des personnes ou sans qu'elles ne soient au courant. À l'époque, on avait déterminé que la meilleure protection était que chaque personne reste maître de ses renseignements personnels.

Quarante ans plus tard, ce concept est toujours l'une des principales théories à la base des lois sur la protection des données et de la vie privée dans le monde, y compris de la LPRPDE. Cependant, la politique fondée sur les avis et les choix n'est plus réaliste. Les individus sont inondés d'un volume d'informations qu'on ne peut s'attendre à ce qu'ils arrivent à comprendre. Comme le Commissariat l'a souligné, les flux d'informations complexes et les nouveaux modèles d'affaires font intervenir une multitude de tierces parties et mettent à mal le modèle classique du consentement.

La première question, si nous voulons conserver le modèle fondé sur le consentement, consisterait à déterminer si nous devrions revoir le concept du consentement dans la LPRPDE. Jean Carbonnier, l'un des plus grands juristes français du XX ^{e} siècle a dit, en français « ne légiférer qu'en tremblant ». Il voulait dire par là que nous devons faire preuve d'une grande prudence quand nous prenons ou modifions des lois. Nous devons veiller à ce que la modification ne devienne pas nuisible ou problématique avec l'émergence de nouvelles technologies. Le libellé actuel sur l'obtention du consentement, dans la LPRPDE, est assez souple. Il l'est assurément assez pour être adapté aux nouvelles technologies et aux nouveaux modèles d'affaires.

Cependant, l'inconvénient de cette souplesse, c'est qu'elle génère de l'incertitude. Par conséquent, il est de plus en plus nécessaire d'établir des lignes directrices sur la transparence et l'obtention d'un consentement valable pour réduire l'incertitude et permettre aux organisations d'innover sans courir de trop grands risques juridiques. Les entreprises tiennent compte des lignes directrices du CPVP, et ses directives récentes sur la publicité comportementale en ligne, le développement d'applications et l'Internet des objets sont très utiles. Ces documents sont plus pertinents et opportuns que jamais.

En vertu de la LPRPDE, lorsqu'elles cherchent à déterminer le type de consentement qu'elles doivent obtenir, les organisations doivent tenir compte des attentes raisonnables de la personne. La nature de ces attentes dans un contexte donné et la légitimité de certaines activités dans une perspective de protection de la vie privée dépendent souvent de nombreux facteurs, y compris des normes sociales prévalentes. Un autre argument contre la modification de la notion du consentement dans la LPRPDE tient au fait que les normes sociales liées aux nouvelles technologies futures ou aux futures pratiques commerciales ne sont peut-être pas encore établies. Au cours des dernières années, le CPVP a commandé des études visant à évaluer le degré de sensibilisation des Canadiens à certains enjeux et aux nouvelles technologies, leur compréhension et leurs perceptions. Ces études sont de plus en plus importantes, puisqu'elles nous permettent de mieux comprendre les consommateurs et leurs attentes et d'évaluer comment évolue la norme sociale en lien avec telle technologie ou telle pratique commerciale.

Au cours des dernières années, j'ai proposé, dans diverses publications, que la solution aux difficultés inhérentes au modèle du consentement pourrait comprendre l'adoption d'une approche ou d'une interprétation fondée sur le risque, qui nous porterait à demander le consentement express seulement pour la collecte, l'utilisation et la communication de données si les activités visées risquent de causer du tort à la personne. Par exemple, il faudrait obtenir le consentement express de la personne pour utiliser ses renseignements personnels afin de prendre une décision en matière d'admissibilité qui aurait une incidence sur elle; pour divulguer de l'information qui pourrait comprendre des renseignements sensibles ou potentiellement embarrassants; ou pour faire quelque chose qui pourrait aller à l'encontre des attentes de la personne.

L'approche fondée sur le risque permettrait peut-être aux organisations de simplifier leurs communications avec les individus, ce qui réduirait le fardeau imposé aux consommateurs, ainsi que la confusion, puisqu'ils recevraient moins de demandes de consentement. Ainsi, ces demandes voudraient dire quelque chose, parce qu'elles mettraient l'accent sur les questions qui les préoccupent. Bien que cette approche sous-entendrait de repenser le modèle de consentement qu'on trouve actuellement dans la LPRPDE, dans une certaine mesure, il vaudrait la peine de l'étudier plus en détail dans un avenir rapproché.

● (1615)

Pour ce qui est de la réputation en ligne, le Commissariat à la protection de la vie privée du Canada a récemment fait de la réputation l'une de ses priorités pour les prochaines années du point de vue de la protection de la vie privée. C'est ainsi qu'il a lancé l'an dernier une consultation pour déterminer s'il y avait une façon d'appliquer le droit à l'oubli au Canada. Les technologies Internet provoquent en quelque sorte une mutation temporelle en ce sens que des éléments d'information peuvent continuer d'exister même si le contexte qui a justifié au départ leur publication est chose du passé. Comme le disait si bien l'expert en sécurité Bruce Schneier il y a quelques années: « Nous sommes une espèce qui oublie des choses... Nous ne savons pas ce que cela signifie de vivre dans un monde où rien n'est oublié. »

Le droit à l'oubli a été institué par la Cour de justice de l'Union européenne en mai 2014. Dans ce jugement historique, la Cour a autorisé la suppression de renseignements personnels concernant les dettes passées d'un individu pour qu'il soit impossible d'y avoir accès via un moteur de recherche. Bien qu'il puisse sembler intéressant au premier coup d'oeil de pouvoir protéger ainsi la vie privée et la réputation des personnes, la question est plus complexe qu'elle ne paraît. En plus des contestations constitutionnelles que pourrait entraîner un tel droit à l'oubli, on court des risques considérables en confiant à des entités privées, comme les entreprises exploitant les moteurs de recherche, la tâche de trancher en ce qui a trait aux valeurs et aux droits fondamentaux des individus. Plusieurs critères devraient être pris en compte avant de pouvoir désindexer du contenu, ce qui rend l'exercice d'autant plus complexe. L'application de ce droit incomberait aux entreprises exploitant des moteurs de recherche, lesquelles seraient davantage tentées de supprimer le plus de contenu possible afin de réduire les coûts et les risques de poursuites juridiques.

Contrairement aux entités du secteur privé, les tribunaux ont l'expertise et l'indépendance nécessaires pour trouver le juste équilibre entre les deux valeurs fondamentales souvent mises en opposition par les requêtes de ce genre, à savoir la liberté d'information et d'expression, d'une part, et la protection de la vie privée, d'autre part. La Cour fédérale du Canada a récemment rendu un jugement à ce sujet dans l'affaire Globe24h, ce qui montre bien que c'est aux tribunaux qu'il devrait revenir d'ordonner que des éléments d'information soient mis à l'abri des recherches via Google.

La province de Québec a mis en place un cadre législatif très strict pour la protection de la vie privée et de la réputation. Le droit à la vie privée a été élevé au rang des droits fondamentaux protégés par la Charte québécoise des droits et libertés de la personne. Le Code civil du Québec protège le citoyen en interdisant que l'on utilise « son nom, son image, sa ressemblance ou sa voix à toute autre fin que l'information légitime du public ». Bien que les recours pour diffamation peuvent être impossibles dans les pays de common law lorsque les affirmations sont véridiques, le simple fait que les informations soient vraies ne suffit pas à éviter les responsabilités juridiques au Québec.

Cela étant dit, il y a encore certaines difficultés à surmonter pour régler toutes les questions liées à la réputation en ligne, et ce, même avec ce cadre juridique strict en place. Disons tout d'abord que le principe de l'autorité de la chose jugée pourrait empêcher que quelqu'un se présente devant le tribunal pour demander la suppression de certaines informations si une requête semblable a déjà fait l'objet d'un jugement. Il faut également revoir les délais de prescription de telle sorte que ce cadre juridique puisse adéquatement tenir compte du fait qu'avec Internet, des données publiées en toute légitimité peuvent devenir caduques après un certain temps ou, inversement, que des données d'abord considérées comme non pertinentes puissent le devenir avec le temps.

Par ailleurs, les poursuites juridiques peuvent être une avenue très onéreuse, tant et si bien que ce genre de recours n'est pas accessible à tous. Des efforts pourraient être déployés pour améliorer notre cadre juridique à ce chapitre. On pourrait notamment faciliter l'accès à la justice ou mettre en oeuvre un système de traitement accéléré pour les demandes de suppression d'information en ligne, plutôt que de chercher à copier la formule européenne du droit à l'oubli.

Enfin, le droit à l'oubli soulève des enjeux extraterritoriaux qui doivent être pris en considération. Dans son récent jugement, la Cour fédérale du Canada a lancé un important débat sur la portée d'application des lois visant la protection de la vie privée. Tous les yeux sont maintenant tournés vers la Cour suprême du Canada qui rendra sous peu sa décision dans l'affaire *Equustek c. Google*.

D'autre part, l'ancienne commissaire à la protection de la vie privée du Canada, Jennifer Stoddart, a demandé des pouvoirs d'application renforcés en vertu de la LPRPDE. Ainsi, le commissaire pourrait notamment émettre des ordonnances exécutoires et imposer des pénalités ou des dommages-intérêts. Dans les autres pays, les instances réglementaires privées disposent de pouvoirs semblables. Les entreprises canadiennes pourraient ainsi être davantage incitées à protéger les renseignements personnels en leur possession. Cela étant dit, j'aurais une réserve à exprimer à ce propos. Tel que mentionné précédemment, la LPRPDE est une loi neutre sur le plan technologique qui est fondée sur des principes de flexibilité. Cette flexibilité permet de s'adapter à de nouveaux types de technologie et de modèles d'affaires, mais elle a pour inconvénient de créer de l'incertitude. Il n'est pas toujours facile pour les entreprises de savoir comment elles doivent s'y prendre pour se conformer à la LPRPDE, surtout quand elles lancent de nouveaux produits ou services ou mettent en oeuvre des technologies novatrices. Si l'on ajoute à cette incertitude le risque de dommages-intérêts ou d'autres sanctions, je crains que certaines entreprises n'hésitent à lancer de nouveaux produits et services, ce qui aurait pour effet de freiner l'innovation et de miner les avantages concurrentiels que procure à notre pays sa démarche orientée vers la recherche, le développement et l'innovation.

● (1620)

À mon avis, les pouvoirs exécutoires, les pénalités et les dommages-intérêts ne devraient entrer en jeu qu'une fois qu'il a été clairement établi que la pratique est illégale et que l'organisation fautive a refusé d'apporter les correctifs nécessaires après avoir été avisée de la situation.

Je vous dirais en terminant que j'ai certaines inquiétudes quant à la vérification du statut d'adéquation dont le Canada fera l'objet au cours des prochaines années. Le Règlement général sur la protection des données de l'Union européenne qui entrera en vigueur en 2018 comprendra certains droits qui ne sont pas actuellement prévus dans la LPRPDE, dont notamment le droit à l'oubli et le droit à la portabilité des données.

Nous avons beaucoup de pain sur la planche si nous voulons nous assurer que notre régime de protection des données demeure pertinent dans les années à venir. Notre modèle actuel fondé sur des avis et des choix pose certaines difficultés qu'il conviendrait peut-être de régler en priorité.

J'ai rédigé des mémoires dans le cadre de la consultation menée par le Commissariat sur le consentement et en réponse à sa demande d'articles sur la protection de la réputation en ligne. Vous pouvez en prendre connaissance sur le site Web du Commissariat.

Je vous remercie et je me ferai un plaisir de répondre à vos questions.

Le président: Merci, madame Gratton.

Nous passons maintenant à M. Dickson pour un maximum de 10 minutes.

M. Robert Dickson (consultant, ancien commissaire à l'information et à la protection de la vie privée de Saskatchewan, à titre personnel): Bonjour à tous.

Mes observations vont porter principalement sur les quatre enjeux cernés par le commissaire à la protection de la vie privée dans la lettre qu'il a envoyée au Comité le 2 décembre 2016.

Je tiens d'abord et avant tout à m'assurer que la LPRPDE fonctionne mieux au bénéfice des PME. J'ai contribué à l'élaboration de la loi albertaine sur la protection des renseignements personnels. Je coprésidais un groupe de travail formé d'avocats spécialisés en protection de la vie privée qui conseillaient les gens chargés de rédiger cette loi. Les avocats participants étaient surtout guidés par leur volonté de tenir compte de la situation des PME. On considérait, tout au moins à l'époque, que la LPRPDE était davantage conçue en fonction de la réalité des grandes banques, des compagnies aériennes et des entreprises nationales que de celle de la librairie du coin.

Lorsque j'étais commissaire à l'information et à la protection de la vie privée de la Saskatchewan, nous avons mis en oeuvre de concert avec le Commissariat à la protection de la vie privée du Canada un programme pilote visant à faciliter la tâche des entreprises des Prairies pour ce qui est de la protection de la vie privée. Nos rencontres avec des dirigeants de PME nous ont permis de constater qu'ils étaient remarquablement peu nombreux à se conformer à la LPRPDE. Je dois même vous dire, ce qui est plutôt décevant, qu'ils étaient aussi très nombreux à ne pas très bien connaître la loi.

Parlons d'abord des pouvoirs d'exécution. Je conviens avec le commissaire que l'on devrait lui donner le pouvoir de rendre des ordonnances. Son bureau se retrouverait ainsi sur le même pied que la plupart des grandes instances internationales chargées de la protection des données ainsi que les provinces canadiennes qui ont adopté des lois pour la protection des renseignements personnels dans le secteur privé.

Je dois reconnaître que le modèle actuel de l'ombudsman fonctionne plutôt bien pour les grandes entreprises canadiennes qui se conforment à la LPRPDE dans une large mesure. Cette situation est peut-être attribuable aux capacités accrues dont ces entreprises disposent et au fait qu'elles comprennent mieux que le respect des règles visant la protection de la vie privée est une saine pratique de gestion.

À ce sujet, je vous signale qu'une étude menée en 2010 par le commissaire à la vie privée du Canada a conclu que la taille relative des entreprises déterminait dans quelle mesure elles peuvent être touchées par les actions du Commissariat en observant notamment que les PME sont généralement plus sensibles aux risques financiers et aux sanctions. On notait en outre que l'effet dissuasif d'une éventuelle intervention du Commissariat s'exercerait encore davantage sur les PME si le commissaire disposait du pouvoir de rendre des ordonnances et d'imposer des sanctions pécuniaires.

Le pouvoir de rendre des ordonnances m'apparaît également souhaitable du fait qu'il permet de compter sur un bassin de décisions qui sont mieux étayées que les sommaires actuellement fournis par le Commissariat. Ainsi, les entreprises sauraient mieux à quoi s'en tenir quant à la façon dont la LPRPDE doit être interprétée et observée.

Par ailleurs, il me semble préférable, dans la perspective du commerce international, qu'il y ait harmonisation avec le Règlement général sur la protection des données. Dans ce contexte, je vous dirais toutefois qu'il ne faut surtout pas perdre de vue les lois sur la protection des renseignements personnels dans le secteur privé de l'Alberta, de la Colombie-Britannique et du Québec, ainsi que les lois sur la protection de l'information sur la santé qui sont considérées comme étant essentiellement similaires en Ontario, à Terre-Neuve-et-Labrador, au Nouveau-Brunswick et dans les autres provinces où elles obtiendront bientôt cette désignation. Tout changement apporté à la LPRPDE exigera une révision parallèle pour s'assurer que ces lois provinciales et territoriales demeurent essentiellement similaires.

Je serais porté à croire que les concepts de portabilité des données et de protection de la vie privée dès la conception sont déjà pris en compte dans la LPRPDE. Il ne semble cependant pas que ce soit le cas pour ce qui est de l'effacement des données.

En ce qui concerne la protection de la réputation, je ne suis pas favorable au droit à l'oubli. Je ne crois tout simplement pas qu'un tel droit pourrait résister à une contestation en vertu de la Charte.

Dans mon ancien rôle de commissaire, j'étais très préoccupé par la question des registres publics créés longtemps avant que l'on ait à s'inquiéter d'enjeux comme le profilage, le couplage de données et le vol d'identité. À ce titre, il faut favoriser un contrôle plus étroit au moment de la cueillette des renseignements pour ces registres en veillant à ce que l'on ne consigne aucune donnée qui ne serait pas essentielle aux fins du registre.

● (1625)

Je me souviens que Chantal Bernier a mené, lorsqu'elle était commissaire adjointe à la protection de la vie privée du Canada, une initiative conjointe avec ses homologues provinciaux en vue d'établir un ensemble de directives traitant de la publication des décisions des tribunaux administratifs sur Internet. Il y a donc assurément un problème à régler, mais je ne suis tout simplement pas convaincu que le droit à l'oubli soit la solution.

Je pense que nous avons en quelque sorte les mains liées par les prescriptions de la Charte en matière de liberté d'expression. Si vous ne pouvez pas obliger un organe d'information à supprimer du contenu, alors je vous soumets que vous ne pouvez pas non plus empêcher l'exploitant d'un moteur de recherche de dire à tout le monde que ce contenu existe.

En ce qui a trait maintenant au consentement valable, je vous dirais que l'on a pu tirer certains enseignements fort utiles de l'expérience canadienne avec les dossiers de santé électroniques au titre desquels la nécessité d'un consentement a perdu énormément de terrain, et ce, malgré le fait que ces dossiers renferment des informations parmi les plus délicates et les plus potentiellement préjudiciables qui soient pour les Canadiens. Je pense notamment à la situation en Alberta et en Saskatchewan où on a presque complété la mise en place d'un système de dossiers de santé électroniques pour tous les citoyens. Ainsi, des milliers de fournisseurs dans toutes les régions de ces provinces peuvent consulter, et ce, pour n'importe quel citoyen, les profils de consommation de médicaments sur ordonnance, les résultats des tests en laboratoire, les rapports d'imagerie diagnostique, les rapports de radiologie, les notes cliniques des pourvoyeurs de soins dans les hôpitaux et les informations sur l'immunisation. Il va de soi qu'une telle consultation n'est autorisée que si elle répond à un besoin légitime aux fins d'un diagnostic, d'un traitement ou de soins, mais le fait demeure que ces gens-là peuvent avoir accès à toute cette information. Grâce au financement fourni par l'Inforoute Santé du Canada, toutes les autres provinces s'emploient à mettre en place un système semblable qui sera relié à tous ses équivalents provinciaux et territoriaux.

Les 10 dernières années nous ont assurément appris que, parallèlement à la question du consentement, il fallait absolument prendre d'autres mesures pour améliorer la protection de la vie privée. En tête de liste, je recommande la création d'un programme de gestion pour assurer une approche coordonnée aux fins de l'application de la LPRPDE. En effet, nous constatons trop souvent que les fournisseurs de soins de santé fonctionnent de façon fragmentée avec l'adoption de politiques à gauche et à droite sans qu'il y ait vraiment de coordination et de leadership. Il serait donc important de pouvoir compter sur un programme de gestion pour la protection de la vie privée.

Nous aurions aussi besoin d'un programme de vérification proactive dont tous les employés connaîtraient l'existence. Trop souvent, des organisations se targuent de disposer d'une capacité de vérification grâce au système électronique qu'elles ont mis en place. Une telle capacité n'est pas vraiment utile en l'absence d'un programme permanent de vérification proactive dont tous les employés ayant accès aux informations confidentielles connaissent l'existence.

Nous avons aussi besoin d'une capacité de surveillance réglementaire renforcée, tant dans les commissariats qu'au sein des instances de réglementation.

Nous pourrions parler pendant des heures de l'expansion de l'utilisation secondaire des renseignements sur la santé et des mégadonnées. Dans le cas des informations permettant d'identifier un patient, on a toujours considéré qu'un consentement additionnel n'était pas requis si l'information est utilisée aux fins prévues au départ, à savoir l'établissement d'un diagnostic, un traitement ou des soins. Par contre, si l'information doit servir à des fins de recherche, il faut normalement obtenir le consentement exprès du patient, à moins qu'un conseil d'éthique n'ait approuvé la recherche en indiquant que ce consentement n'était pas nécessaire.

Il y a des problèmes importants qui se posent à ce chapitre, d'où la nécessité d'appliquer des mesures de protection rigoureuses.

Contrairement à l'Australie où les patients doivent choisir d'adhérer ou non au système de dossiers de santé électroniques My Health Record, la participation est obligatoire pour tous les Canadiens qui voient les renseignements sur leur santé être automatiquement versés dans le système. On ne leur demande pas s'ils y consentent. Notre système des dossiers de santé électroniques est fondé sur le consentement implicite, plutôt que sur le consentement exprès. En outre, le consentement implicite exige généralement une certaine transparence au moment de la cueillette de l'information. On doit en effet indiquer au patient quels types de renseignements sur sa santé seront consignés et comment ces renseignements seront utilisés et communiqués. Dans une formule de consentement implicite, l'individu devrait normalement avoir l'option de participer ou non au programme. La forme de masquage offerte dans le système de dossiers de santé électroniques que nous mettons en place au Canada assure généralement aux patients une forme de protection bien différente et certes moins solide qu'une possibilité de refus de consentement.

● (1630)

Comme nous avons pu le constater au cours des 10 dernières années, la protection de la vie privée des patients est souvent renforcée au moyen de différentes mesures indirectes, y compris un serment de confidentialité par tous les travailleurs du secteur de la santé; des politiques et des procédures écrites régissant la cueillette, l'utilisation et la communication de données personnelles sur la santé; la formation du personnel; et une piste de vérification ciblant tous ceux qui ont accès aux renseignements sur la santé.

Il faut toutefois constater que ces mesures indirectes de protection n'ont pas su empêcher une émergence des cas d'indiscrétion. Vous êtes déjà au courant du fait qu'il y a actuellement, si je ne m'abuse, des recours collectifs en instance dans au moins cinq provinces canadiennes à l'égard de situations où des personnes non autorisées ont consulté les renseignements personnels sur la santé de différents patients. Dans ce contexte, on cherche plus que jamais à mettre en place des mesures de protection plus rigoureuses pour appuyer ces mesures indirectes.

Je recommanderais donc que, si vous envisagez — comme le commissaire vous a invité à le faire — des solutions de rechange ou des améliorations possibles à la formule de consentement, vous considériez la mise en place de mesures de protection rigoureuses comme celles qui ont été conçues pour les dossiers de santé électroniques. Il est notamment question de renvois motivés ou d'autres mesures disciplinaires de la part des employeurs, de poursuites et d'amendes — qui sont très élevées dans le cas des lois régissant expressément l'information sur la santé —, de recours collectifs et de mesures disciplinaires imposées par les instances de réglementation des professions.

Pour ce qui est du consentement et des solutions de rechange possibles, je crois que la gestion actuelle des dossiers de santé électroniques au Canada pourrait vous fournir de précieux enseignements.

Merci beaucoup, monsieur le président.

Le président: Merci beaucoup.

Chers collègues, nous avons entendu quatre témoins et nous avons déjà eu droit à différents points de vue qui semblent contradictoires... Cette étude s'annonce intéressante.

Je suis désolé; je ne devrais pas commenter, mais j'essaie simplement de voir clair dans tout ce que vous venez de nous dire, monsieur Dickson, et je me dis que si tout cela est vrai, notre étude ne va pas manquer de mettre au jour un grand nombre de problématiques.

Sans plus tarder, je vais maintenant laisser la parole à mes collègues du Comité.

Monsieur Massé, vous avez sept minutes.

● (1635)

[*Français*]

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

D'abord, je tiens à vous remercier de votre participation aux travaux importants du Comité.

J'avais une série de questions, mais, madame Bernier, vous avez attiré mon attention sur un élément particulier que vous jugez urgent d'aborder. Vous avez parlé de la préservation de l'adéquation de la Loi au règlement général européen sur la protection des données. Vous avez dit que le Canada est le seul État nord-américain bénéficiant du statut d'adéquation face à l'Europe, mais que ce statut est à risque, étant donné que l'examen doit être fait tous les quatre ans. Vous dites qu'il faut rehausser la loi canadienne au niveau nécessaire, afin de préserver l'avantage que présente, pour les entreprises canadiennes, l'adéquation avec l'Europe.

Quelles mesures recommandez-vous qu'on prenne pour rehausser la loi canadienne?

Me Chantal Bernier: Malheureusement, il faut prendre des mesures législatives. Je dis « malheureusement », parce que l'effort législatif est le plus grand effort.

Comme M[e] Gratton l'a mentionné, le nouveau règlement européen prévoit le droit à l'effacement. Or la loi canadienne est silencieuse là-dessus. Le nouveau règlement européen prévoit aussi la portabilité des données, c'est-à-dire qu'un consommateur aura le droit d'exiger que ses données qui sont sous la garde d'une organisation *x* soient transférées, s'il veut commencer à travailler pour une autre organisation ou être le consommateur ou le client d'une autre entreprise.

M. Rémi Massé: Cela se fera-t-il avec ou sans le consentement des individus concernés?

Me Chantal Bernier: Supposons que je fasse affaire avec l'organisation *x* et que je veuille maintenant m'adresser à un compétiteur. Je vais avoir le droit de dire à l'organisation *x* de transporter mes données auprès de l'organisation *y* avec laquelle je vais dorénavant être en relation commerciale.

J'ai un autre exemple. Dans certains cas, des évaluations des facteurs relatifs à la vie privée vont être exigées avant de mettre en oeuvre une pratique ou un programme. Il y a toute une série de nouveaux droits créés dans ce règlement qui n'existent pas dans la loi fédérale. Je me permets de parler franchement: l'Union européenne a appris de ses erreurs. En effet, l'Europe avait peut-être accordé l'adéquation de façon un peu aléatoire. À présent, le nouveau règlement prévoit des critères plus stricts, et il faut donc se conformer au droit européen.

Dans le cadre de l'examen de la loi canadienne qui sera fait, on va donc étudier la LPRPDE pour déterminer si elle correspond aux niveaux désirés pour avoir le caractère adéquat. Si la réponse est non, cela veut dire que nos compagnies canadiennes, pour recevoir des renseignements de compagnies européennes — et cela inclut quelque chose d'aussi simple que d'avoir un site Web auquel les Européens peuvent accéder —, vont être obligées de soit négocier des clauses modèles, qui sont des clauses vraiment très contraignantes, très lourdes, qui sont approuvées par la Commission européenne, soit négocier des règles d'entreprise contraignantes, qui sont des règles internes, soit obtenir le consentement individuel, qui n'est pas facile à obtenir dans le cas de chaque transaction.

Le Canada a l'adéquation, alors que les États-Unis ne l'ont pas. Ils viennent de négocier le Privacy Shield pour cela, mais c'est un espace juridique, ce n'est pas un espace territorial. Le Mexique ne l'a pas non plus. Cela nous donne un avantage concurrentiel que, il me semble, nous ne voudrions pas perdre.

M. Rémi Massé: Merci, c'est fort apprécié.

Je vais maintenant aborder le domaine du consentement, parce que c'est un problème qui nous interpelle davantage. Je vais m'adresser à M. Lawford ou à Mme Lau.

La LPRPDE exige évidemment que les organisations obtiennent le consentement des individus pour recueillir, utiliser ou communiquer de l'information. Dans l'environnement numérique et d'information dans lequel on vit, les Canadiens fournissent leur consentement à plusieurs organisations. Ils accordent leur consentement pour que soient recueillis, utilisés ou communiqués des renseignements personnels.

J'aimerais connaître votre avis au sujet de ces situations au cours desquelles les Canadiens, peut-être par automatisme, pour pouvoir utiliser un logiciel, pour pouvoir utiliser un outil, apposent rapidement un crochet dans la petite boîte à cet effet. J'aimerais recevoir vos commentaires à ce sujet et connaître votre opinion quant à la manière d'aborder cette question pour aider à protéger les renseignements personnels des Canadiens et des Canadiennes.

● (1640)

M. John Lawford: Actuellement, au Centre pour la défense de l'intérêt public, nous étudions des façons possibles de régler ce problème.

Comme je l'ai dit dans ma présentation orale, nous avons pensé à des paramètres standards pour nous assurer que, dès que les gens visitent un site, qu'il s'agisse de médias sociaux ou d'autres, ils se voient offrir toujours les mêmes choix, si possible. C'est une idée.

Nous travaillons aussi à la préparation d'un rapport afin de trouver les moyens de présenter les choix beaucoup plus clairement, de façon à ce que cela demande moins d'efforts aux petits et aux grands, surtout aux gens qui ont accès à des services au moyen d'applications.

Il y a donc des gestes à poser pour améliorer la situation. Cela dit, nous avons toujours des problèmes en ce qui a trait au consentement informé et valide dans ce domaine, mais, selon moi, ce n'est pas une raison pour abandonner la partie. Le principe est bon, et nous ne devons pas jeter le bébé avec l'eau du bain.

M. Rémi Massé: Merci, monsieur Lawford.

Madame Gratton, vous avez aussi piqué ma curiosité lorsque vous avez fait référence aux dispositions en vigueur au Québec. Vous avez utilisé certains qualificatifs pour expliquer qu'il y a des dispositions intéressantes.

Je ne suis pas avocat, mais j'aimerais vous entendre parler des mesures que le Québec a mises en place et dont nous devrions nous inspirer pour élaborer nos recommandations.

Me Éloïse Gratton: Oui, absolument.

Il s'agit de protection de la réputation et de la vie privée. Au Québec, le droit à la vie privée est protégé par la Charte des droits et libertés de la personne, qui s'applique aux entreprises du secteur privé. Le Code civil comprend également des dispositions en matière de droit à la réputation et à la vie privée.

À la base, il y a l'interdiction de publier ou de diffuser sans consentement certains renseignements personnels d'un individu, par exemple son nom ou sa photo. Le principe de base est le consentement de l'individu, à moins que l'information ne soit d'intérêt public.

Si l'information est diffusée, ce sont les tribunaux, en l'occurrence les juges, qui prennent connaissance de la publication en vue de déterminer notamment si cette information était d'intérêt public à ce moment précis. Enfin, ils mettent dans la balance la liberté d'expression et d'information, d'un côté, et la protection de la vie privée et de la réputation, de l'autre côté.

Certaines décisions remontent à plus de 100 ans. Il est intéressant d'observer comment ont évolué les choses au fil des ans. On voit ce qui est d'intérêt public et ce qui ne l'est pas, ce qui passe et ce qui ne passe pas. En matière de réputation, je voulais faire valoir un dernier point, à savoir que ce n'est pas parce que des informations sont vraies qu'elles peuvent être publiées. Pour que ce soit d'intérêt public, on retourne au test de légitimité.

Il reste que, malgré ce régime, il y a deux enjeux en matière de droit à l'oubli ou droit à l'effacement.

Le premier enjeu est la chose jugée, ou *res judicata*. Supposons que mes renseignements personnels soient publiés et que j'aie recours aux tribunaux pour que ce soit évalué. La décision pourrait être différente dans 10 ans, mais le tribunal pourrait déclarer la chose jugée, c'est-à-dire qu'il a déjà statué sur cet enjeu. Je me dis que, pour évoluer dans ce cadre juridique et aborder les problèmes en matière de réputation en ligne, il faut garder cela en tête.

L'autre problème est évidemment...

[*Traduction*]

Le président: Madame Gratton, nous avons dépassé de plusieurs minutes le temps alloué à M. Massé. J'attendais une pause pour intervenir, mais il n'y en a pas eue. Il faudra attendre pour avoir l'occasion de compléter votre réponse plus tard.

Nous passons à M. Kelly.

[*Français*]

Me Éloïse Gratton: D'accord.

[*Traduction*]

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

J'aimerais d'abord, monsieur Dickson, porter mon attention sur une portion de vos observations préliminaires. Vous avez parlé de vérifications de la conformité — et je ne sais plus trop si c'était en Saskatchewan ou en Alberta — qui ont permis de constater que très peu d'entreprises se conformaient à la LPRPDE et même que très peu connaissaient bien cette loi. C'est un constat qui ne m'étonne guère.

Il est bien certain que le fait de ne pas se conformer à des pratiques ou protocoles d'application obligatoire peut être problématique, mais j'aimerais savoir si vous avez mis au jour des cas d'atteinte à la vie privée de façon généralisée, et des preuves de torts causés à des Canadiens en raison du non-respect de la LPRPDE.

● (1645)

M. Robert Dickson: Pour que les choses soient bien claires, disons d'abord que c'est en Saskatchewan que nous avons effectué ces vérifications. La Saskatchewan n'a pas de loi sur la protection des renseignements personnels; la province est totalement assujettie à la loi fédérale.

Je dois préciser d'entrée de jeu que ce projet pilote lancé par le commissaire à la protection de la vie privée du Canada en partenariat avec mon bureau ne visait pas expressément à déterminer qui se conformait ou non avec la loi. On cherchait surtout à voir si des actions pouvaient être entreprises pour évaluer dans quelle mesure les gens connaissaient la loi et s'y conformaient, le tout dans le but d'élaborer des stratégies afin de rectifier le tir, le cas échéant.

Chantal n'a pas joué un rôle direct dans ce projet qui a été réalisé à l'époque par le commissariat fédéral. Force est d'admettre qu'il y a eu quelques problèmes avec le processus, si bien que le projet pilote n'a pas abouti à un rapport final.

Nous avons certes pu constater que certaines organisations n'avaient pas nommé d'agent chargé de la protection de la vie privée, pas plus qu'elles n'avaient mis en place les politiques et les procédures nécessaires pour que leur personnel assure bel et bien la protection de la vie privée. C'est ce que devrait faire toute organisation pour satisfaire aux exigences de la loi.

Je ne sais pas si je réponds bien à votre question, mais il ne s'agissait pas pour nous de recenser les gens qui contrevenaient à la loi. Nous rencontrions des groupes pour essayer de déterminer dans quelle mesure ils connaissaient bien la loi. Nous avons conclu que la loi n'était pas suffisamment connue et qu'il fallait que ces gens-là aient accès à des mesures de soutien et à des ressources pour pouvoir se conformer à la loi.

M. Pat Kelly: Je ne suis pas étonné que vous ayez pu observer dans une petite entreprise comptant par exemple une dizaine d'employés que l'on ignorait qu'il fallait désigner un agent chargé de la protection de la vie privée devant accomplir certaines fonctions pour se conformer à la loi.

Ce que j'aimerais vraiment savoir, mais que vous ne m'avez pas dit, ne serait-ce qu'en fonction d'observations isolées, car vous avez indiqué qu'il n'y avait pas eu de rapport final, c'est si vous avez pu dégager des éléments montrant que des torts ont été causés aux clients de ces petites entreprises. Avez-vous vu des preuves indiquant qu'il y aurait eu atteinte à la vie privée de certains clients?

M. Robert Dickson: Comme nous ne traitions pas vraiment avec les clients — ce sont les représentants des organisations que nous rencontrions —, les organisations n'ont pas été nombreuses à prendre les devants et...

M. Pat Kelly: Vous avez indiqué au départ que vous vous intéressiez surtout aux PME.

M. Robert Dickson: Oui, c'est vrai.

M. Pat Kelly: Ce sont des responsables de petites entreprises que vous avez rencontrés?

M. Robert Dickson: Exactement. Nous avons constaté d'une manière générale — car il y avait certaines exceptions, comme vous pouvez vous en douter — que le niveau de connaissance de la LPRPDE était incroyablement faible et que ces entreprises n'avaient aucune idée des mesures à prendre pour s'assurer de ne recueillir que le strict minimum de renseignements requis aux fins de leurs activités, de ne pas conserver les renseignements personnels plus longtemps que nécessaire, et toutes sortes de choses semblables.

Nous avons découvert que ces règles n'étaient pas respectées.

● (1650)

M. Pat Kelly: Mais je reviens à ma question. Vous ne savez pas si des torts ont été causés en raison du non-respect...

Peut-être devrais-je permettre à votre collègue de répondre. M. Dickson ne semble pas...

Me Chantal Bernier: Bien sûr.

Une des enquêtes qui me vient à l'esprit portait sur une nouvelle entreprise qui vendait des produits quelconques sur le Web. Les entrepreneurs étaient manifestement emballés par leur démarrage d'entreprise et n'ont pas pensé au respect de la vie privée. Ils s'intéressaient principalement à devenir une entreprise intéressante sur le Web, jusqu'à ce qu'un de leurs clients se plaigne d'avoir été fraudé de milliers de dollars. Les entrepreneurs n'ont pas trouvé la faille. Plus tard, un autre client a dit avoir été fraudé. Tout le monde a donc retracé la source du problème jusqu'à eux, qui étaient coupables, bien entendu.

Il y a des tonnes d'exemples du genre. En fait, de nombreuses grandes entreprises vous diront que les PME de leur chaîne d'approvisionnement représentent leur maillon le plus faible. C'est là où une grande partie de l'attention est dirigée.

Pour répondre à votre question, les gens subissent bel et bien des préjudices.

M. Pat Kelly: Très bien. Excellent.

Le président: Il vous reste environ une minute.

M. Pat Kelly: Je doute que nous puissions vraiment aborder un sujet important en une minute, mais je vais simplement vous lancer la question. J'ignore si vous aurez le temps d'y répondre, mais pourriez-vous établir des distinctions entre un consentement éclairé et un consentement implicite?

Nous en avons beaucoup parlé. Dans toute entreprise, en particulier dans une petite entreprise, il est difficile, à un point de vente ou au moment de diffuser l'information pouvant entraîner une vente, de se conformer aux exigences de la loi tout en donnant au client ce qu'il veut, à savoir des renseignements.

Ce sera peut-être pour le prochain tour...

Le président: Quand je vous dis qu'il vous reste une minute pour poser une question et que vous parlez pendant une minute, vous épuisez votre temps de parole.

Des députés: Ah, ah!

Le président: Monsieur Blaikie.

M. Daniel Blaikie (Elmwood—Transcona, NPD): Je suis conscient que vous êtes tous ici en tant que spécialistes de la protection de la vie privée, et non pas comme spécialistes du commerce, mais nous venons de voter en troisième lecture sur l'accord économique et commercial global, ou AECG. L'accord est censé éliminer les barrières commerciales non tarifaires entre le Canada et l'Europe, et donner une certaine assurance aux entreprises canadiennes voulant qu'elles ne rencontrent pas les mêmes difficultés qu'auparavant, lorsqu'elles font des échanges commerciaux avec des entreprises européennes.

Puisque je suis le seul membre du Comité qui a voté contre l'entente, j'aimerais que vous nous parliez des enjeux considérables entourant les barrières commerciales non tarifaires qui ne sont pas abordées dans l'AECG.

Pouvez-vous nous parler davantage de ce qui manque à cet accord? Comment faire pour éviter que les entreprises canadiennes perdent leur avantage actuel, même si le Canada vient de signer un accord censé faciliter les échanges commerciaux avec l'Europe?

Me Chantal Bernier: La seule façon de les protéger est la suivante: au moment où l'Europe déterminera le caractère adéquat du Canada, nous devrons avoir renforcé nos mesures de protection de la vie privée à un niveau convenable. Cela ne veut pas dire que nous devons atteindre exactement le même niveau, mais bien que les Européens doivent le trouver adéquat. Sinon, chaque fois que nous voudrons faire affaire avec l'Europe — un marché de 500 millions d'habitants qui ont de l'argent, de sorte que nous avons besoin de cet avantage concurrentiel —, nous devrons composer avec des dispositions très exigeantes.

La réponse à votre question revient à ce que j'ai dit à M. Massé: nous devons renforcer la loi maintenant pour qu'elle réponde aux critères après 2018.

Me Éloïse Gratton: Puis-je ajouter quelques mots?

La Loi québécoise sur la protection des renseignements personnels est considérée comme étant sensiblement similaire à la Loi sur la protection des renseignements personnels et les documents électroniques, ou LPRPDE. Cette loi québécoise est en vigueur depuis 1993, et elle est probablement la plus sévère en la matière au Canada. Or, l'Europe a examiné notre loi en 2014, mais ne l'a pas jugée adéquate — des questions demeuraient. Je m'interroge donc sur la pertinence de l'évaluation ou de la méthodologie employée en Europe.

Il va sans dire que nous aimerions idéalement respecter les critères européens, mais j'ai encore des réserves à ce chapitre.

M. Daniel Blaikie: Merci beaucoup.

Madame Bernier, vous avez dit que si le commissaire avait le pouvoir d'imposer des amendes, il serait logique que celles-ci soient établies en fonction des recettes globales de l'entreprise.

Vous avez ensuite brièvement abordé la question des bénéfices. Par souci de clarté, parlez-vous d'un pourcentage des bénéfices ou des recettes?

● (1655)

Me Chantal Bernier: En fait, si nous respectons le modèle européen, il s'agit des recettes annuelles. Le président a dit que les points de vue étaient divergents, mais je crois qu'il y a une certaine harmonie entre nos propos. Mme Gratton dit qu'il faut prendre en compte la situation de l'organisation. Gary Dickson a dit que les PME sont plus sensibles aux amendes. Je trouve plus équitable d'employer un pourcentage, puisque cela évite de coller une amende d'un million de dollars à une petite entreprise. Un pourcentage correspondrait donc à la gravité de l'infraction et serait plus équitable dans les faits.

M. Daniel Blaikie: La prochaine question s'adresse à nos amis du Centre pour la défense de l'intérêt public. Pouvez-vous mieux nous expliquer vos propos sur l'adoption d'une loi distincte ou sur l'élargissement de la portée de la loi en place pour qu'elle cible plus particulièrement les droits des enfants à la vie privée?

Par exemple, comment pensez-vous qu'une loi pourrait encadrer les sites Web que les enfants consultent? Selon vous, comment pourrions-nous cibler les préoccupations et les activités en ligne propres aux enfants?

M. John Lawford: Notre proposition ne vise pas à cibler des sites particuliers. Elle repose plutôt sur l'ajustement de la notion du consentement. Comme vous le savez, il est interdit aux États-Unis de demander l'identité des enfants de moins de 13 ans, ce qui devrait aussi être la norme au Canada. Ce n'est toutefois pas prévu à la loi. Compte tenu de son règlement général sur la protection des données, l'Europe exigera désormais le consentement des parents jusqu'à l'âge de 16 ans dans la plupart des cas.

Toutes sortes de recherches en sciences sociales ont été réalisées sur le sujet, sur la maturation du cerveau chez l'adolescent et sur le moment à partir duquel les jeunes comprennent suffisamment pour donner un consentement valide. Cela ressemble au consentement à des traitements médicaux. Nous pourrions essentiellement adopter de telles règles générales pour protéger les adolescents de moins de 16 ans contre la distribution de leurs renseignements personnels à une tierce partie, par exemple. Nous avons publié un document sur ce thème, qui s'intitule « All in the Data Family » et qui se trouve sur notre site Web. On y expose une de nos propositions.

En dernier lieu, dans le cas des enfants qui ont donné leur consentement avant d'atteindre la majorité, nous proposons également de leur offrir le choix, lorsqu'ils ont 18 ou 19 ans, selon la province, d'autoriser ou non l'entreprise ayant recueilli l'information à continuer de l'utiliser. C'est ce que nous appelons la carte « Vous êtes libéré de prison ». Le Comité pourrait y réfléchir.

Voilà le genre de propositions que nous envisageons.

M. Daniel Blaikie: Merci beaucoup.

Le président: Vous avez encore une minute.

M. Daniel Blaikie: Oh, c'est tout? Eh bien, je vais m'arrêter ici dans ce cas.

Le président: Merci beaucoup, monsieur Blaikie. Je vous en suis reconnaissant.

Nous allons maintenant terminer la série de questions de sept minutes avec M. Saini. Allez-y, s'il vous plaît.

M. Raj Saini (Kitchener-Centre, Lib.): Je remercie infiniment tous les témoins d'être avec nous aujourd'hui. Vous nous avez donné beaucoup d'information.

Madame Gratton, vous avez écrit quelque chose dans votre mémoire sur le fait de changer les normes sociales, de conserver la neutralité technologique et de veiller à ne pas modifier la LPRPDE. Vous citez un passage:

[*Français*]

« Ne légiférer qu'en tremblant ».

[*Traduction*]

Cette citation provient de M. Carbonnier, un juriste qui a tenu ces propos en 2001, il y a maintenant 16 ans.

En 2001, je doute qu'il ait pu anticiper tous les changements technologiques à venir et la rapidité de l'explosion technologique. Si vous croyez qu'il ne faut pas régler les problèmes relatifs à la vie privée au moyen de la LPRPDE, proposez-vous un autre mécanisme à cette fin? Quand il est question de la technologie, nous ignorons ce qui va se produire d'ici deux ans, ou même d'ici cinq ans, tout comme le juriste n'aurait pas pu imaginer il y a 16 ans ce qui se passerait aujourd'hui.

Me Éloïse Gratton: Sa citation est valable aujourd'hui encore. Ce qu'il voulait dire, c'est que vous réglez des problèmes lorsque vous adoptez des lois. Or, les mesures ont un caractère permanent et sont moins flexibles. Voilà pourquoi je trouve que sa citation est toujours pertinente aujourd'hui.

La LPRPDE est souple. Si nous voulons adopter un modèle de consentement, n'y changeons rien. Nous pouvons faire tout ce que nous voulons en périphérie. Nous pourrions nous servir de l'interprétation, ou bien obtenir des orientations stratégiques du Commissariat à la protection de la vie privée, ou CPVP. C'est pour cette raison que j'ai cru bon de mentionner ses propos, qui sont pertinents aujourd'hui encore.

M. Raj Saini: Mon autre question porte sur un sujet que nous avons abordé dans une autre étude, et dont nous discutons maintenant en ce qui concerne la LPRPDE, à savoir la conservation et la destruction des données. Puisque nous sommes en début d'étude, il est intéressant d'en parler maintenant pour orienter la suite des choses.

Je m'adresse à tous les témoins. Selon vous, quelle devrait être la norme? Le modèle européen est-il meilleur, ou est-ce plutôt celui des Américains qui est préférable? Quelles mesures pouvons-nous mettre en place pour conserver les données des gens de façon sécuritaire? De plus, une fois que les données ne sont plus nécessaires, devrait-on prévoir une échéance pour leur destruction?

● (1700)

Me Éloïse Gratton: Il devrait bel et bien y avoir une échéance. Cela dit, les organisations ont parfois besoin de conserver des données afin de prévenir les risques. Puisqu'une entreprise pourrait être poursuivie, elle doit garder l'information pendant un certain temps. Ne l'oubliez pas. Il y a aussi toutes sortes de lois qui s'appliquent à différents types de données.

En fait, il peut être extrêmement complexe pour une organisation de se doter d'une politique de conservation détaillée, ce qui peut être très cher. Quoi qu'il en soit, je suis tout à fait en faveur de la conservation des données et de la fixation d'échéances raisonnables qui tiennent compte du fait que les données ne sont plus utilisées. Il faut s'en débarrasser et les détruire.

M. John Lawford: J'ajouterais que dans bien des discussions sur le droit à l'oubli, que nous appelons le « droit à l'effacement », je pense qu'il est souvent question de retirer les renseignements sur les consommateurs des bases de données de marketing à l'avenir. C'est vraiment la nature du droit sur lequel les Européens se concentrent. Ils s'attardent beaucoup moins à retirer des informations de Google. Or, les gens sont tannés de recevoir des publicités en fonction de leurs préférences d'il y a 20 ans. Il est souvent question d'ajouter à la loi ce droit à l'effacement. À l'heure actuelle, les politiques de protection de la vie privée ne prévoient toutefois rien de tel.

Nexopia, l'entreprise dont je parlais, n'avait aucune politique en matière de conservation. Personne ne savait combien de temps elle comptait conserver les renseignements personnels, ce qui est une source de conflits.

Vous devriez bel et bien adopter une politique de conservation plus précise, qui devra toutefois être appuyée par le droit de retirer ses données dans les limites de la constitutionnalité, de la liberté d'expression et de tout ce que les gens ont mentionné.

M. Robert Dickson: J'aimerais simplement ajouter que lorsque j'étais en Saskatchewan, où je surveillais les administrateurs de la santé et leur gestion des renseignements personnels sur la santé, j'étais surpris de constater à quelle fréquence des dossiers médicaux inactifs étaient laissés dans des entrepôts et des bureaux abandonnés. Des fournisseurs de soins de santé ont pris leur retraite ou ont quitté leur poste pour d'autres raisons sans jamais disposer correctement des dossiers. Ce qui pose problème, c'est que les dossiers médicaux abandonnés n'étaient souvent plus actifs et auraient dû être détruits. Il aurait dû y avoir un calendrier de conservation des dossiers. Voilà qui m'a fait comprendre l'importance et l'intérêt non seulement d'avoir un calendrier adéquat sur la conservation des dossiers, mais aussi de le suivre et de détruire les dossiers qui n'ont plus leur raison d'être dans les meilleurs délais. C'est un enjeu de taille au Canada, surtout dans le cas des dossiers médicaux, car les médecins prennent leur retraite sans avoir disposé convenablement des dossiers au moment opportun.

M. Raj Saini: Est-ce que quelqu'un d'autre souhaite intervenir? Non? D'accord.

Me reste-t-il du temps?

Le président: Vous avez deux minutes.

M. Raj Saini: Deux minutes?

J'aimerais aborder une autre question qui a été soulevée, à savoir la publicité comportementale en ligne dont vous avez parlé.

Le CPVP a déclaré qu'il s'agit d'un objectif commercial légitime. La pratique doit toutefois être fondée sur un modèle de consentement qui correspond à la sensibilité de l'information. Par conséquent, comment pouvons-nous déterminer ce qui est sensible et ce qui ne l'est pas? À quoi le seuil correspond-il? Pourriez-vous nous donner des conseils à ce chapitre?

Me Chantal Bernier: Je pourrais vous donner une petite leçon d'histoire sur le cheminement du CPVP. La première enquête relative à la publicité comportementale en ligne a été menée en 2009 et portait sur Facebook. Le CPVP a alors déclaré que puisque Facebook est une plateforme gratuite, ses utilisateurs doivent s'attendre à recevoir de la publicité étant donné que c'est la seule source de revenu de l'entreprise. Il fallait donc prendre en compte ce modèle commercial dans l'interprétation des dispositions sur la protection de la vie privée. Tant que Facebook ne divulgue pas les renseignements personnels à des tiers et qu'il n'utilise l'information que pour filtrer les publicités et les afficher en fonction des intérêts, l'entreprise respecte la loi. Le CPCP a ensuite fait enquête sur Google en 2014. Il s'est avéré que la société avait diffusé des publicités à un homme qui s'attendait à ce qu'elle ne le fasse pas, comme elle le promettait dans sa politique de confidentialité lorsqu'il s'agit de renseignements sensibles. Or, des publicités ont quand même été diffusées. Dans son cas, il s'agissait de renseignements médicaux, et Google lui a diffusé des publicités afférentes. En fait, on a découvert que c'était la faute d'un conseiller indépendant qui ne suivait pas les règles de Google. Le problème, c'est que même s'il s'agit d'un service gratuit, cela outrepasse les limites de la politique de confidentialité, d'une part, et d'autre part, les limites des dispositions sur la protection de la vie privée, qui interdisent à la société de se servir de renseignements sensibles.

Pour ce qui est d'établir quels renseignements sont sensibles ou non, la décision est surtout prise en fonction du préjudice subi — ce qui revient à l'argument de Mme Gratton. Il faut se demander quel préjudice résulterait de la diffusion de l'information en question. Le préjudice est grave notamment dans le cas de données financières, qui exposent le consommateur à la fraude. Dans le cas de renseignements médicaux, il s'agit d'une violation grave et d'information sensible. C'est donc le critère que nous utilisons habituellement: quel préjudice découlerait de la divulgation? Ensuite, la dernière décision à ce sujet fait suite à l'enquête sur Bell, dont vous avez parlé, où le CPVP a déterminé que la société n'offre pas de service gratuit. Contrairement à la décision de 2009 concernant Facebook, il ne s'agit pas d'un service gratuit. Les utilisateurs ont déjà payé le service. Si la société souhaite en plus recueillir leurs renseignements personnels, c'est comme si elle prélevait un paiement supplémentaire, de sorte qu'elle doit alors obtenir un consentement explicite.

● (1705)

Le président: Très bien. Nous devons poursuivre. Gardez vos réflexions à l'esprit.

Nous passons maintenant à une série d'interventions de cinq minutes.

Nous allons commencer par M. Jeneroux. Allez-y, s'il vous plaît.

M. Matt Jeneroux (Edmonton Riverbend, PCC): Parfait.

Merci, monsieur le président. Je remercie tous les témoins d'être ici aujourd'hui.

Madame Bernier, il est bon de vous revoir. Vous n'avez peut-être pas été dans cette salle-ci, mais je vous souhaite la bienvenue au Parlement.

M. Dixon a parlé du « droit à l'oubli », malgré la contestation fondée sur la Charte. Nous aimerions savoir ce que vous en pensez.

Me Chantal Bernier: Comme vous l'avez constaté, j'en ai parlé très prudemment puisque la contestation fondée sur la Charte pourrait porter sur une restriction excessive de la liberté d'expression, ce qui irait à l'encontre de la Charte. Je crois que le droit à l'effacement — et je pense que le Centre pour la défense de l'intérêt public est du même avis — peut être formulé de façon à protéger la vie privée sans porter atteinte à la liberté d'expression, tout comme la Loi sur la protection des Canadiens contre la cybercriminalité. Dans ce texte législatif, nous criminalisons en quelque sorte une forme d'expression — par exemple, la publication non consensuelle d'une image intime sur le Web. Jusqu'à présent, la loi n'a pas été contestée ou déclarée inconstitutionnelle, car l'atteinte à la vie privée est si flagrante qu'elle ne s'applique pas à la liberté d'expression en général.

M. Matt Jeneroux: Savez-vous s'il y a d'autres provinces? Vous avez mentionné qu'il y a un lien avec les provinces, que ce n'est pas si facile et que nous pouvons simplement le faire au niveau fédéral. Est-ce dans les priorités des provinces? Le savez-vous?

Me Chantal Bernier: La Nouvelle-Écosse a précédé le gouvernement fédéral en ce qui concerne le suicide de Rehtaeh Parsons, et nous avons suivi. La loi de la Nouvelle-Écosse va plus loin et a fait l'objet d'une contestation constitutionnelle.

L'autre loi que j'ai mentionnée est celle appliquée dans les quatre provinces de common law et fait de la violation de la vie privée un acte délictuel. Ensuite, au Québec, comme madame Gratton l'a si bien décrit, la loi est probablement la plus claire et robuste de toutes.

Cependant, pour revenir au point de M. Massé quant à savoir si nous pourrions utiliser cela pour la LPRPDE, je dois vous rappeler que toutes les mesures législatives provinciales s'appliquent aux particuliers, tandis que la LPRPDE s'applique aux organisations. C'est la raison pour laquelle je dis que si vous voulez utiliser la LPRPDE, vous devez passer par des organisations. Comment les organisations peuvent-elles contribuer à réduire les torts causés à la réputation en ligne? Ce serait par l'entremise d'une obligation de supprimer les propos tenus lorsque la diffusion de renseignements est déclarée illégale en vertu de ces autres mesures législatives.

M. Matt Jeneroux: Je m'excuse auprès des autres membres, mais je pense que nous pourrions passer une autre journée entière ici avec Mme Bernier, monsieur le président.

Le président: Nous l'inviterons à nouveau.

M. Matt Jeneroux: Nous devrions l'inviter à nouveau. Expliquez-moi ce qui se produit maintenant si une personne demande que ses renseignements soient supprimés. Les gens ont ce droit par l'entremise d'ententes.

Me Chantal Bernier: C'est seulement en Europe. Une personne en fait la demande, par exemple, à Google car c'est la seule plate-forme qui la protégeait. Les tribunaux européens sont allés très loin en prenant un risque. Vous pouvez voir qu'ils voulaient que le droit d'être oubliés soit reconnu. Certains pourraient dire qu'ils ont quelque peu interprété la loi librement pour ce faire.

Donc, une personne s'adresse à Google et dit qu'elle veut que ses renseignements soient supprimés et ne puissent plus faire l'objet d'une recherche. Il y a des critères à respecter. La demande doit être légitime. Il faut qu'elle ait une certaine valeur, et si la personne répond au critère, les renseignements sont alors retirés.

● (1710)

M. Matt Jeneroux: C'est bien.

Le président: Merci beaucoup.

Monsieur Bratina, s'il vous plaît, vous avez cinq minutes.

M. Bob Bratina (Hamilton-Est—Stoney Creek, Lib.): Merci.

Merci à tout le monde.

J'imagine que le Centre pour la défense de l'intérêt public interagit avec le public plus souvent concernant des questions de la sorte. Ces questions sont-elles souvent soulevées dans vos activités de tous les jours?

M. John Lawford: Notre expérience avec la conservation des données et le droit à l'effacement découle en grande partie de notre plainte contre un site Web pour enfants et du refus absolu de l'entreprise de supprimer des renseignements personnels. Nous avons été engagés à contrat par des anciens membres de ce réseau social, lorsque nous avons déposé la plainte. Un certain nombre d'entre eux nous ont téléphoné et nous dit qu'ils avaient ce problème avec le site et que cela causait des difficultés.

À l'occasion, une personne nous enverra un courriel pour nous informer qu'elle n'aime pas la politique en matière de protection de la vie privée d'une entreprise X ou Y et pour savoir si l'entreprise peut faire telle ou telle chose. Nous avons donc des communications avec les gens, mais sur cette question particulière, c'était davantage après l'avoir soulevée que les gens ont dit qu'ils ne savaient pas comment faire pour que leurs renseignements soient supprimés, et si c'est possible.

La réponse pour l'instant est non, malheureusement. Toutefois, le commissaire à la protection de la vie privée a dit que dans ce cas-ci, il aimerait que le site retire l'information. C'était la première fois que je voyais cela. Nexopia tergiversait sur la question. L'entreprise a subséquemment été vendue à d'autres propriétaires, qui ont promis de supprimer les renseignements. Je ne suis pas certain si on l'a fait.

M. Bob Bratina: Puis nous nous penchons sur la question du temps de verbe, comme Mme Lau l'a mentionnée, je crois: il devrait, plutôt qu'il doit, et il y aurait...

M. John Lawford: Exact.

M. Bob Bratina: Cela se rapporte-t-il à un modèle exécutoire pour le commissaire à la protection de la vie privée? Opteriez-vous pour un tel modèle?

M. John Lawford: Oui, absolument. S'il y avait une exigence de produire une politique sur la conservation des données ou sur la suppression de renseignements, et qu'une entreprise refusait d'appliquer la politique, alors nous avons... Si les gens craignent de devoir payer des amendes élevées, on a vu ce qui s'est passé avec les lois anti-pourriel et la liste de numéros de télécommunication exclus. Les autorités dans ces cas-là ont un vaste éventail de mesures d'application. Elles n'ont pas besoin d'imposer d'emblée une amende d'un million de dollars, mais elles peuvent commencer par émettre des avertissements, des avis et des lignes directrices, et peuvent par la suite imposer diverses amendes. Nous pensons que ce modèle fonctionnerait.

M. Bob Bratina: Ce que nous avons entendu en partie durant la discussion d'aujourd'hui, c'est qu'il faut déterminer comment on peut rédiger les lois en tenant compte de l'évolution des technologies. C'est difficile à faire, mais en raison de la notion d'un calendrier de conservation des données, pourriez-vous rédiger des lois qui obligeraient les entreprises à demander votre approbation pour prolonger la durée au cours de laquelle elles conservent vos renseignements qu'elles ont obtenues d'une façon ou d'une autre? Autrement dit, toutes les entités communiqueraient avec vous dans un délai de cinq ans après avoir obtenu vos renseignements pour vous informer qu'elles devront rendre vos renseignements caducs à moins d'obtenir votre approbation de les conserver plus longtemps. Est-ce une mesure qui pourrait être incluse dans la loi?

M. John Lawford: Je pense que ce pourrait être possible. J'imagine que le commissaire à la protection de la vie privée pourrait vous donner un point de vue intéressant à ce sujet, peut-être jeudi. Il pourrait falloir faire de nombreuses vérifications, mais cette mesure permettrait à tout le moins d'offrir une certaine certitude.

C'est un peu comme si l'on dit qu'il devrait y avoir par défaut une politique sur la conservation des données pendant cinq ans. C'est possible. Vous pouvez poser la question au commissaire à la protection de la vie privée lorsqu'il sera ici.

M. Bob Bratina: Je dois revenir sur le problème de la rédaction des lois; c'est très compliqué. Je peux voir qu'il y a quelques contradictions dans les éléments qui ont été présentés.

Monsieur Dickson, vous avez dit que si l'on ne peut pas dire aux médias de supprimer... Que pensez-vous de notre capacité de prendre la situation en mains?

M. Robert Dickson: Je pense que c'est difficile, pour toutes les raisons qui ont été soulevées. Vous voyez le commissaire à la protection de la vie privée du Canada qui essaie de sanctionner les méfaits, qui reconnaît la présence d'un problème et qui tente de le régler. Nous avons vu la Cour fédérale essayer de résoudre le problème par l'entremise d'un cas qui est survenu. J'ai bien peur qu'il n'y ait pas de solution facile — ou de solution à toute épreuve, pour ainsi dire.

● (1715)

M. Bob Bratina: Pourquoi avez-vous renoncé à rédiger ou n'avez-vous pas terminé le rapport en Saskatchewan?

M. Robert Dickson: Tout ce que je sais, c'est que le commissaire à la protection de la vie privée avait embauché une organisation pour faire le travail. J'ai communiqué avec la commissaire adjointe Denham pour élaborer la mesure, nous l'avons déployée en Saskatchewan, de nombreuses réunions avec des organisations commerciales et des petites et moyennes entreprises ont eu lieu, et nous avons recueilli des renseignements et des observations durant ce processus. Il y a eu ensuite quelques problèmes, si je ne m'abuse, entre la firme de consultation et le bureau qui l'avait embauchée, et à un moment donné, je pense qu'on a mis fin au contrat. Je n'ai pas participé directement à ce processus.

C'était regrettable, car c'était un exercice intéressant qui permettait d'examiner la situation dans une région du pays où il n'y a pas de loi provinciale sur la protection de la vie privée s'appliquant au secteur privé et où la LPRPDE était la loi applicable. Il est important d'avoir des moyens de pression dans toutes les régions du Canada, et nous avons trouvé beaucoup d'éléments de preuve — c'était manifeste — démontrant qu'il y avait peu de moyens de pression dans cette province, et je présume que ce n'est pas seulement dans cette province.

M. Bob Bratina: Merci beaucoup.

Le président: Merci, monsieur Bratina.

Je vais prendre la parole pour les cinq prochaines minutes au nom de mon organisation politique. Je vais vous poser à tous mes questions d'emblée. J'ai essentiellement une question pour chacun de vous.

Tout d'abord, pour le CPIP, vous avez mentionné M. Owen Charters, président des Clubs garçons et filles du Canada. Dans votre mémoire, vous avez dit que ces outils de repérage surveillent nos enfants lorsqu'ils naviguent sur le Web pour colliger des données sur leur comportement et sur leurs intérêts et que ces renseignements sont souvent vendus à des entreprises de marketing.

Avez-vous une source pour corroborer votre déclaration? J'aimerais connaître cette source.

M. John Lawford: C'est sa citation. Je me ferais un plaisir de fournir l'article du *Wall Street Journal* au greffier.

Le président: Ce serait formidable. Je vous en serais reconnaissant.

M. John Lawford: Oui.

Le président: Nous voudrons peut-être l'inviter à témoigner pour nous parler de ce type de renseignements.

M. John Lawford: D'accord.

Le président: La prochaine question que j'ai pour vous — et je vais vous l'adresser directement — porte sur le paragraphe 25 de votre mémoire au CPVP. Vous mentionnez la mise en oeuvre des préférences en matière de normes relatives à la protection des renseignements personnels et d'un système de marques de confiance.

Je vais vous poser ma question, puis passer à un autre sujet, et vous pourrez y répondre plus tard. Existe-t-il un système de préférences volontaire ou dirigé par l'industrie ou un système de marques de confiance à l'heure actuelle?

Monsieur Dickson, ma question pour vous a trait aux dossiers médicaux.

N'est-il pas dans l'intérêt public de conserver les dossiers médicaux des gens pendant de très longues périodes, pour la simple raison que j'ignore si un jour mes renseignements génétiques pourraient être utiles à mes enfants, à mes petits-enfants et à mes arrières-petits-enfants? Pour les recherches dans le domaine de la santé et ce genre de travaux, il pourrait être bon de conserver ces dossiers de santé électroniques à tout jamais, dans l'intérêt public.

Ma question pour vous, madame Gratton, a trait à l'Union européenne.

Je crois que c'est une politique de l'Union européenne qu'aucune de ses directives ou initiatives n'influencent les politiques nationales d'autres pays avec lesquels elle traite, notamment en ce qui concerne les barrières non tarifaires. Je me demande si c'est exactement ce que fera la loi sur la protection des renseignements personnels: influencer notre capacité de faire des échanges commerciaux, simplement parce que la directive interne oppose la politique étrangère et la politique nationale pour le Canada.

Ma question pour vous, madame Bernier, est la suivante. Vous avez dit que l'infraction est proportionnelle aux revenus de l'organisation. Un organisme à but non lucratif pourrait avoir de grandes quantités de données, mais peu de revenus. Un organisme bénévole pourrait avoir un grand nombre de données, mais aucun revenu. Vous pouvez avoir une petite entreprise qui possède de nombreuses données pouvant causer des torts considérables mais qui génère peu de recettes. Vous pouvez avoir une grande société qui génère des revenus élevés et qui cause peu de torts, et elle peut payer plus pour une infraction qu'une petite organisation qui cause beaucoup plus de torts.

Pourriez-vous m'expliquer ce paradoxe?

Je vais vous laisser le soin de choisir l'ordre que vous voulez suivre pour répondre aux questions.

M. John Lawford: J'imagine que nous commencerons de gauche à droite. Il y a des systèmes de marques de confiance. Certains ont été créés et ont été abolis au fil des ans. Je sais qu'il y a le programme Choix de pub, un exemple américain, qui est également suivi par l'Association canadienne des annonceurs. Je crois qu'Alysia a mentionné qu'Ann Cavoukian dirige l'un de ces programmes pour Protection des renseignements personnels intégrée à la conception.

Mlle Alysia Lau: Oui, il y en a un. C'est un partenariat entre l'Université Ryerson et Deloitte.

M. John Lawford: De façon générale, nous estimons que ce serait une bonne chose d'avoir un système de marques de confiance. Nous pouvons dire que ce serait une bénédiction pour le commissaire à la protection de la vie privée, qui s'est penché sur ce système volontaire et estime que c'est une bonne approche qui serait utile car elle accroîtrait la confiance des consommateurs.

● (1720)

Le président: Merci beaucoup.

Allez-y, monsieur Dickson.

M. Robert Dickson: De façon générale, lorsqu'il est question de la conservation des dossiers, les lois sur la protection des renseignements personnels prévoient qu'il n'est pas approprié de conserver ces renseignements car on pourrait avoir besoin de cette information à d'autres fins ultérieurement. Vous colligez des renseignements dans un but précis. C'est fondamental à toutes les lois sur la protection des renseignements personnels.

Lorsque le but initial pour conserver les renseignements est atteint, il faut les détruire.

Dans la pratique, cela signifie que dans pratiquement toutes les provinces qui ont une loi autonome relative aux renseignements sur la santé, il y a une exigence voulant que les gardiens ou les administrateurs doivent établir un calendrier de conservation des données. C'est habituellement influencé par des avis juridiques quant à la durée pendant laquelle il y a une responsabilité légale éventuelle, puis les dossiers doivent être détruits.

Il y a aussi une disposition dans chacune de ces lois autonomes relatives aux renseignements sur la santé qui prévoit que ce peut être applicable à un conseil d'éthique en matière de recherche ou à un comité d'éthique pour la recherche afin d'accéder à des renseignements dans le cadre de projets précis.

Dans sa forme actuelle, la loi prévoit qu'il est inapproprié et illégal de conserver des renseignements parce que mes données médicales pourraient être utiles un jour pour mes petits-enfants ou leurs enfants.

Ce qui se passe en partie, à mesure que l'on fait des avancées en génétique, c'est que les renseignements au sujet de ma santé ou de votre santé deviennent plus précieux. Cela sera un défi pour les législateurs et vous à l'avenir. À l'heure actuelle, il n'y a pas le type de disposition que vous aimeriez qu'il y ait.

Le président: C'est de bonne guerre.

C'est à votre tour, madame Gratton.

Me Éloïse Gratton: Oui, je crois que l'Union européenne impose clairement des normes en matière de protection de la vie privée. J'ai quelques inquiétudes à ce sujet.

De plus, je pense que nous devons tenir compte du fait que tous les quatre ans, ce sera réévalué, non seulement à la lumière de la LPRPDE mais aussi à la lumière de notre législation en matière de sécurité nationale. C'est quelque chose auquel il faut réfléchir.

Le mois dernier, il y a eu un article de Gabe Maldoff et d'Omer Tene, des professeurs américains, qui ont fait remarquer que, à la lumière de la récente décision Schrems en Europe, il n'est pas clair que le Canada répond toujours à ce critère.

Je pense donc que nous devrions nous concentrer sur nos problèmes et nous ne devrions pas plier autant.

Le président: Madame Bernier, nous aimerions entendre votre réponse rapidement, s'il vous plaît.

Me Chantal Bernier: Tout d'abord, je tiens simplement à clarifier au sujet des amendes que la LPRPDE ne s'applique qu'aux activités commerciales, si bien qu'il y a toujours un revenu lié aux renseignements personnels.

De plus, à mon avis, l'utilisation d'un pourcentage serait précisément proportionnel et, par conséquent, juste pour imposer des sanctions équivalentes à toutes les organisations.

En ce qui concerne les torts, ils ne reflètent pas la faute. On peut avoir un piratage très nuisible. Prenons l'exemple de Carbanak. Carbanak a ciblé 100 institutions financières et des milliards de dollars. Les vérificateurs de Kaspersky ont examiné la situation et ont découvert un cas de piratage des plus sophistiqués et ont déclaré qu'ils n'arrivaient pas à trouver de lacunes dans les systèmes de sécurité des 100 banques qui ont été piratées. C'était tout simplement de la malchance. Par conséquent, nous ne devrions pas associer les torts et la culpabilité.

Enfin, je crois que le meilleur endroit pour évaluer et accorder les dommages-intérêts, ce sont les tribunaux.

Le président: Merci beaucoup.

Monsieur Erskine-Smith, vous avez cinq minutes, s'il vous plaît.

M. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Merci beaucoup.

Ma première question porte sur quelque chose dont nous n'avons pas encore beaucoup discuté, à savoir les recours civils en vertu de la LPRPDE. À quel point sont-ils efficaces, d'après vous, et croyez-vous qu'il y a une administration modèle dont nous devrions nous inspirer qui a une meilleure structure?

Me Chantal Bernier: Il n'y a aucun recours civil à l'heure actuelle.

M. Nathaniel Erskine-Smith: Les articles 14 et 16.

Me Chantal Bernier: Eh bien, vous vous adressez au CPVP, puis vous vous adressez aux tribunaux.

M. Nathaniel Erskine-Smith: C'est le recours civil et...

Me Chantal Bernier: Oui.

M. Nathaniel Erskine-Smith: ... cela me semble insuffisant. Y a-t-il une administration modèle dont nous pourrions nous inspirer afin d'améliorer notre régime actuel?

● (1725)

Me Chantal Bernier: Comme je l'ai mentionné dans mes remarques liminaires, il y a tout un éventail. Il y a le Royaume-Uni, où les amendes vont jusqu'à 250 000 livres. Il y a la France, où elles peuvent s'élever jusqu'à 300 000 euros.

M. Nathaniel Erskine-Smith: Je m'excuse de vous interrompre, mais si le commissaire à la protection de la vie privée commence à imposer des sanctions...

Disons qu'un groupe de consommateurs a subi un préjudice quelconque. Nous ne devrions pas nécessairement attendre... Nous devrions attendre le rapport du commissaire, d'après ce que je comprends, en vertu de l'article 14, mais nous pourrions nous adresser aux tribunaux après avoir reçu le rapport.

Je comprends que le CPVP devrait probablement pouvoir imposer des amendes, mais devrions-nous en plus renforcer les recours civils?

Me Chantal Bernier: Les recours civils sont prévus. Je précise que Me Gratton, M. Richard Dickson, M. Gary Dickson et moi parlions justement de la prolifération des recours collectifs. Les recours civils existent et sont utilisés. Des sommes considérables sont en jeu. Le cas de Casino Rama est un exemple. Il y a eu un règlement important. D'autres cas pour lesquels des sommes considérables sont en jeu sont en instance. Donc, cela se fait.

M. John Lawford: Vous pourriez examiner ce qui se fait dans la loi antipourriel, qui accorde un droit privé d'action et prévoit une amende pouvant aller jusqu'à 200 $ par violation. C'est quelque chose de comparable. Cela permet les recours collectifs, car il est difficile de faire la preuve d'un préjudice. Il y a actuellement au Canada divers recours collectifs qui visent à savoir s'il est possible d'obtenir des dommages-intérêts lorsqu'il n'y a pas de préjudice réel. La loi antipourriel pourrait vous servir de modèle si vous décidez d'inclure une disposition quelconque dans la loi. Cela favoriserait les mécanismes d'exécution privée du régime. Si les mesures d'application administratives ne sont pas adéquates, les avocats de pratique privée pourraient se charger de certains dossiers.

M. Nathaniel Erskine-Smith: Je pense que c'est aussi le cas pour les droits d'auteur.

Monsieur Dickson, madame Gratton, avez-vous quelque chose à ajouter?

M. Robert Dickson: Je n'ai rien à ajouter aux observations de Chantal.

Me Éloïse Gratton: Je n'ai rien à ajouter.

M. Nathaniel Erskine-Smith: Quant au droit à l'oubli, il y a diverses façons de l'appliquer. À titre d'exemple, si j'avais la possibilité de publier en ligne un article sur une autre personne, cette personne pourrait faire valoir le droit à l'oubli. Évidemment, la liberté d'expression ferait office de contrepoids, comme vous l'avez indiqué, madame Bernier.

Toutefois, en ce qui concerne les index, je constate que ce n'est pas seulement une question de liberté d'expression. Il y a également l'intérêt public quant à l'accès aux informations dans des contenus archivés. De toute évidence, certaines personnes voudraient que des informations qui les concernent tombent dans l'oubli, mais le public pourrait penser le contraire.

Madame Bernier, vous avez mentionné l'Union européenne. A-t-elle établi un équilibre adéquat par rapport à l'intérêt du public, en particulier pour les index?

Me Chantal Bernier: M. Gary Dickson a évoqué précédemment notre collaboration à la rédaction de lignes directrices en matière de diffusion des décisions des tribunaux administratifs sur Internet. C'est directement lié à votre propos. Nous voulions assurer la protection des renseignements personnels des parties concernées tout en maintenant la transparence judiciaire pour la raison que vous avez mentionnée, soit l'intérêt du public pour l'accès à cette information. Une des solutions consiste simplement à utiliser les initiales plutôt que le nom complet et les identifiants. Donc, la transparence des tribunaux est assurée, tandis que l'identité des parties en cause — qu'il n'est pas nécessaire de connaître — est protégée.

En Europe, le droit à l'oubli est défini de façon assez pointue, comparativement au droit plutôt discret à l'effacement. Toute demande en ce sens doit être fondée sur la non-pertinence ou l'inexactitude. Ce que je veux dire, c'est qu'il y a des critères.

Pour revenir à la congruence entre les deux aspects, on fait valoir que des paramètres sont nécessaires pour que cela n'empiète ni sur le droit de savoir — la liberté de l'accès à l'information — ni sur la liberté d'expression. Il y a sans aucun doute moyen de trouver le juste milieu.

Le président: Très bien. Merci beaucoup.

La dernière intervention de trois minutes revient à M. Cullen. Ensuite, nous mettrons fin à la séance, car nous avons dépassé le temps imparti.

Je tiens à remercier d'avance tous nos témoins. Je sais que certaines personnes ont un horaire assez serré.

Monsieur Cullen, vous avez trois minutes.

M. Nathan Cullen (Skeena—Bulkley Valley, NPD): Je vais m'en tenir au temps qui m'est imparti, avec l'aide du président.

Merci de vos témoignages. J'ai lu diverses études. Si je pose une question qui a déjà été posée, je vous prie de m'excuser, mais il est difficile pour un politicien de résister lorsqu'il a un microphone et qu'il a du temps devant lui. De plus, l'ignorance ne m'a jamais empêché de parler.

J'ai une question d'ordre technique concernant le droit à l'oubli. Les progrès technologiques permettent l'intégration d'une option de suppression, comme pour la location d'un film, par exemple, où la durée de l'accès est simplement limitée. A-t-on déjà envisagé cette solution pour les renseignements personnels, de sorte que les renseignements fournis à une entreprise privée pourraient être supprimés automatiquement après cinq ans grâce à un algorithme intégré? Des technologies de ce genre ont-elles déjà été implantées avec succès? Cela pourrait-il être inclus dans la loi? Vous avez parlé des coûts considérables des vérifications qui sont menées après cinq ans pour déterminer si les informations ont bel et bien été supprimées ou si elles se retrouvent dans un registre quelconque en Saskatchewan, comme vous l'avez indiqué, je crois. Cela me semble tout simplement typique, d'une certaine façon. A-t-on déjà envisagé une solution technologique à ce problème?

● (1730)

M. John Lawford: Je ne pense pas que cela ait déjà été commercialisé, mais il serait sans doute possible de créer un tel algorithme. Je pense que ce serait très facile.

Me Éloïse Gratton: Nous devrions encourager le recours aux technologies qui ne conservent pas les données éternellement; je pense notamment à des applications de messagerie éphémère comme Snapchat. Donc, c'est tout à fait possible.

M. Nathan Cullen: J'ai une deuxième question. Il a eu récemment une pétition sur la réforme électorale par l'intermédiaire du Parlement; c'était une pétition parlementaire officielle. J'ai notamment remarqué — et c'est l'une des premières fois que cela m'arrivait — que beaucoup de gens m'écrivaient pour savoir si les informations accompagnant leur signature allaient être transmises aux partis. Ils posent la question parce que c'est une réalité: les partis politiques utilisent les pétitions pour recueillir des données.

Y a-t-il eu beaucoup d'études sur l'aspect de la conservation des données tant par le gouvernement que par les partis politiques, par extension? Je ne parle pas des partis politiques comme un prolongement du gouvernement, mais plutôt comme une autre forme de participation citoyenne. A-t-on observé de manière concrète que les Canadiens et certains groupes de Canadiens évitent de participer à la vie civile par crainte que leurs données soient conservées? Je pense à ce qu'on voit chez nos voisins du sud actuellement. Si j'étais un Américain musulman, voudrais-je vraiment signer une pétition, même si elle était destinée au gouvernement des États-Unis?

M. Robert Dickson: Vous soulevez un enjeu sur lequel le Comité s'est penché dans son étude de la Loi sur la protection des renseignements personnels. L'un des témoins était le professeur Colin Bennett, de l'Université de Victoria, le plus éminent spécialiste canadien des questions de protection de la vie privée dans le contexte des partis politiques et des élections. Je sais que l'Association du Barreau canadien mène des études à cet égard. Je sais que le directeur général des élections — ou plutôt le prédécesseur de son prédécesseur, en fait — a recommandé d'étudier la question. Cela pourrait être une excellente, mais longue discussion qui mènerait certainement à des recommandations, soit de ce Comité, soit d'autres organisations, demandant que le Parlement se penche enfin sur les pratiques des partis politiques en matière de protection des renseignements personnels.

Le président: Mesdames et messieurs, c'est tout le temps que nous avons. J'ai quelques observations, étant donné que nous devons mettre fin à la séance. Monsieur Cullen, je vous remercie de vos questions. Chers témoins, si vous avez des informations que vous n'avez pas eu l'occasion de nous transmettre aujourd'hui, je vous prie d'en prendre note et de les faire parvenir au Comité pour que nous puissions les ajouter aux réponses que vous avez données aujourd'hui. Si vous avez d'autres renseignements, des commentaires que vous auriez souhaité faire ou qui vous viennent à l'esprit plus tard, n'hésitez pas à les transmettre au Comité.

Merci beaucoup de votre temps. Veuillez excuser notre retard. Merci beaucoup. Je suis convaincu que vous nous serez d'une grande aide si nous vous invitons de nouveau à comparaître.

La séance est levée.