



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 049 • 1^{re} SESSION • 42^e LÉGISLATURE

TÉMOIGNAGES

Le jeudi 23 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 jeudi 23 février 2017

• (1530)

[Traduction]

Le président (M. Blaine Calkins (Red Deer—Lacombe, PCC)): Bonjour, chers collègues.

Je sais que bon nombre d'entre nous sont impatients, puisque c'est la dernière semaine de quatre semaines avant que nous retournions dans nos circonscriptions pendant la pause parlementaire. Nous avons parmi nous d'éminents témoins pour nous aider dans nos délibérations dans le cadre de l'étude que nous menons à l'heure actuelle sur la Loi sur la protection des renseignements personnels et les documents électroniques, que les Canadiens appellent plus communément la LPRPDE.

Du Centre for Law and Democracy, nous accueillons à nouveau M. Michael Karanicolas, conseiller juridique principal, par vidéoconférence.

Nous sommes ravis de vous revoir, monsieur Karanicolas.

À titre personnel, nous recevons encore une fois Teresa Scassa, professeure titulaire à l'Université d'Ottawa.

Merci, Teresa, de vous joindre à nouveau à nous. C'est toujours un plaisir de vous recevoir ici.

Pour une première fois au Comité, pour son premier passage ici, ou comparution, nous accueillons Florian Martin-Bariteau, professeur adjoint, Section de common law de la Faculté de droit, et directeur, Centre de recherche en droit, technologie et société à l'Université d'Ottawa.

Conformément à notre procédure habituelle, nous entendrons une déclaration liminaire de 10 minutes de chacun des témoins. Nous suivrons l'ordre selon lequel je vous ai présentés. Je pense que tout le monde connaît notre façon de faire.

Nous allons commencer avec vous, monsieur Karanicolas. Vous avez 10 minutes maximum, s'il vous plaît.

M. Michael Karanicolas (conseiller juridique principal, Centre for Law and Democracy): Merci au Comité de m'avoir invité à comparaître à nouveau.

J'aimerais tout d'abord féliciter le Comité permanent pour ses recommandations concernant la Loi sur la protection des renseignements personnels, qui ont été publiées à la fin de l'année dernière et qui étaient, à mon avis, excellentes.

Je crois qu'il est assez clair que le modèle de protection de la vie privée fondé sur le consentement est désuet. La dynamique qui sous-tend ce modèle et qui fait tourner une bonne partie de l'économie numérique est le fait que les utilisateurs peuvent choisir d'échanger leurs renseignements personnels contre des services. Ce modèle présente des avantages indéniables, qui a contribué à la croissance

rapide d'Internet en faisant baisser les coûts d'entrée. Cependant, cette dynamique repose sur le consentement valable, ce qui signifie que la partie contractante doit avoir une compréhension superficielle de ce qu'elle signe. En fait, pratiquement personne ne lit les modalités des ententes de services, ce qui mine considérablement la légitimité du consentement obtenu.

Le rapport du CPVP souligne en partie la longueur de ces ententes et la fréquence à laquelle elles sont présentées aux utilisateurs comme étant la cause de ce manque de compréhension, mais il convient également de signaler que ces ententes sont souvent rédigées dans des termes très complexes, ambigus et contradictoires que même des gens qui ont une formation technique et juridique ont du mal à comprendre. C'est un cercle vicieux au travail. Le fait que très peu d'utilisateurs lisent ces ententes ou en utilisent le contenu comme fondement pour accepter ou refuser un service donne aux entreprises une autorisation, un incitatif, pour les rédiger dans un libellé très général. Ce style de rédaction et le manque d'accès contribuent à ce que les signataires prêtent attention aux modalités.

Il convient également de souligner que l'entreprise qui présente l'entente et offre un service peut souvent être différente de celles qui recueillent et traitent les renseignements. Des courtiers en information sont très présents dans l'écosystème d'Internet. Une étude réalisée en 2014 a révélé que des 950 000 sites Web les plus populaires, 88 % d'entre eux communiquaient systématiquement les renseignements de leurs visiteurs avec des tierces parties, avec en moyenne 9,5 tierces parties différentes par site Web. Ces renseignements sont en grande partie recueillis subrepticement, avec seulement 2 % des tierces parties qui utilisent un message pour mettre en garde les utilisateurs de leur présence.

Il y a visiblement un problème ici. Cependant, il est important de chercher des solutions qui ne feront pas dérailler l'économie numérique actuelle. Bien qu'il y ait des avantages et des inconvénients à un système où les renseignements personnels sont utilisés comme monnaie d'échange pour obtenir des services en ligne, les avenues possibles devraient être conçues de manière à maintenir les énormes avantages que l'accès à Internet offre.

Une solution, que nous appuyons fermement, serait de rehausser la qualité du consentement en améliorant les renseignements disponibles aux utilisateurs. Une pratique exemplaire pourrait être de publier un résumé ou un guide d'explication des modalités avec la version juridique intégrale, afin de s'assurer que l'entente peut être facilement examinée, et d'aviser clairement les utilisateurs lorsqu'un changement important est apporté à l'entente.

Le CPVP a un rôle important à jouer ici: promouvoir de meilleures pratiques en matière de clarté et d'accessibilité des modalités des ententes de services et vérifier les ententes actuelles pour en examiner la clarté, l'accessibilité et l'exactitude des renseignements, de même que la façon dont l'information est recueillie et traitée. Par ailleurs, nous appuyons la proposition de passer à un mécanisme de consentement préalable comme mécanisme par défaut.

L'amélioration de la transparence est un autre facteur important pour rehausser la qualité du consentement, permettant ainsi aux gens d'examiner de plus près les services et les plateformes qu'ils utilisent. Cela peut inclure, par exemple, le droit de demander des explications sur la façon dont leurs renseignements personnels sont utilisés pour personnaliser leur expérience en ligne ou sur les facteurs qui sont entrés en ligne de compte dans une décision prise par l'entreprise. Cependant, il y a encore grandement place à l'amélioration au niveau de la participation des utilisateurs et de la qualité du consentement. Ces améliorations ne suffiraient pas pour protéger les droits à la vie privée des Canadiens. Le CLD appuie la création de zones d'accès interdit clairement définies, de même que de zones de mise en garde, comme le rapport du CPVP le suggère. Un point important à envisager ici est la nécessité de clarifier comment les renseignements peuvent être communiqués à des tierces parties ou être revendus et la nécessité de préciser les règles qui devraient régir ces utilisations externes. Il faut également accorder des pouvoirs d'enquête plus vastes au CPVP pour promouvoir des pratiques exemplaires en matière de gestion de l'information et de la sécurité.

En ce qui concerne la dépersonnalisation et l'anonymisation de l'information, bien que je pense que c'est une pratique qui devrait être encouragée, ce n'est pas une panacée pour régler les problèmes actuels en matière de protection des renseignements personnels. J'ajouterais à l'observation formulée dans le rapport du CPVP qu'à mesure que l'anonymisation augmente, la valeur commerciale de l'information peut souvent diminuer, donnant ainsi un incitatif pour les entreprises à opter pour des solutions incomplètes. De plus, le fait que ces renseignements ont été, pour ainsi dire, dépersonnalisés, peut créer un faux sentiment de sécurité, ce qui pousse les entreprises à être moins vigilantes pour protéger ces renseignements et porte les consommateurs à assumer que les menaces à leur vie privée ont disparu.

Je veux également aborder brièvement la réputation, le droit à la vie privée et le droit à l'oubli.

● (1535)

L'effet transformateur d'Internet sur nos fonctions sociales a fait de l'empreinte virtuelle d'une personne un aspect essentiel de son identité. Toutefois, la permanence et l'accessibilité accrue des renseignements en ligne ont suscité des préoccupations chez certains concernant l'incidence d'Internet sur la vie privée et la réputation des gens.

Il y a des avantages à rendre le passé des gens plus accessible. Un musée de l'Holocauste, par exemple, voudra, et avec raison, savoir si un candidat à un emploi a fait des commentaires racistes dans le passé. Cependant, nous sommes également une société qui croit au fait d'accorder aux gens une seconde chance. Il peut y avoir des problèmes quant à la façon dont les dossiers numériques se présentent, notamment lorsqu'une décision d'un procureur de retirer des accusations ne reçoit peut-être pas autant de couverture médiatique que l'arrestation initiale ou lorsqu'un reportage médiatique erroné ou sensationnaliste attire plus d'attention que lorsqu'on le retire plus tard.

Cependant, les expériences en Europe en lien avec le droit à l'oubli devraient être perçues comme des leçons à tirer sur ce qu'il ne faut pas faire. Par exemple, toute mesure en vue de créer un droit à l'oubli devrait être incluse dans des définitions claires et limitées de son application, de transparence rigoureuse et de processus d'application de la loi robuste. Je vais aborder successivement chacun de ces éléments.

Premièrement, pour appliquer le droit à l'oubli, il faut établir un juste équilibre entre la liberté d'expression, la protection des renseignements personnels et le droit à l'information. Cet équilibre devra être fondé sur un critère bien précis pour déterminer où l'intérêt public repose. Les gens n'ont jamais eu le droit de contrôler ou de gérer leur réputation. Toute tentative de créer un droit à l'oubli devrait être axée exclusivement sur les nouveaux aspects de la réputation qui sont survenus avec l'avènement d'Internet et devrait être réservée à des circonstances où il y a clairement une injustice, notamment lorsqu'une personne est injustement arrêtée.

Deuxièmement, la transparence est un élément clé, ce qui comprend notamment le fait de mettre à la disposition des renseignements détaillés sur le fonctionnement et l'application des processus de prise de décisions. Il devrait y avoir le plus de renseignements possibles, sans toutefois nuire à l'efficacité des processus.

Troisièmement, dans tous les cas de restriction de la liberté d'expression, l'application régulière de la loi est extrêmement importante. Les moteurs de recherche ne sont tout simplement pas équipés pour contribuer à l'atteinte d'un juste équilibre des droits et ont malheureusement un incitatif dans le cadre du système européen actuel à retirer les renseignements sans appliquer un processus rigoureux, ce que l'on devrait faire avec des questions délicates de ce genre. Toute tentative de retirer des renseignements et de réduire l'accessibilité devrait être laissée à la discrétion d'un tribunal ou d'une autorité quasi judiciaire, y compris les considérations prévues dans un processus d'application régulière de la loi rigoureux.

Je tiens à souligner que rien de ce que je viens de dire ne devrait être interprété comme étant une forme d'appui au droit à l'oubli. On peut certainement soutenir que les problèmes actuels en lien à la réputation des gens se régleront tout seuls avec le temps, à mesure qu'ils s'habitueront graduellement à la prépondérance des renseignements gênants ou désagréables et apprendront à prendre ces renseignements avec un grain de sel. Cependant, en ce qui concerne le droit à l'oubli qui est envisagé, il est important de ne pas répéter les erreurs largement critiquées qui ont été commises par la Cour de justice de l'Union européenne dans ce dossier.

J'ai hâte d'entendre vos questions.

● (1540)

Le président: Merci beaucoup, monsieur Karanicolas.

Nous allons maintenant entendre Mme Scassa, pour 10 minutes.

Mme Teresa Scassa (professeure titulaire, Université d'Ottawa, Chaire de recherche du Canada en droit d'information, à titre personnel): Merci de l'invitation à vous rencontrer aujourd'hui pour contribuer à vos discussions sur la LPRPDE. Je suis professeure à la Faculté de droit de l'Université d'Ottawa, où je suis titulaire de la chaire de recherche du Canada en droit d'information. Je comparais devant vous à titre personnel.

Nous faisons face à ce que nous pourrions considérer comme étant une crise de la légitimité en ce qui concerne la protection des données personnelles au Canada. Chaque jour, nous entendons des histoires dans les nouvelles de piratages de données ou d'atteintes à la sécurité des données, ainsi que de collecte subreptice de renseignements personnels par les appareils qui se trouvent dans nos maisons ou sur nous et qui sont branchés à Internet. Il y a des histoires sur la façon dont le profilage de données a une incidence sur la capacité des gens d'obtenir l'assurance-maladie ou du crédit ou de trouver un emploi. Il y a également des préoccupations quant à la mesure dans laquelle les autorités d'État peuvent accéder à nos renseignements personnels que détiennent des entreprises du secteur privé. La LPRPDE, dans sa forme actuelle, ne suffit pas pour régler ces problèmes.

Mes observations s'articulent autour de la transparence. La transparence est fondamentalement importante à la protection des données et a toujours joué un rôle important en vertu de la LPRPDE. Essentiellement, la transparence est synonyme d'ouverture et d'accessibilité. Dans le cadre de la protection des données, les organismes doivent faire preuve de transparence en ce qui concerne la collecte, l'utilisation et la communication des renseignements personnels, ce qui signifie que le commissaire doit également être transparent dans son rôle de surveillance en vertu de la loi.

Je dirais également que les acteurs étatiques, ce qui comprend les organismes d'application de la loi et de sécurité nationale, doivent faire preuve d'une plus grande transparence concernant leur accès aux renseignements personnels que détiennent des organismes du secteur privé et l'utilisation qu'ils en font.

En vertu de la LPRPDE, la transparence est au coeur du régime de protection des données axé sur le consentement. C'est au coeur de l'obligation des entreprises de rendre accessibles aux consommateurs leurs politiques en matière de protection de la vie privée et d'obtenir leur consentement pour recueillir, utiliser ou communiquer des renseignements personnels. Or, ce type de transparence a été soumis à d'importantes pressions et a été grandement affaibli par les changements technologiques et un amendement législatif fragmentaire.

Le volume de renseignements qui sont colligés par l'entremise de nos interactions numériques, mobiles et électroniques et leurs utilisations réelles et potentielles sont sans limite. Ce faisant, de plus en plus d'appareils que nous avons sur nous et à la maison recueillent et transmettent nos renseignements. Ils peuvent même le faire sans que nous le sachions, et ce de façon continue. Le résultat est qu'il y a bien moins de points ou de moments bien définis où la collecte de données a lieu, ce qui fait en sorte qu'il est difficile de dire qu'un avis a été présenté et qu'un consentement éclairé a été obtenu.

De plus, le nombre d'interactions et d'activités quotidiennes qui entraînent la collecte de données se sont multipliées au point où nous ne pouvons plus lire et évaluer toutes les politiques en matière de protection de la vie privée. Même si nous avons le temps, ces politiques, comme je viens de le mentionner, sont souvent trop longues, complexes et vagues, si bien que même si nous les lisons, nous ne pouvons pas avoir une idée des données qui sont recueillies et communiquées, avec ou par qui, ou à quelles fins.

Dans ce contexte, le consentement est une farce en quelque sorte, et les consommateurs sont malheureusement en grande partie les dindons de la farce. Les seules parties qui peuvent dire que notre modèle actuel axé sur le consentement fonctionne toujours sont ceux

qui bénéficient du fait que les consommateurs se résignent face à cette collecte omniprésente de données.

Le récent processus de consultation sur le consentement du commissaire à la protection de la vie privée a permis de relever un certain nombre de stratégies possibles pour combler les lacunes du système actuel. Il n'y a pas de solution facile ou de changement mineur au libellé qui pourrait régler les problèmes entourant le consentement. Cela signifie, d'une part, qu'il faut apporter d'importants changements à la façon dont les organismes offrent une réelle transparence concernant leurs pratiques de collecte, d'utilisation et de communication des données et, d'autre part, il faut également adopter une nouvelle approche à l'égard du respect de la loi qui confère au commissaire des pouvoirs de surveillance et d'application de la loi beaucoup plus grands. Les deux changements sont inextricablement liés.

Le mandat plus large de protection du public du commissaire prévoit qu'il dispose des pouvoirs nécessaires pour prendre des mesures dans l'intérêt public. Le contexte technologique dans lequel nous évoluons est tellement différent de ce qu'il était lorsque cette loi a été adoptée en 2001 que le fait de discuter d'apporter seulement quelques modifications mineures à la loi fait fi des effets transformateurs des mégadonnées et de l'Internet des objets.

Une réforme importante de la LPRPDE est attendue depuis longtemps, et elle pourrait offrir des avantages importants qui vont beaucoup plus loin que seulement régler les problèmes entourant le consentement. Je signale que si l'on demandait à quelqu'un de rédiger une loi comme s'il s'agissait d'une oeuvre d'art pour évoquer le problème relativement aux politiques en matière de protection des renseignements personnels incompréhensibles, alambiquées et déformées et leur manque de transparence, alors la LPRPDE serait cette loi. Même si l'idée de reformuler la loi pour qu'elle ne soit plus considérée comme la pire de toutes les politiques est mal reçue, c'est une idée que ce comité devrait considérer.

Je fais cette recommandation dans le contexte où tous ceux qui recueillent, utilisent et communiquent des renseignements personnels dans le cadre de leurs activités commerciales, ce qui comprend un grand nombre de petites et moyennes entreprises qui ont un accès limité à l'expertise d'avocats expérimentés, doivent se conformer à la loi. De plus, les membres du public devraient idéalement avoir une chance de lire la loi et de comprendre les mesures de protection de leurs renseignements personnels et les droits de recours. Dans sa forme actuelle, la LPRPDE est un ramassis de mesures alambiquées où les principes normatifs ne figurent pas dans la loi, mais ont été ajoutés dans une annexe.

• (1545)

Pire encore, la signification de certains mots dans l'annexe, de même que les principes qu'elle contient, est modifiée par la loi, de sorte qu'il est impossible de bien comprendre les règles et les exceptions sans devoir faire les liens nécessaires, ce qui s'avère complexe. Après une série de modifications ponctuelles, la LPRPDE forme maintenant en grande partie une série de plus en plus longue d'exceptions aux règles sur la collecte, l'utilisation ou la communication avec consentement. Bien que le CPVP ait travaillé fort pour rendre accessibles les principes juridiques contenus dans la LPRPDE aux entreprises et aux individus, la Loi en tant que telle n'est pas accessible.

Dans une récente demande liée à la LPRPDE concernant un demandeur non représenté — et la plupart des gens qui comparaissent devant la Cour fédérale ne sont pas représentés, ce qui, à mon avis, est un autre problème que pose la LPRPDE —, le juge Roy a dit qu'il n'est guère étonnant qu'une partie ne comprenne pas la portée de la Loi.

J'ai déjà parlé des modifications ponctuelles qui ont été apportées à la LPRPDE au fil des ans, de même que des préoccupations au sujet de la transparence. À ce sujet, il est important de souligner que la Loi a été modifiée de sorte que soit augmenté le nombre d'exceptions à la règle du consentement qu'il serait autrement nécessaire de respecter pour la collecte, l'utilisation ou la communication de renseignements personnels.

Par exemple, les alinéas 7(3)d.1) et d.2) ont été ajoutés en 2015. Ils permettent à une organisation de communiquer des renseignements personnels à une autre organisation en vue d'une enquête sur la violation d'un accord ou sur des contraventions au droit fédéral ou provincial qui ont été commises ou qui sont sur le point de l'être, ou en vue de la détection d'une fraude ou de sa suppression. Bien qu'il s'agisse d'objectifs importants, je signale qu'aucune exigence en matière de transparence n'a été établie pour ces pouvoirs plutôt importants de communiquer des renseignements personnels à l'insu de l'intéressé ou sans son consentement. Notamment, il n'est pas obligatoire d'aviser le commissaire d'une telle communication. La portée de ces exceptions crée une lacune importante sur le plan de la transparence qui affaiblit la protection des renseignements personnels. Cela devrait être corrigé.

La LPRPDE contient également des exceptions qui permettent à des organisations de communiquer des renseignements personnels à des acteurs gouvernementaux à des fins d'application de la loi et de sécurité nationale à l'insu de l'intéressé ou sans son consentement. Il n'y a pas non plus de mesures de protection en matière de transparence pour ces exceptions. Compte tenu de l'énorme quantité de renseignements personnels très détaillés, dont les lieux, qui sont maintenant recueillis par des organisations du secteur privé, l'absence d'exigences en matière de transparence constitue un problème flagrant sur le plan de la protection de la vie privée.

Le ministère de l'Innovation, des Sciences et du Développement économique a créé un ensemble de lignes directrices volontaires sur la transparence pour les organisations qui choisissent de divulguer le nombre de demandes qu'elles reçoivent et la façon dont elles les traitent. Il est temps d'établir des obligations en matière de transparence pour de telles communications, qu'il s'agisse de la présentation de rapports publics ou de la présentation de rapports au commissaire, ou d'un mélange des deux. De plus, cela devrait s'appliquer tant aux acteurs du secteur privé qu'à ceux du secteur public.

Un autre changement majeur qui doit être apporté pour que la LPRPDE puisse répondre aux défis de l'heure qui sont liés à la protection des données concerne les pouvoirs du commissaire. Lorsqu'elle a été adoptée en 2001, la LPRPDE représentait un changement fondamental dans la façon dont les entreprises allaient recueillir, utiliser et communiquer des renseignements personnels. Ce changement majeur a été effectué avec une grande délicatesse. La LPRPDE illustre un modèle d'ombudsman prévoyant un certain doigté avec un accent mis sur la persuasion plutôt que sur l'imposition. Seize ans plus tard, et avec des exaoctets de données personnelles, il est grand temps que l'on fournisse au commissaire un ensemble de nouveaux outils pour garantir une protection suffisante des renseignements personnels au Canada.

Tout d'abord, le commissaire devrait avoir le pouvoir d'imposer des amendes aux organisations dans des situations de non-conformité importante ou systémique aux obligations en matière de protection de la vie privée. Bien adaptées, de telles amendes peuvent avoir un effet dissuasif important qui n'existe pas actuellement dans le cadre de la LPRPDE. Elles représentent également des moments transparents de responsabilité qui sont importants pour que le public continue d'avoir confiance envers le régime de protection des données.

La boîte à outils devrait également inclure le pouvoir du commissaire de rendre des ordonnances exécutoires. Je suis sûre que vous êtes bien conscients que les commissaires du Québec, de l'Alberta et de la Colombie-Britannique disposent déjà de tels pouvoirs. À l'heure actuelle, le seul moyen de faire en sorte qu'une ordonnance exécutoire soit rendue dans le cadre de la LPRPDE, c'est de faire appel à la Cour fédérale, et seulement après qu'une plainte a franchi les étapes du processus interne du commissaire. C'est un chemin beaucoup trop long et complexe pour une ordonnance ayant force exécutoire, et cela requiert un investissement de temps et de ressources qui impose un fardeau injuste sur les plaignants.

Je souligne également que la LPRPDE ne fournit pas d'orientations générales sur les jugements en dommages-intérêts. La Cour fédérale s'est montrée extrêmement conservatrice à cet égard pour des infractions à la LPRPDE, et il est peu probable qu'il y ait d'autres effets dissuasifs que de dissuader les personnes qui se battent pour défendre leur droit à la vie privée. Il conviendrait d'accorder une attention particulière à l'établissement de paramètres pour des dommages non pécuniaires aux termes de la LPRPDE. À tout le moins, cela aiderait les plaignants non représentés à comprendre les limites de tout recours possible.

Merci. Je serai ravie de répondre à toutes les questions.

Le président: Merci beaucoup, madame Scassa.

C'est maintenant au tour de M. Martin-Bariteau, qui dispose de 10 minutes. Allez-y, s'il vous plaît.

M. Florian Martin-Bariteau (professeur adjoint, Section de common law, Faculté de droit, et directeur, Centre de recherche en droit, technologie et société, Université d'Ottawa, à titre personnel): Merci, monsieur le président.

• (1550)

[Français]

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, ou la LPRPDE, et de partager avec vous mes réflexions sur un sujet d'importance pour les Canadiennes et les Canadiens.

Je suis professeur adjoint en droit et technologie à la Section de common law de la Faculté de droit de l'Université d'Ottawa, où j'enseigne notamment le droit de l'économie numérique. Je suis aussi le directeur du Centre de recherche en droit, technologie et société. C'est néanmoins à titre personnel que je compare devant vous aujourd'hui.

Mes commentaires prendront pour point de départ la lettre que vous adressait le commissaire, le 2 décembre dernier. Je me concentrerai sur les questions des pouvoirs d'exécution et de réputation. Je m'intéresserai ensuite au champ d'application de la Loi, avant de terminer sur des réflexions relatives à son accessibilité et à sa lisibilité.

Tout au long de ma présentation, je ferai un lien avec le nouveau règlement général européen sur la protection des données, ou RGPD, notamment en raison des questions d'adéquation soulevées par le commissaire.

Sur la question des pouvoirs d'exécution, il m'apparaît essentiel de renforcer les pouvoirs du commissaire afin d'assurer l'efficacité de la Loi, notamment en lui octroyant des pouvoirs d'ordonnance et de sanction financière. La possibilité d'imposer des amendes semble la mesure la plus efficace pour assurer une réelle protection.

Comme pour tout, la protection des renseignements personnels fait l'objet d'une analyse coûts-avantages. Il s'agit aujourd'hui de choisir entre investir dans une protection dès la conception et l'éventualité de se faire taper sur les doigts. Face au risque de sanctions financières, l'analyse coûts-avantages basculera vers une protection dès l'origine. Évidemment, la détermination du montant de cette amende sera un paramètre essentiel de son efficacité; il faut un montant prohibitif. Par exemple, si une amende de 500 000 \$ peut sembler importante — et elle le sera pour les petites et moyennes entreprises —, elle sera négligeable pour des sociétés comme Amazon, Facebook ou Google. Ainsi, c'est par une amende de 22,5 millions de dollars que la Federal Trade Commission des États-Unis a amené Google à modifier son programme de publicité DoubleClick.

Pour être efficace face aux gros joueurs, il faudrait que le montant maximum de l'amende soit basé sur un pourcentage du chiffre d'affaires mondial, par exemple 1 %. Pour éviter que l'amende soit ridicule pour les petites et moyennes entreprises, on devrait également prévoir un deuxième seuil chiffré, par exemple 500 000 \$, la limite la plus élevée devant être retenue. Le RGPD se base d'ailleurs sur une telle approche mixte.

À mon sens, cela ne présente pas de risque d'atteinte à la relation de collaboration entre les acteurs et le commissaire. Au contraire, je suis d'avis que l'existence d'un pouvoir renforcé incitera les acteurs à une plus grande collaboration, en amont de tout dommage. Du reste, ces pouvoirs m'apparaissent nécessaires pour obtenir une décision d'adéquation au RGPD.

Pour éviter les apparences de conflit d'intérêts, les amendes devraient être payables au receveur général. Pour sécuriser les petites entreprises et pour ne pas freiner l'innovation, on pourrait par ailleurs prévoir une procédure d'avis de conformité préalable. En cas de dommage, il ne pourrait alors y avoir de sanction qu'après l'émission d'une recommandation qui n'aurait pas été suivie dans un délai raisonnable.

Finalement, je suis d'avis qu'aucun pouvoir du commissaire, y compris ceux d'ordonnance et de sanction, ne devrait être limité à la réception préalable d'une plainte formelle, l'ensemble de ces pouvoirs restant évidemment soumis à un possible contrôle judiciaire.

Concernant les droits des individus et la réputation en ligne, certains voudraient créer un « droit à l'oubli ». Telle qu'elle est imaginée et demandée par certains, je trouve la proposition dangereuse. L'Internet représente les archives et les bibliothèques de demain. C'est la nouvelle mémoire collective. On n'a jamais effacé les archives seulement parce qu'elles étaient dérangeantes, du moins pas légalement dans une démocratie. Il s'agit là d'un terrain dangereux, tout comme il serait également dangereux de vouloir déléguer un pouvoir de censure à des acteurs privés ou de ne donner le droit qu'à certains acteurs de décider ce qui doit être accessible ou non. Dans la même veine, le droit au « déréférencement » m'apparaît

illogique dans la mesure où l'on supprimerait l'entrée d'index, mais pas le contenu lui-même.

La législation sur la protection des renseignements personnels ne doit pas être un outil de gestion de la réputation pour faire disparaître ce qui est gênant, mais uniquement tout ce qui présente un caractère injustifié ou inexact. À défaut de cela, je ne suis pas certain que de tels mécanismes passeraient le test de la Charte.

Le réel problème du droit canadien est que la LPRPDE recommande, mais n'oblige pas en tant que telle la suppression des données inexactes ou non nécessaires. Certes, dans sa récente et déjà célèbre décision sur *Globe24h.com*, la Cour fédérale est venue contourner cette lacune par l'intermédiaire du caractère illégitime et non autorisé de la divulgation.

Il conviendrait néanmoins de rendre obligatoire, et non plus recommandable, la suppression des données dès lors qu'elles ne sont plus nécessaires ou à jour en encadrant plus strictement la rétention des données dans le temps. Je préciserai d'ailleurs que ce besoin ne concerne pas qu'Internet, mais bien toutes les bases de données, qu'elles soient informatisées ou non.

Il me semble encore que ces modifications seraient nécessaires, mais suffisantes, pour une adéquation au RGPD.

Au sujet du champ d'application, les Canadiennes et Canadiens devraient être assurés que toute cueillette, utilisation ou communication de données pouvant leur porter préjudice sont assujetties à des normes exigeantes de protection.

La détermination du champ d'application des deux lois fédérales ne répond pas à cette attente de protection des citoyens dans un monde global et interconnecté, notamment quant aux données protégées et, en particulier, à l'égard des organisations concernées.

Pour les organisations, une solution serait de redéfinir le champ d'application de la LPRPDE de manière négative, en la rendant applicable à toutes les organisations oeuvrant dans le champ de la compétence fédérale et non couvertes par la loi sur le secteur public ou une autre loi fédérale. Évidemment, et de manière similaire à nos partenaires, la loi devrait conserver les exceptions d'utilisation à des fins personnelles ou journalistiques.

En ce qui concerne le problème de l'accès au droit, s'il est certain que la loi a besoin d'ajustement pour s'adapter aux nouvelles réalités, le législateur devrait se saisir de l'occasion de cette réforme pour effectuer une réécriture complète de la loi, et non pas y apporter de simples amendements.

En effet, la LPRPDE appartient sans aucun doute au tableau d'honneur des lois les plus mal rédigées du corpus fédéral — et on sait pourtant qu'il y a là une certaine compétition. Le coeur de la LPRPDE se trouve dans une annexe, qui est le copier-coller d'un document rédigé par un organisme privé de normalisation. La loi ne vient que compléter ce document et les autres annexes en opérant des renvois incessants.

Cela pose un problème en termes d'accès au droit pour le public. Il serait ainsi approprié de refondre la loi en expliquant clairement les droits et obligations de chacun et, notamment, de rendre contraignant tout ce qui est aujourd'hui conditionnel.

En termes de rédaction, la loi devrait rester conçue selon un principe d'indépendance technologique et se fonder sur des principes d'application générale. Une telle approche est essentielle, afin de permettre au cadre juridique canadien de s'adapter aux évolutions sociales et technologiques à venir, notamment avec le développement de la robotique, de l'Internet des objets et de l'intelligence artificielle.

En termes de lisibilité, il serait également bon que la loi ne concerne que la protection des renseignements personnels. Les règles d'équivalence fonctionnelle pour les documents électroniques n'y ont pas leur place et devraient être transférées ailleurs.

À l'inverse, il serait souhaitable qu'une seule loi contienne tout le régime de protection des renseignements personnels, c'est-à-dire tant pour le secteur privé que pour le secteur public. La réouverture concomitante de l'étude de ces deux lois par ce comité, qui est d'ailleurs à souligner, en offre l'occasion. Cela permettrait d'ailleurs d'établir un cadre cohérent, tant pour la protection des renseignements personnels que pour le rôle du commissaire, quitte à prévoir plusieurs parties, notamment s'il était jugé nécessaire de conserver un régime dérogatoire pour le secteur public.

Je terminerai en attirant votre attention sur le besoin de prévoir des droits d'actions et des dommages et intérêts statutaires. De même, je soulignerai qu'il convient certes de mettre à jour notre droit pour passer le test d'adéquation du RGPD, mais qu'il faut néanmoins garder en tête deux paramètres importants. Tout d'abord, le test d'adéquation ne demande pas une copie carbone du RGPD et, ensuite, celui-ci concerne tous les régimes de protection et pas seulement la LPRPDE.

J'espère que ces quelques réflexions et recommandations seront utiles au Comité. Malheureusement, je n'ai pas été en mesure de finaliser à temps un court document bilingue avec mes exemples et recommandations. Néanmoins, je pourrai vous le communiquer par la suite.

Je vous remercie et je serais heureux de répondre à vos questions.

•(1555)

[Traduction]

Le président: Merci beaucoup.

Chers collègues, nous passons maintenant aux interventions de sept minutes.

C'est M. Bratina qui commence. Allez-y, s'il vous plaît.

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

Merci à tous.

Madame Scassa, j'ai aimé les mots que vous avez employés: un « ramassis de mesures alambiquées », un document auquel ont été apportées des « modifications ponctuelles ». Est-ce en raison du caractère dynamique de l'élaboration des lois — la technologie évolue et des éléments sont ajoutés — que le tout ne fonctionne pas, au bout du compte?

Mme Teresa Scassa: Je crois que c'est vraiment en raison de l'historique législatif de la Loi. Elle a vu le jour à une époque où il fallait adopter des mesures législatives rapidement. L'Europe venait d'adopter sa première directive sur la protection des données, et il y avait des préoccupations sur les flux transfrontaliers de données. Nous nous retrouvons dans une situation similaire aujourd'hui.

Il était évident que nous devions adopter des mesures. Les lois n'étaient pas très rassurantes. On a déterminé que si c'était fondé sur le code type de l'ACN, ce serait mieux accepté, tant ici qu'au sud de la frontière, pour ce qui est des obligations imposées aux entreprises.

Le noyau normatif, c'est le code type de l'ACN, qui se trouve dans l'annexe. La Loi en tant que telle contient toutes les exceptions et les modifications, de même que les pouvoirs d'application, etc. Pour un citoyen ordinaire qui essaie de s'y retrouver, ce n'est pas intuitif. Ce n'est pas facile à trouver. À mesure que des modifications y sont

apportées, il devient encore plus complexe de voir la correspondance entre les deux documents.

Je crois que c'est en grande partie en raison de cet historique que nous avons les dispositions actuelles. Je crois que nous avons suffisamment évolué maintenant dans notre parcours sur la protection de nos données pour pouvoir corriger la Loi.

•(1600)

M. Bob Bratina: Dans les témoignages, on nous a parlé du règlement général sur la protection des données de l'Union européenne. Toute proportion gardée, la LPRPDE ne va pas assez loin au chapitre du droit à l'oubli. Je vais poser ma question à M. Karanicolas, parce qu'il a fait une observation à ce sujet, mais je vais vous la poser d'abord.

Avez-vous examiné le règlement général sur la protection des données de l'Union européenne et qu'en pensez-vous, si on le compare à nos mesures?

Madame Scassa, je vous pose la question d'abord.

Mme Teresa Scassa: En ce qui concerne le droit à l'oubli, je ferais une distinction entre le droit à l'oubli, dont il est beaucoup question dans le contexte d'une décision de la cour dans l'Union européenne, et le droit à l'effacement, qui, je crois, correspond plus au contenu de la directive sur la protection des données. Je pense que ce sont des choses très différentes.

Le droit à l'oubli, dans un sens, va jusqu'à porter sur ce que les moteurs de recherche doivent rayer de la liste, de sorte que cela a une incidence sur la façon de faire des recherches et de trouver de l'information sur Internet. C'est très différent du droit des gens qui ne veut plus qu'une entreprise, avec laquelle ils ont déjà fait affaire et qui recueillait leurs renseignements personnels, ait leurs renseignements personnels parce qu'ils ne souhaitent plus faire affaire avec elle. Ils demandent que leurs renseignements personnels soient supprimés.

Le droit à l'oubli et le droit à l'effacement sont des choses très différentes. Le droit à l'effacement me semble visé par la LPRPDE, tandis que le droit à l'oubli va plus loin, et je crois que comme mon collègue l'a souligné, c'est lié aux droits relatifs à la liberté d'expression.

M. Bob Bratina: Monsieur Karanicolas, est-il possible de déterminer comment les données circulent? J'ai fait une observation l'autre jour au sujet des paradis fiscaux. Peut-il y avoir des paradis pour les données, que des gens peuvent glisser dans d'autres serveurs, cacher et utiliser à leur gré? La technologie vous permet-elle de suivre les données qui circulent?

M. Michael Karanicolas: Si je vous ai bien compris, je dirais qu'il est possible d'imposer des règles de localisation des données. Divers gouvernements ont essayé de différentes façons d'imposer ce type d'exigences.

Ce n'est pas nécessairement quelque chose que je recommanderais pour le Canada, mais il est possible de contrôler la façon dont l'information est acheminée. Ce type de mesures a tendance à soulever des préoccupations importantes sur la fonctionnalité et le fonctionnement d'Internet dans son ensemble, qui est conçu pour permettre la circulation de l'information par la voie la plus efficace.

Je ne sais pas si je réponds à votre question, ou si...

M. Bob Bratina: À mon sens, puisque la technologie évolue si rapidement, nous essayons de fixer un libellé dans les lois qui peut ne pas convenir pour la prochaine fonction technologique, ce qui aurait des effets indirects, si l'on veut.

M. Michael Karanicolas: D'accord.

La neutralité technologique est un objectif admirable. Je crois comprendre qu'à l'origine, l'objectif des auteurs de la LPRPDE était de faire en sorte que la Loi soit la plus neutre possible. Pour ce qui est de savoir s'ils ont réussi, c'est autre chose. Je crois que mes collègues ont soulevé de bons points, surtout concernant la mesure dans laquelle l'Internet des objets a changé en profondeur la collecte d'information. Il a créé toutes ces nouvelles possibilités qui dépassent largement ce que l'on concevait à l'époque où la LPRPDE a été rédigée.

De façon générale, je crois que la neutralité technologique dans les mesures législatives est un bon objectif. Dans l'élaboration d'une nouvelle loi ou la révision d'une loi existante, il faut chercher à éviter le plus possible de tomber dans ce piège.

M. Bob Bratina: Puis-je vous poser une question au sujet de vos observations sur le droit à l'oubli de l'Union européenne, etc.? Vous ne sembliez pas vraiment appuyer cette approche. D'autres témoignages allaient dans le sens inverse.

M. Michael Karanicolas: Je ne m'oppose pas fortement au droit à l'oubli. Je suis en quelque sorte indécis sur cette question. Je vois des arguments d'un côté comme de l'autre pour ce qui est de déterminer si tel type de droit est potentiellement une bonne idée, car je vois un problème et un changement dans la façon dont l'information est consignée, ce qu'a provoqué Internet.

Cela dit, il y a d'énormes problèmes concernant la façon dont c'est mis en oeuvre en Europe, en partie parce que la décision, lorsque la Cour européenne de justice l'a rendue, n'était pas très claire quant à l'application. Il y avait de vastes catégories quant à ce qui pouvait être lié au droit à l'oubli, ce qui a semé beaucoup de confusion. Je crois qu'aux dernières nouvelles, 150 000 ou 170 000 sites Web ont été retirés en raison de cela. Énormément de demandes ont été soumises.

J'ai des réserves quant à la manière dont les choses ont été mises en oeuvre, quant au manque de clarté. Je m'interroge également sur le bien-fondé de regrouper cela avec les moteurs de recherche. En tant qu'acteurs du secteur privé, ils sont mal équipés pour ce type d'équilibrage. Lorsqu'on leur impose cette responsabilité possible, sans qu'il n'y ait nécessairement de processus permettant de respecter les intérêts liés à la liberté d'expression en cause, on se retrouve avec une tendance à ce que l'information soit retirée chaque fois qu'il y a une plainte. C'est une approche qui pose problème.

•(1605)

Le président: Merci beaucoup.

C'est maintenant au tour de M. Jeneroux, qui dispose de sept minutes.

M. Matt Jeneroux (Edmonton Riverbend, PCC): Je vous remercie tous les trois, soit de revenir comparaître devant nous, dans le cas de deux d'entre vous; soit de comparaître pour la première fois, dans le cas de M. Martin-Bariteau. Bienvenue.

Je voulais tout d'abord vous demander ce que vous pensiez de la LPRPDE, mais c'est très clair. Personne ici n'est très satisfait de la Loi, et je vais donc poser ma deuxième question.

En ce qui concerne le pouvoir de rendre des ordonnances, madame Scassa, vous avez exprimé clairement votre opinion dans

votre dernière réponse, mais est-ce que ces deux messieurs peuvent également nous dire, pour le compte rendu, ce qu'ils pensent de l'idée d'accorder au commissaire à la protection de la vie privée le pouvoir de rendre des ordonnances?

Allez-y en premier, monsieur Martin-Bariteau.

M. Florian Martin-Bariteau: Je ne suis pas sûr de comprendre...

[Français]

Comme ma collègue Teresa Scassa, je suis entièrement favorable à l'idée qu'on donne un pouvoir d'ordonnance au commissaire.

[Traduction]

M. Matt Jeneroux: Monsieur Karanicolas.

M. Michael Karanicolas: Je ne suis pas totalement convaincu qu'il faille lui donner le pouvoir de rendre des ordonnances. Je ne m'y oppose pas nécessairement, mais je crois que cela soulève certaines questions liées à l'équité procédurale pour les enquêtes, ce que le CPVP a lui-même mentionné.

À mon avis, il faut se demander si c'est nécessaire. Je crois que si je ne suis pas complètement convaincu concernant le pouvoir de rendre des ordonnances, c'est que le commissaire à la protection de la vie privée a dit que la plupart des recommandations sont respectées, au bout du compte. S'il en est ainsi, et si on donne déjà suite aux recommandations dans le cadre du système, j'ignore pourquoi il faudrait renforcer les pouvoirs.

Il a été mentionné qu'on tarde souvent à appliquer les recommandations, ce qui est un problème important. Certaines personnes ont proposé un modèle hybride par lequel il faudrait que les entreprises demandent à la cour la permission de ne pas se conformer pendant une certaine période. Je ne comprends pas très bien pourquoi un pouvoir de rendre des ordonnances réglerait le problème plus qu'un modèle hybride, et je crois que c'est la raison pour laquelle, bien que je ne m'oppose pas nécessairement à l'idée, je ne suis pas totalement convaincu de la nécessité d'accorder un pouvoir de rendre des ordonnances.

M. Matt Jeneroux: Nous allons revenir sur certaines de vos réponses, monsieur Karanicolas. Je pense au droit à l'oubli; vous semblez incertain à ce sujet. Il semble que le commissaire à la protection de la vie privée ait aussi du mal à déterminer le type de loi à mettre en oeuvre, le cas échéant. Je trouve cela fascinant. Certaines personnes veulent être oubliées tandis que d'autres veulent qu'on se souvienne de ces personnes.

Votre argument n'était pas clair. Je vais commencer par vous puis nous ferons un tour de table pour voir si quelqu'un peut nous éclairer ou nous aider. Le commissaire à la protection de la vie privée présentera un exposé de position à ce sujet, mais notre étude sera malheureusement terminée à ce moment-là. Nous cherchons à obtenir des conseils ou du soutien en ce qui a trait à nos recommandations à l'intention du commissaire à la protection de la vie privée.

M. Michael Karanicolas: À l'heure actuelle, je ne recommanderais pas le droit à l'oubli.

La raison pour laquelle je suis un peu vague, c'est que je vois que cela permettrait de régler certains problèmes, mais si vous voulez que je me prononce sur la légifération du droit à l'oubli, je serais contre. Je crois que les possibilités de causer des préjudices ou de rédiger la loi d'une façon qui aurait une incidence négative sur la liberté d'expression sont énormes.

Je suis conscient du problème, mais il y a tellement de possibilités de mal faire, et c'est ce qui m'inquiète.

• (1610)

M. Matt Jeneroux: C'est un peu mieux.

Madame Scassa.

Mme Teresa Scassa: Je vais préciser la distinction que je fais entre le droit à l'oubli et l'effacement des données.

Disons que vous vous inscrivez à un site de réseautage social, que vous avez créé un profil, que vous avez ajouté des photos et que vous présentez certains renseignements sur votre profil; ou disons que vous avez créé un profil sur un site de rencontre. Vous y êtes inscrit depuis quelques années, puis vous décidez que vous ne voulez plus y être. Vous ne voulez plus faire affaire avec l'entreprise — cela arrive tout le temps — et vous lui dites: « Supprimez mon compte et détruisez mes renseignements personnels, parce que c'est terminé pour moi. » C'est le droit à l'effacement des données, qui diffère du droit à l'oubli.

Vous ne dites pas qu'on a publié certains articles à votre sujet et que vous voulez qu'on cesse de les lire, qu'ils soient retirés du répertoire. Vous dites que vous avez eu une relation avec une entreprise du secteur privée, que vous y mettez un terme et que vous voulez que les données que vous avez fournies dans le cadre de cette relation soient supprimées. De nombreuses personnes ont eu du mal à faire respecter ce droit: le droit à l'effacement des données.

Je crois que ce droit est très important. Il serait important d'accroître le droit des personnes de prendre ces mesures avec les organisations du secteur privé qui recueillent et utilisent leurs renseignements personnels.

J'ai toutefois des réticences en ce qui a trait au droit à l'oubli.

M. Matt Jeneroux: Très bien.

Si je peux me permettre — et j'espère que M. Martin-Bariteau interviendra également —, disons qu'un jeune de 16 ans publie quelque chose sur sa page Facebook. Ensuite, 20 ans plus tard, cette personne décide de se lancer dans la course pour un siège au Parlement, par exemple. Même si elle a passé un tel contrat avec l'entreprise, il se peut que quelqu'un ait fait une saisie d'écran de cette publication et qu'on en fasse une nouvelle. Je crois que c'est ce qui me dérange à propos du droit à l'oubli. Le problème, ce n'est pas nécessairement le contrat avec l'entreprise, mais bien les répercussions publiques qui s'en suivent.

J'ai utilisé l'exemple d'un député seulement parce que c'est un problème courant. Je suis certain que vous en conviendrez.

Mme Teresa Scassa: Je crois que c'est aussi un problème grave. Je ne sais pas s'il relève de la LPRPDE. Certains cas ont été réglés par l'entremise du système de responsabilité civile délictuelle ou quasi-délictuelle, en cas d'intentions malveillantes, et on utilise aussi d'autres mécanismes. Je crois que cela dépasse la simple protection des données.

Bien que je convienne qu'il s'agit d'un enjeu important, je ne suis pas totalement convaincue que cela relève de la LPRPDE, puisqu'il faut avoir recours à diverses solutions, selon les circonstances. La pornographie vengeresse fait partie de cette catégorie. Il s'agit clairement de malveillance et donc peut-être d'une activité criminelle.

M. Matt Jeneroux: Je crois que mon temps est écoulé.

Le président: Absolument, mon ami.

Des voix: Oh, oh!

Le président: Monsieur Blaikie, vous disposez de sept minutes.

M. Daniel Blaikie (Elmwood—Transcona, NPD): Merci beaucoup.

Monsieur Karanicolas, j'aimerais vous poser quelques questions au sujet du droit à l'oubli. Vous avez dit que les choses ne s'étaient pas bien passées en Europe à cet égard. Pourriez-vous, aux fins du compte rendu, nous donner quelques exemples des ratés dans le contexte européen?

M. Michael Karanicolas: Je veux d'abord souligner la distinction faite par Mme Scassa entre la protection des données, le droit à la suppression et le droit à l'oubli, parce que c'est une distinction importante.

Le premier problème avait trait à la façon de rendre la décision. Dans sa décision, la Cour européenne de justice ne faisait même pas mention de la liberté d'expression et énonçait par exemple que le droit à la vie privée l'emportait habituellement sur le droit à l'information. On n'a pas suffisamment tenu compte des droits qui étaient compromis. C'est la première chose. Cette décision, qui était assez minimale, et qui constituait la seule ligne directrice que pouvait utiliser Google — du moins au départ —, était très problématique, parce qu'on créait cette énorme responsabilité sans créer des lignes directrices appropriées sur la façon de la mettre en oeuvre.

Comme je l'ai dit rapidement plus tôt, le fait d'imposer cette responsabilité au secteur privé est très problématique, parce qu'il s'agit d'une décision très délicate. Il faut opposer certains droits à d'autres et tenir compte de l'intérêt public général. L'entreprise Google, malgré sa grande taille, n'est absolument pas outillée pour faire cela. Il faut des décideurs judiciaires ou quasi judiciaires pour le faire. C'était donc une erreur importante. On venait d'ouvrir les vannes. J'ai fait des recherches et j'ai constaté que Google avait reçu 348 000 demandes de suppression de liens.

Je crois que dans certains cas restreints, on pourrait appliquer le droit à l'oubli et j'éprouve de la sympathie pour les personnes visées, mais je crois qu'il serait difficile d'appliquer la loi à ces cas extrêmes seulement. Je crois que l'exemple européen montre qu'une fois qu'on établit ce droit, on ouvre les vannes et on se retrouve avec des demandes de suppression pour des renseignements tout à fait légitimes, exacts ou pertinents.

• (1615)

M. Daniel Blaikie: C'est une décision de la Cour européenne de justice. Je ne connais pas ce sujet en détail; est-ce que la réglementation générale sur la protection des données aborde le droit à l'oubli?

M. Michael Karanicolas: Ma compréhension à l'égard de l'application de la loi se fonde sur la décision initiale de la Cour européenne de justice. Je crois que le règlement sur la protection des données aborde cette question, mais je n'ai pas étudié cet élément en particulier.

M. Daniel Blaikie: Pour moi, la prochaine question — et peut-être que les témoins ont une opinion à ce sujet — est la suivante: on se demande si nos lois en matière de protection de la vie privée sont adéquates et respectent les critères européens, afin de ne pas nuire au flux de données commerciales; est-ce que le droit à l'oubli est un élément essentiel pour répondre aux critères européens?

[Français]

M. Florian Martin-Bariteau: Non. Absolument pas.

Même dans le nouveau RGPD, qui aborde la question du droit à l'oubli, c'est entre guillemets. On le nomme dans ce contexte « droit à l'effacement ». Le Règlement fait la distinction que précisait la professeure Scassa. En fait, le droit à l'effacement prévu dans le RGPD est passablement conforme à celui qui existait déjà dans la directive de 1995 et qui était en vigueur dans la plupart des pays de l'Union européenne.

On peut demander la suppression des données, mais uniquement de celles dont la collecte, la communication ou la divulgation constituent une violation au Règlement. Or celui-ci prévoit des exceptions quant à la liberté d'expression, la liberté de la presse, le droit à l'information et ainsi de suite.

M. Daniel Blaikie: Le droit à l'effacement existe déjà au Canada. Or je me demande s'il cadre avec le modèle européen ou s'il faudrait créer cette possibilité.

M. Florian Martin-Bariteau: Comme la professeure Scassa, je pense qu'il faudrait inclure de manière claire dans la LPRPDE le droit à l'effacement des données inexactes et erronées, de façon à ce qu'il ne s'agisse pas d'une simple recommandation.

J'aimerais aussi préciser que le deuxième paragraphe de l'article 45, qui parle d'adéquation, ne demande pas d'effectuer un copier-coller, mais plutôt de considérer les droits effectifs et opposables. Des droits directs seraient donc appropriés. En matière de protection des données, cela ne vise pas directement un quelconque droit à l'effacement, mais indique que les règles du pays concerné en matière de droits de l'homme et de libertés fondamentales seront prises en compte. Dans le cas qui nous concerne, on parle de la Charte canadienne des droits et libertés.

[Traduction]

M. Daniel Blaikie: Merci.

J'aimerais obtenir quelques conseils pratiques au sujet du consentement. Je crois qu'il est assez clair que le modèle actuel en matière de consentement ne fonctionne pas très bien. Quiconque a voulu télécharger un logiciel sur Internet et a dû accepter un contrat d'utilisation sait que ces contrats sont opaques, longs et techniques. Même si on les lit, ils sont si vastes qu'on a l'impression de signer n'importe quoi lorsqu'on clique sur « J'accepte ».

Comment fait-on pour établir un modèle qui ne soit pas trop normatif, mais qui offre tout de même des renseignements que peuvent comprendre les Canadiens ordinaires qui n'ont pas d'expérience avec ce type de loi afin qu'ils soient à l'aise de donner leur accord? Est-ce qu'on peut établir des ententes types ou est-ce qu'elles sont trop normatives et risquent de ne pas correspondre aux services qui sont offerts? Comment peut-on rédiger une loi qui donne lieu à un modèle de consentement viable?

● (1620)

Mme Teresa Scassa: C'est une très bonne question.

C'est difficile. Je crois qu'on peut corriger certaines petites choses, avec des outils et des lignes directrices pour rédiger de meilleures politiques sur la protection de la vie privée et des modèles plus condensés ou plus courts, comme vous le proposez.

En ce qui a trait à la collecte omniprésente et continue, on a proposé de faire apparaître une fenêtre contextuelle de temps en temps pour rappeler aux gens qu'on recueille leurs renseignements afin qu'ils décident s'ils souhaitent que cela continue. Certaines de ces mesures pourraient être prévues par la loi et d'autres pourraient être intégrées aux lignes directrices du commissaire à la protection de la vie privée.

Comme vous le savez, d'autres personnes proposent des solutions plus vastes, comme la collecte de toutes sortes de renseignements de façon régulière, sans demander le consentement. Ce qui m'inquiète là-dedans, c'est le seuil voulant qu'il n'y ait aucun risque et aucun préjudice. Je crois que dans le contexte des métadonnées, on tente toujours de déterminer de façon exacte ce que sont ces risques et ces préjudices. Les conséquences de la collecte de certains types de données ne sont pas toujours évidentes dès le départ, et varient selon les renseignements qui sont recueillis et réunis par la suite.

Je crois que les défis sont très importants et j'aimerais pouvoir dire: « Voici les trois choses à faire pour régler la situation », mais j'ai du mal à bien comprendre la situation moi-même.

Le président: Le temps de parole de M. Blaikie est écoulé, mais je sais que d'autres intervenants pourront revenir sur le sujet s'ils le souhaitent.

La parole est maintenant à M. Saini, pour la dernière intervention de sept minutes.

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

J'aimerais aborder un point pour commencer. Comme il a récemment signé l'AECG, le Canada subira des pressions afin d'atteindre le niveau du Règlement général sur la protection des données, qui entrera en vigueur en mai 2018 en Europe. Il y a des différences marquées entre ce qui est en place aujourd'hui et ce qui est prescrit par le Règlement. Je pense notamment à l'effacement des données et à la protection de la vie privée intégrée dès la conception et par défaut.

Pourriez-vous nous donner une idée des éléments importants que nous devrions aborder? Je suppose qu'au bout du compte, il faudra atteindre ce niveau pour faire affaire avec l'Europe. Y a-t-il des indicateurs clés sur lesquels nous devrions nous concentrer?

Mme Teresa Scassa: Je vais céder la parole à notre résident européen.

Des députés: Oh, oh!

M. Raj Saini: J'ai beaucoup de questions. Je peux en poser une autre.

[Français]

M. Florian Martin-Bariteau: À mon avis, dans la LPRPDE, il faudrait clarifier la question de la rétention des données dans le temps, prévoir une obligation à la charge des organisations et également donner un droit direct aux justiciables. Les droits directs des justiciables sont l'une des conditions de l'adéquation. Comme pour ce qui est des pouvoirs d'ordonnance et d'amende, c'est l'alinéa 45(2)b du Règlement qui nous dit qu'on va regarder si l'autorité de contrôler est vraiment indépendante et a des pouvoirs appropriés d'application.

[Traduction]

M. Raj Saini: Madame Scassa, voulez-vous ajouter quelque chose?

Mme Teresa Scassa: Oui. Je suis d'accord. Je crois que la plus grande faiblesse de la LPRPDE en ce qui a trait à la conformité aux normes européennes, c'est le volet de l'application de la loi. Le commissaire n'a tout simplement pas assez de pouvoirs.

M. Raj Saini: Monsieur Martin-Bariteau, vous avez parlé d'une structure d'amendes en Europe, en vertu du Règlement général sur la protection des données. Les amendes représentent 4 % du roulement annuel ou 29 millions d'euros, le plus élevé des deux montants étant retenu. Croyez-vous que nous devrions utiliser un tel mécanisme? À l'heure actuelle, comme vous l'avez si bien dit, nous n'avons aucune procédure à cet égard. Le Commissariat à la protection de la vie privée ne peut pas imposer d'amendes.

Madame Scassa, dans vos écrits, vous faites référence à Globe24h. Dans ce cas en particulier, l'amende imposée n'était que de 5 000 \$ et il n'y avait aucun moyen de récupérer cet argent ou même d'empêcher la Roumanie d'indexer les dossiers du site Web de CanLII.

Croyez-vous qu'on devrait imposer des amendes, et si oui, dans quelle mesure?

[Français]

M. Florian Martin-Bariteau: Je crois que le mécanisme mixte du RGPD est le bon, quel que soit le pourcentage, parce que même à 4 %, je crois que c'est aussi calculé en fonction du nombre de citoyens concernés par les éventuels bris de confidentialité et en fonction du territoire.

On sait qu'il y a moins de citoyens à l'intérieur des frontières canadiennes qu'à l'intérieur de celles de l'Union européenne. Par contre, c'est important de ne pas avoir un simple pourcentage, parce que 4 % d'une petite structure, par exemple d'une entreprise en démarrage, ce n'est pas grand-chose. Cette entreprise pourrait vouloir prendre le risque avec ses investisseurs et leur dire de se lancer. Si jamais il se passait quelque chose, au maximum, cela pourrait être environ 4 % de 500 000\$. Ce n'est rien. C'est pour cela qu'il faut établir le double.

Par exemple, en France, jusqu'en 2016, le montant maximum était de 150 000 \$ à la première sanction et de 300 000 \$ par la suite. Cela n'avait aucune efficacité. La France vient donc de monter cela uniquement à 3 millions de dollars. Cela a été adopté quasiment en même temps que le Règlement, ce qui montre aussi selon moi la prise en compte du nombre de citoyens concernés à l'intérieur des limites d'un territoire.

•(1625)

[Traduction]

M. Raj Saini: Madame Scassa, dans votre déclaration préliminaire, vous avez parlé des entreprises. À l'heure actuelle, la

différence entre le Règlement général sur la protection des données et la loi canadienne, c'est que nous n'avons pas de mécanisme de protection de la vie privée dès la conception ou par défaut. Croyez-vous que c'est important ou s'agit-il d'une première étape pour veiller non seulement à ce que les entreprises respectent le Règlement dans une certaine mesure, mais aussi à garantir une certaine pertinence?

Vous avez parlé des PME. Croyez-vous qu'il faudrait créer une sorte de document ou d'entente en matière de protection de la vie privée qui serait la norme sur Internet, dans la mesure du possible, et qu'on pourrait par le fait même utiliser des marques de confiance garantissant la protection de la vie privée? De cette façon, nous aiderions les consommateurs, qui sauraient que ces entreprises ont recours à un mécanisme de protection de la vie privée dès la conception ou par défaut et, de façon plus importante, qu'elles ont reçu la marque de confiance d'un organisme à cet égard. Est-ce qu'une telle solution serait viable?

Mme Teresa Scassa: Je sais qu'après l'entrée en vigueur de la LPRPDE, on a beaucoup parlé des marques et des sceaux de confiance. Ils ont été utilisés, mais pas dans une large mesure. Je crois qu'on craignait la contrefaçon des marques et des sceaux de confiance. Je ne sais pas à quel point il s'agit d'une solution viable.

Il y a des progrès technologiques qui sont intéressants. On travaille actuellement à l'élaboration de codes et d'applications, par exemple, qui serviront à évaluer les politiques en matière de protection des renseignements personnels. J'hésiterais à adopter la solution des marques de confiance, alors qu'il pourrait exister d'autres outils technologiques plus utiles et plus efficaces pour aider les consommateurs à comprendre les politiques en matière de protection de la vie privée.

Cela étant dit, je sais que, depuis un certain temps, on parle de la protection de la vie privée dès la conception et de la protection des renseignements personnels par défaut. Ce sont là des principes importants, mais il faudra peut-être modifier la loi pour que les gens s'y intéressent.

M. Raj Saini: D'accord.

Monsieur Karanicolas, vous avez mentionné que Google avait reçu 350 000 ou 340 000 demandes concernant le droit à l'oubli. De ce nombre, 42 % ont été acceptées. Vous avez fait allusion à une affaire en Europe, et je crois que vous faisiez probablement référence à l'affaire mettant en cause Google et un Espagnol. Est-ce bien cela?

M. Michael Karanicolas: C'est la première affaire dont a été saisie la Cour européenne de justice.

M. Raj Saini: Pensez-vous que cette affaire et la décision qui a été rendue devraient être utilisées d'une certaine façon? Le jugement était clair en ce qui concerne le droit à l'oubli et le droit à l'effacement. Trouvez-vous ce jugement satisfaisant, et devrions-nous nous en servir ou non?

M. Michael Karanicolas: Non. Le jugement qui a été rendu dans cette affaire en particulier est tout à fait insatisfaisant. C'est ce dont je parlais en ce qui concerne le manque de clarté et la solution proposée.

En outre, dans ce cas-là, je ne crois pas qu'il s'agit d'une très bonne cause type relativement au droit à l'oubli. À mon avis, les renseignements dont il était question, c'est-à-dire la faillite ou les difficultés financières de la personne qui remontent à 15 ou 20 ans, sont tout à fait pertinents. Cette information ne devrait pas être supprimée. Je crois que ce qu'ils...

M. Raj Saini: Mais...

Le président: Mais votre temps est écoulé, monsieur Saini.

Des voix: Oh, oh!

Le président: Monsieur Kelly, vous disposez de cinq minutes.

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

En écoutant les témoins que nous avons reçus jusqu'à maintenant, y compris ceux d'aujourd'hui, je m'étonne du nombre considérable d'organisations différentes qui sont assujetties à la loi et du nombre de situations et d'exemples différents qui sont couverts par cette même loi. Pourtant, elle est pratiquement inutile pour certains secteurs d'activité et certains types d'entreprises. Je pense notamment à des cabinets d'avocats, des entreprises de services financiers, des firmes comptables et des entreprises de courtage hypothécaire, car j'étais courtier hypothécaire avant d'être élu député. Ce sont là des entreprises qui ont compris depuis très longtemps la nécessité de protéger les renseignements personnels de leurs clients. Elles n'essaient pas de rendre publics ces renseignements ni d'en tirer profit en faisant cela. Elles iraient totalement à l'encontre de tous les principes qu'on respecte dans les nombreuses professions différentes qui impliquent de recueillir des renseignements personnels, et pourtant, cette loi s'applique également aux réseaux sociaux, dont le produit est la communication de renseignements.

Devons-nous avoir deux lois différentes? La protection des renseignements personnels et de la vie privée est une chose, et il me semble que la protection des données électroniques, ou la communication délibérée de renseignements électroniques, est une tout autre chose.

J'aimerais que vous me disiez si, selon vous, il faudrait avoir deux lois étant donné les différents types d'activités qu'on tente de réglementer.

• (1630)

Mme Teresa Scassa: Je peux répondre.

Je crois que créer deux lois comporterait certains dangers. Au fil du temps, le commissariat a cherché de plus en plus à fournir des lignes directrices propres à des secteurs ou à des situations en particulier, de sorte qu'il n'y ait qu'une seule loi qui s'applique à tous, mais qui s'applique différemment selon les situations. Le commissariat s'est intéressé aux applications mobiles, aux appareils pour la mise en forme et à divers éléments précis pour fournir une orientation aux petites entreprises et aux entreprises qui oeuvrent dans des secteurs en particulier.

On accorde de plus en plus d'attention à l'idée d'élaborer des codes de pratique. Certains secteurs pourraient élaborer conjointement des codes de pratique visant la collecte, l'utilisation et la divulgation de certains types d'information dans le cadre d'activités particulières. Ces codes pourraient être élaborés en collaboration avec le commissariat et approuvés par celui-ci. On contribuerait ainsi à établir des normes et des lignes directrices pour des secteurs en particulier sous l'égide d'une seule loi et d'un seul commissariat. Il me semble que cette approche serait préférable à la mise en oeuvre de deux lois distinctes.

Il faut aussi penser, bien entendu, que certaines entreprises qui ont d'abord pignon sur rue se lancent ensuite dans le commerce électronique et conçoivent des applications. Les besoins en renseignements et les pratiques en matière de traitement de l'information des entreprises évoluent constamment.

M. Florian Martin-Bariteau: Je n'ai rien à ajouter.

M. Pat Kelly : D'accord.

Monsieur Karanicolas.

M. Michael Karanicolas: [*Note de la rédaction — inaudible*] se fier aux incitatifs commerciaux ou penser que les entreprises qui ont tout intérêt à protéger les renseignements de leurs utilisateurs ou à adopter des pratiques exemplaires le feront nécessairement. Ashley Madison est un excellent exemple d'une entreprise qui avait tout intérêt à appliquer des mesures rigoureuses pour protéger les renseignements personnels, mais qui ne s'était pas dotée de telles mesures et qui n'appliquait aucune des pratiques exemplaires de l'industrie pour protéger les renseignements personnels et la vie privée des utilisateurs.

Je ne crois pas que favoriser une certaine souplesse...

M. Pat Kelly: Si vous me le permettez, j'aimerais parler de cet exemple. Je ne sais pas exactement comment il y a eu atteinte. Est-ce à cause d'une lacune dans la loi ou simplement d'une lacune au sein de cette entreprise en particulier?

M. Michael Karanicolas: Il est certain que c'est en raison d'une lacune au sein de cette entreprise, mais je crois qu'on pourrait dire que le fait que cette entreprise pouvait fonctionner de cette façon, avec une telle négligence, est potentiellement attribuable à une lacune dans la loi ou dans son application en ce sens que des erreurs fondamentales ont été commises parce qu'il n'y a pas nécessairement eu de surveillance ou de suivi.

Le président: Je vous remercie beaucoup, monsieur Kelly.

La parole est maintenant à M. Long pour cinq minutes.

M. Wayne Long (Saint John—Rothsay, Lib.): Je vous remercie, monsieur le président.

Je souhaite à nouveau la bienvenue à certains de nos témoins, et je souhaite la bienvenue pour la première fois à M. Martin-Bariteau.

Monsieur Karanicolas, j'aimerais m'adresser d'abord à vous au sujet du consentement valable et de la façon dont il s'applique aux enfants.

J'ai parlé de cela lors de notre dernière réunion. J'ai des amis qui ont de jeunes enfants. Nous étions chez eux la fin de semaine dernière. Leurs enfants étaient à l'ordinateur et cliquaient ici et là. Quelles mesures doit comporter la LPRPDE pour assurer la protection de nos enfants?

Je vais commencer par vous, monsieur Karanicolas, et ensuite Mme Scassa pourra répondre.

• (1635)

M. Michael Karanicolas: On reconnaît très bien qu'il faut mettre en place des règles distinctes pour protéger les enfants pour ce qui est de recueillir leurs renseignements et d'en suivre la trace. Je crois qu'il est très difficile d'appliquer ces règles, car il n'est vraiment pas facile de savoir l'âge d'une personne qui navigue dans un site Web en particulier. On peut lui demander d'entrer sa date de naissance, mais ce n'est pas un obstacle qui est particulièrement difficile à surmonter...

M. Wayne Long: Je vais intervenir, si vous me le permettez.

J'ai lu récemment dans un article qu'un grand nombre de sites Web américains comportent davantage de pièges à clics pour les enfants que pour les adultes. Encore une fois, que pouvons-nous faire pour assurer la protection de nos enfants?

M. Michael Karanicolas: Étant donné qu'on ne peut pas nécessairement connaître l'âge de l'internaute, je crois que la meilleure solution est d'exiger que des normes supérieures soient imposées aux sites Web destinés aux enfants ou qui s'adressent principalement à de jeunes utilisateurs.

M. Wayne Long: Je vous remercie.

Madame Scassa.

Mme Teresa Scassa: Les États-Unis ont choisi de mettre en oeuvre des lois qui visent précisément la protection des renseignements personnels des enfants. Au Canada, nous avons décidé d'utiliser la LPRPDE et de reconnaître que les enfants constituent un groupe particulier aux fins de l'interprétation de la loi, et c'est pourquoi nous tenons compte du fait qu'un site Web pourrait viser les enfants.

Je crois qu'il faut se demander si nous voulons que la loi comporte des dispositions très précises qui démontrent clairement que, lorsqu'il s'agit d'enfants, les règles sont différentes ou plus strictes. Je crois que ce serait justifié de préciser très clairement que les règles concernant le consentement sont différentes lorsqu'il s'agit d'enfants.

Il est profitable pour nous dans une certaine mesure que de nombreux sites Web destinés aux enfants se trouvent aux États-Unis, où ils doivent respecter les lois américaines. Au Canada, nos lois ne sont pas claires et précises à propos des mesures qu'il faut prendre pour protéger les renseignements personnels des enfants.

M. Wayne Long: Monsieur Martin-Bariteau.

[Français]

M. Florian Martin-Bariteau: Je dirais la même chose. Il y a déjà la loi américaine qui existe, mais il y a un problème d'application. Cela ne fonctionne pas. On sait très bien que normalement, en bas de l'âge de 13 ans, il y a des règles supplémentaires qui s'appliquent. Les enfants de moins de 13 ans sont présents sur tous les réseaux sociaux en Amérique, comme dans le reste du monde.

[Traduction]

M. Wayne Long: Je vous remercie.

Monsieur Karanicolas, j'aimerais obtenir votre opinion au sujet de la décision rendue dans l'affaire impliquant Globe24h. Je vais être honnête avec vous. Je ne connais pas bien cette décision, mais à mon avis, elle ouvre la voie à une version canadienne du droit à l'oubli. Pouvez-vous en dire plus long à l'intention du Comité au sujet de Globe24h et des répercussions de la décision?

M. Michael Karanicolas: Je n'ai pas examiné cette affaire et je n'ai pas pu la décision. J'ai seulement lu des comptes rendus.

Je peux dire que ce qui m'a frappé à propos de cette affaire, c'est qu'elle met en évidence certaines des difficultés que posent ce genre d'affaires qui concernent plus d'un pays. Cette situation ne vise pas uniquement le droit à l'oubli. Elle a des répercussions sur ce qui est diffusé en ligne, car il y a des difficultés en ce qui concerne l'application de la loi et l'imposition d'une norme canadienne aux sites Web exploités à l'étranger mais qui visent les Canadiens.

M. Wayne Long: Madame Scassa, avez-vous un commentaire à formuler?

Mme Teresa Scassa: Oui. J'hésiterais à dire que cette décision contribue à créer un droit à l'oubli au Canada. Dans cette situation particulière, il s'agissait de décisions judiciaires qui avaient été rendues publiques par les tribunaux en vertu de conditions précises qui n'ont pas été respectées, et...

M. Wayne Long: Ces décisions étaient accessibles, mais elles n'étaient pas recensées par Google, n'est-ce pas?

Mme Teresa Scassa: C'est exact. Elles étaient accessibles, mais elles n'étaient pas indexées, et les tribunaux les ont rendues accessibles à condition qu'elles ne soient pas indexées.

M. Wayne Long: D'accord. C'est bien.

Mme Teresa Scassa: Elles ont été indexées par ce site. J'hésiterais à dire qu'il s'agit véritablement d'une affaire concernant le droit à l'oubli.

Le président: Je vous remercie beaucoup.

La parole est de nouveau à M. Kelly pour cinq minutes.

M. Pat Kelly: Je vous remercie.

Lorsque nous parlons du droit à l'oubli, cette version de ce droit — être désindexé par un moteur de recherche — semble être davantage un droit d'être perdu qu'un droit d'être oublié. Ce n'est certes pas un effacement. Je suis heureux qu'on fasse finalement la distinction entre ces différents éléments.

Madame Scassa, j'ai été ravi de vous entendre dire durant votre exposé et aux fins du compte rendu que la LPRPDE est lourde pour les petites entreprises, et certainement impopulaire, probablement mal comprise et, je dirais, probablement une source d'appréhensions. Les propriétaires de petites entreprises avec lesquels je me suis entretenu ne connaissent pas bien la loi sur la protection des renseignements personnels. Ils savent qu'elle existe, mais dans bien des cas, ils ne savent probablement pas comment s'y conformer, et il est vrai effectivement que de nombreuses entreprises ne peuvent pas compter sur les conseils d'un expert relativement à la façon de s'y conformer, comme vous l'avez mentionné dans votre exposé.

Par ailleurs, dans votre déclaration, vous avez dit que le modèle axé sur le consentement est une vraie farce. Alors, quelle est la solution?

• (1640)

Mme Teresa Scassa: Je ne le sais pas, mais je sais par contre qu'en ce moment-même un très grand nombre de mes renseignements personnels sont en train d'être rassemblés et transmis probablement par mon téléphone, des renseignements que je ne veux pas communiquer. Je ne sais même pas de quels renseignements il s'agit ni de quelle façon ils ont été obtenus. C'est pour cette raison que je trouve que le consentement est une vraie farce, car même une personne qui possède une formation juridique et qui travaille dans le domaine de la protection des renseignements personnels ne peut pas comprendre ce qui se passe avec ses renseignements personnels. Cela m'indique que le système ne fonctionne pas.

Comment faire en sorte qu'il fonctionne? Je crois que la consultation menée par le commissariat a donné lieu à des suggestions, à des idées et à des possibilités intéressantes. Je crois qu'il suffit d'essayer de trouver la bonne combinaison. Je ne sais pas quoi vous répondre, je suis désolée. J'aimerais vraiment pouvoir vous dire quelle solution serait efficace.

M. Pat Kelly: La relation entre les consommateurs et les entreprises devrait à coup sûr être fondée sur le consentement.

Qu'il s'agisse d'aller à la salle de quilles, de souscrire un emprunt hypothécaire, de signer un contrat pour un téléphone cellulaire ou de décider d'afficher certaines photos dans Facebook, il est vrai que les fournisseurs de services doivent être conscients que leurs clients ont des attentes en matière de protection de la vie privée. Les clients doivent pouvoir donner leur consentement ou non pour ces services. Je ne sais pas comment nous pouvons passer outre le fait que le consentement doit être le fondement de ces relations commerciales.

Allez-y, monsieur Karanicolas.

M. Michael Karanicolas: À mon avis, le consentement est certainement un prérequis et l'accès à tout système doit être assujéti à une forme ou à une autre de consentement, mais dans plusieurs des exemples que vous donnez, le consentement n'est pas la seule chose qui entre en ligne de compte. Il y a aussi les règlements qui régissent ces relations.

Selon moi, il y a des façons d'améliorer le modèle actuel de consentement grâce à une plus grande transparence sur ce qui se fait, c'est le point principal, et en présentant cette information à l'utilisateur de façon à promouvoir l'engagement et l'accessibilité. Encore une fois, c'est contraire à la pratique actuelle avec les conditions d'utilisation très légalistes et complexes. Je crois également qu'il faudrait adopter des règles centrales sur ce qui peut et ce qui ne peut pas être fait ou les modèles à suivre.

M. Pat Kelly: Allez-y, monsieur Martin-Bariteau.

[Français]

M. Florian Martin-Bariteau: Je ne pense pas qu'il y ait de recette magique dans le cas du consentement. Bien sûr, cela doit rester la base, mais encore faut-il savoir à quoi l'on consent. On a eu un problème du côté des consommateurs et on sait que les provinces ont légiféré sur cette question.

Peut-être serait-il avisé que le consommateur sache qu'il consent à quelque chose qui est lié à la protection ou à la gestion de ses données personnelles, étant donné que l'avis de confidentialité va plutôt dans le sens inverse, en ce sens qu'il touche tout ce qui perd son aspect confidentiel.

En outre, une loi plus claire aiderait peut-être les petites entreprises à mieux gérer cela. On pourrait établir des principes et faire en sorte que les politiques suivent ces derniers. On pourrait expliquer, pour chacun des principes de la loi, comment y adhérer et coopérer.

●(1645)

[Traduction]

Le président: Merci beaucoup.

[Français]

Monsieur Dubourg, vous avez la parole et vous disposez de cinq minutes.

M. Emmanuel Dubourg (Bourassa, Lib.): Merci, monsieur le président.

Je remercie les témoins d'être parmi nous cet après-midi.

Monsieur Martin-Bariteau, c'est à vous que j'aimerais adresser mes questions.

Dans votre mémoire, vous avez mentionné ce qui suit: « En termes de rédaction, la loi devra rester conçue selon un principe d'indépendance technologique et se fonder sur des principes d'application générale. »

Le commissaire à la protection de la vie privée a dit que la loi devrait être neutre sur le plan technologique et fondée sur des

principes. Or il est évident, compte tenu de ces propos, que nous sommes sur la même longueur d'ondes.

Cependant, vous dites que parmi les lois fédérales, celle-ci est sans aucun doute parmi les plus mal rédigées du fait qu'elle a été en quelque sorte calquée. Dans ces conditions, que nous suggérez-vous? Comment pouvons-nous procéder à une refonte plutôt qu'à une amélioration?

M. Florian Martin-Bariteau: En réalité, il ne s'agit que d'un petit débat doctrinal. Cela veut pratiquement dire la même chose.

L'idée que la loi soit basée sur des principes vise justement à permettre une plus grande flexibilité, à permettre de fixer des limites et, comme le disait plus tôt la professeure Scassa, à permettre aux petites et grandes entreprises, au monde du mobile et de la santé de s'adapter.

La loi actuelle évoque en quelque sorte de grands principes, mais pas au même moment. Pour comprendre un principe, il faut lire le texte de la Loi à trois endroits différents. L'idée serait peut-être, comme pour certaines lois, de tout remettre à plat. Il s'agit d'essayer de se mettre tous d'accord sur ce que devrait être les grands principes et quel devrait en être le nombre. Par la suite, après les articles obligatoires où l'on définit le titre, on peut décrire le premier principe, puis le deuxième, le troisième et ainsi de suite. On peut ensuite indiquer très clairement quelles sont les limites et préciser quels sont les recours des utilisateurs et les pouvoirs du commissaire.

M. Emmanuel Dubourg: Est-ce de cette façon qu'on procède en Europe?

M. Florian Martin-Bariteau: Je vous dirais que oui, même si je n'ai ni le Règlement, ni l'ancienne directive sous les yeux. La suite d'articles comprend ceux sur la cueillette, sur la communication et ainsi de suite. Il est aussi question de ce fameux droit à l'effacement — et non à l'oubli —, qui est un point qu'il faudrait peut-être clarifier.

M. Emmanuel Dubourg: Tout comme Mme Scassa, vous êtes d'accord pour donner plus de pouvoirs au commissaire. Pour ce qui est de l'exécution, vous avez beaucoup parlé des amendes qu'on devrait imposer. Cependant, vous nous dites aussi que, pour éviter les apparences de conflit d'intérêts, les amendes devraient être payables au receveur général.

Pourriez-vous nous en dire davantage à ce sujet?

M. Florian Martin-Bariteau: Il s'agit simplement d'éviter d'éventuelles attaques du secteur privé. Ce dernier pourrait en effet prétendre que le commissaire sortirait de son rôle d'ombudsman pour passer à celui de « sanctionneur ». Pour augmenter son budget ainsi que ses pouvoirs, il appliquerait des sanctions plus importantes.

M. Emmanuel Dubourg: Toutefois, vous êtes d'accord que c'est le commissaire qui déterminerait et appliquerait les sanctions, sans toutefois que son budget soit déterminé en fonction de cela.

M. Florian Martin-Bariteau: Exactement.

Son budget serait totalement indépendant des sanctions qu'il imposerait ou non et cela reviendrait aux contribuables, donc aux citoyens.

M. Emmanuel Dubourg: D'accord.

Cependant, d'autres organisations ou d'autres ministères, même s'ils recueillent de l'argent, ne le gardent pas nécessairement. Prenons le cas, par exemple, de l'Agence du revenu du Canada.

Pour terminer, il est question du droit à l'oubli. Vous avez dit qu'il ne faudrait pas que cela serve à gérer la réputation des gens. Plus tôt, vous avez entendu nos collègues parler des jeunes, par exemple, qui affichent des messages sur Facebook ou sur d'autres médias sociaux. En ce qui concerne la gestion de la réputation, qu'est-ce que vous nous dites à ce sujet?

• (1650)

M. Florian Martin-Bariteau: Je crois que ma porte de sortie serait de dire que je ne pense pas que ce serait à la LPRPDE de régler cette question, mais qu'il s'agit davantage de relations privées. Certaines provinces ont mis en place des recours. On a le Code criminel qui prévoit un recours au criminel. Cependant, si c'était mis en ligne et que c'était d'intérêt public...

M. Emmanuel Dubourg: Par contre, on sait que ces organisations ont des algorithmes, qu'elles vont prendre ces informations, qu'elles vont les utiliser et qu'elles vont ensuite proposer des services. Elles veulent vendre des produits. C'est là l'aspect soulevé. Ne croyez-vous pas que c'est la LPRPDE qui devrait continuer à réglementer tout cela?

M. Florian Martin-Bariteau: Oui, dans ce cas-là, mais dans le cas de quelqu'un qui va récupérer une photo et la mettre ailleurs, on n'est alors plus assujéti selon moi à la LPRPDE. On parle davantage de questions de droit à l'image et de responsabilité civile, ce qui relève généralement plutôt du champ de compétence des provinces.

M. Emmanuel Dubourg: D'accord. Il y a Mme Scassa...

[Traduction]

Le président: En fait, monsieur Dubourg, votre temps est écoulé.

Monsieur Blaikie, vous serez notre dernier intervenant pour cette série de questions.

[Français]

M. Daniel Blaikie: Merci, monsieur le président.

Ma prochaine question s'adresse à M. Martin-Bariteau.

Évidemment, il y a un lien économique important entre le Canada et les États-Unis et il y a un vrai partage d'informations. Il peut s'agir d'un transfert d'informations entre des compagnies canadiennes et des compagnies américaines. Cela se fait même quand on enregistre des données auprès d'une compagnie canadienne, puisque l'infrastructure que nous utilisons alors se trouve aux États-Unis. Nous savons que la loi américaine ne donne pas beaucoup de protection aux citoyens des autres pays.

Est-ce que notre relation comme telle, sans parler des autres ententes avec les États-Unis, menace notre relation avec l'Europe et le jugement que les Européens pourraient porter en ce qui touche la protection de leurs données personnelles?

M. Florian Martin-Bariteau: C'est une excellente question. Je vous avoue que je n'y ai pas réfléchi.

M. Daniel Blaikie: Est-ce que vous pourriez le faire? Ce ne sera peut-être pas aujourd'hui, mais je vous invite à y penser un peu et à nous donner votre opinion éventuellement.

M. Florian Martin-Bariteau: Avec plaisir.

Il est certain que le problème en ce moment, à la suite des dernières décisions de la nouvelle administration, c'est que cela est un enjeu pour les Canadiens. Je peux évaluer à quel point cela aurait un impact sur une décision d'adéquation.

M. Daniel Blaikie: D'accord. Merci beaucoup.

[Traduction]

J'aimerais revenir au consentement. Je sais qu'il en a été question à quelques reprises.

En tant que profane en ce qui a trait au consentement, il serait agréable de pouvoir dissocier de l'utilisation du service le consentement relatif à l'utilisation de mes renseignements personnels. Les gens ne peuvent pas décider de ne plus utiliser leur ordinateur parce qu'ils ne veulent pas que leurs renseignements personnels soient partagés ou de ne pas utiliser un produit Microsoft dans un milieu professionnel où ils doivent souvent partager des documents. Certains outils sont devenus essentiels pour le travail ou même pour administrer ses affaires personnelles. On ne peut donc plus refuser les conditions d'utilisation pour certains logiciels, car on ne pourrait plus travailler ou s'occuper de ses affaires personnelles.

Peut-être ai-je tort de dire cela, mais le consentement à des fins de collecte de données et l'utilisation par un tiers des renseignements personnels n'ont souvent rien à voir avec l'utilisation du service concerné. Y a-t-il une façon légale de limiter l'utilisation des renseignements personnels en fonction des nécessités du service et éviter le partage à grande échelle des renseignements personnels?

Prenons l'application Foursquare, par exemple. Cette application vise à informer les autres d'où vous êtes. Évidemment, il est nécessaire pour l'application de savoir, par l'entremise de mon téléphone cellulaire, où je me trouve. Par contre, pour utiliser d'autres logiciels, il faut consentir à une utilisation de ses renseignements personnels, ce qui n'a rien à voir avec l'utilisation du logiciel en question. Ce n'est pas nécessaire à l'utilisation du service.

Y a-t-il une façon de corriger le problème sans que cela devienne trop lourd?

• (1655)

Mme Teresa Scassa: C'est là la difficulté. Bien entendu, l'un des problèmes, c'est qu'il y a beaucoup d'applications soi-disant gratuites. Or, en réalité, les plateformes gratuites des médias sociaux et les services gratuits ne sont pas gratuits. La monnaie d'échange, ce sont vos renseignements personnels. Dans ce contexte, il est plus difficile de définir ce qui est nécessaire, car les fournisseurs de ces applications sont les seuls à décider ce dont ils ont besoin pour maintenir leur modèle d'affaires. C'est un autre problème.

Le président: Merci beaucoup.

Chers collègues, nous avons terminé nos séries de questions. Je sais que certains d'entre vous ont des questions complémentaires à poser à nos témoins.

Monsieur Massé, je sais que vous aviez d'autres questions à poser, alors je vous laisse la parole.

Chers témoins, s'il y a des choses que vous aimeriez ajouter ou qui vous viennent à l'esprit, vous aurez l'occasion de le faire à la fin de la séance.

Monsieur Massé, vous avez la parole.

[Français]

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

Je remercie les témoins de comparaître devant le Comité et de participer à ses travaux. Je sais que vous devez faire beaucoup de travail afin de venir nous rencontrer. C'est fort apprécié.

Monsieur Martin-Bariteau, vous avez plus tôt fait référence au terme « d'indépendance technologique ». Je veux juste être certain de bien comprendre ce terme. Pour vous, « l'indépendance technologique » est l'équivalent de la « neutralité technologique ». Il s'agit pour vous du même concept. Est-ce exact?

M. Florian Martin-Bariteau: Oui. C'est le même concept. C'est juste que, dans ma thèse de doctorat, je viens de défendre qu'il fallait plutôt parler « d'indépendance » que de « neutralité » à cause du double sens du mot « neutralité ».

M. Rémi Massé: C'est un bon point.

Dans ce contexte, quelles recommandations pourriez-vous nous faire pour que la Loi sur la protection des renseignements personnels et les documents électroniques, communément appelée en anglais PIPEDA, assure cette indépendance technologique?

M. Florian Martin-Bariteau: Je pense que sur ce point, outre l'écrit, c'est actuellement le cas. On n'a pas de règles qui sont propres au papier ou à Internet.

Vous allez proposer des modifications au projet de loi et le Parlement va l'adopter. Le temps que cela prendra pour que la loi soit en vigueur, la technologie aura avancé. Si on pense à l'intelligence artificielle et à la robotique, par exemple, on ne sait pas ce que demain sera. On ne connaît que la situation d'aujourd'hui. Il est donc préférable de rester toujours sur cette idée de principe. Cela permettra à la loi, une fois qu'elle aura été bien rédigée et non comme elle est libellée actuellement, d'être en vigueur pendant de longues années et de s'adapter à toutes les évolutions technologiques qu'on ne peut même pas encore imaginer.

M. Rémi Massé: D'accord. Merci.

Dans un autre ordre d'idées, les propos de tous les témoins ont évidemment retenu mon attention.

Dans votre allocution, monsieur Martin-Bariteau, vous avez fait état du droit à l'oubli. Vous trouvez que la proposition imaginée et demandée par certains est dangereuse.

J'aimerais que vous nous parliez davantage de ce qui vous a amené à faire ce type de commentaires. Vous avez dit qu'en démocratie, on n'a jamais effacé les archives pour la seule raison qu'elles étaient dérangeantes, du moins pas légalement. Il s'agit là selon vous d'un terrain très dangereux. J'aimerais vous entendre davantage sur cette question.

M. Florian Martin-Bariteau: Cela revient à l'idée de la gestion de la réputation. Pour de nombreuses personnes, quand elles proposent un droit à l'oubli, elles veulent avoir le droit de pouvoir effacer de l'information qui les concerne. Par exemple, cela peut être des articles de presse dérangeants qui parlent de certaines choses qu'elles ont faites par le passé. L'année dernière, un article a pu paraître dans la presse et, par la suite, elles vont à une entrevue pour obtenir un emploi. Elles voudraient pouvoir effacer l'information qui est consignée.

C'est vrai qu'aujourd'hui, on est dans un monde où il est de plus en plus difficile d'oublier. Internet n'oublie pas et ne pardonne pas. On n'a jamais autorisé les gens à aller à *La Presse* ou au quotidien *Le Devoir* pour demander d'effacer des articles. Une personne pourrait se dire que comme un article ne lui convient plus, on va l'enlever des archives et l'effacer de toutes les bibliothèques.

Je ne vois pas pourquoi aujourd'hui, parce que cela est facilité par les technologies, on autoriserait ce genre d'actions qui est d'effacer la mémoire.

Par contre, comme on le disait tout à l'heure, il y a un certain nombre d'autres collectes d'information et c'est le cas dans l'affaire Globe 24h.com. Un de mes collègues a insisté sur le fait qu'avec ce cas, c'est peut-être le début du droit à l'oubli. Quand je lis la décision de la cour — de mémoire ce sont les pages 70 à 76 du jugement —, je retiens surtout que le problème, c'est que la collecte de l'information est en violation de la Loi et est utilisée à des fins illicites. Dans ce cas, c'était d'extorquer les gens en leur disant qu'on allait supprimer des données en échange d'un montant d'argent. Cela n'est pas là de la gestion de réputations. Ce sont juste des tentatives de fraude.

• (1700)

M. Rémi Massé: Merci.

[Traduction]

Le président: Monsieur Dubourg, auriez-vous d'autres questions à poser aux témoins? Non?

Monsieur Saini, vous avez la parole.

M. Raj Saini: J'aurais une brève question à poser à Mme Scassa.

Mon bon ami, Wayne Long, a posé une question sur les enfants et la vie privée. J'aimerais connaître votre opinion. Aux États-Unis, à partir de 13 ans, un jeune est considéré comme un mineur. C'est une réglementation adoptée par la FTC. Selon le nouveau RGPD, le seuil sera fixé à 16 ans. Le Canada n'a pas de seuil. Semble-t-il que la Loi sur la protection des renseignements personnels protège les gens de tous âges.

J'aimerais savoir s'il est important pour vous, un, d'avoir une référence pour permettre aux gestionnaires de sites Web de savoir à qui ils ont affaire et, deux, concernant le droit à l'oubli, de faciliter la tâche des jeunes de moins de 16 ans comparativement aux adultes.

Mme Teresa Scassa: En tant que mère d'adolescents, j'appuie la hausse du seuil à 16 ans, car, à mon avis, il y a aussi un rôle éducatif à jouer. Ce n'est pas uniquement une question de consentement. Il faut aussi s'assurer que les enfants d'âge mineur ont davantage d'occasions de réfléchir à ce qu'ils font, à ce à quoi ils consentent, et de comprendre ce que signifie la collecte de données. Il y a de l'éducation à faire à ce chapitre.

M. Raj Saini: Donc, 16 ans, ça va?

Mme Teresa Scassa: En tant que mère d'adolescents, je pencherais plutôt pour 25 ans...

Des voix: Ha, ha!

Mme Teresa Scassa: ... mais, 16 ans, ça me convient.

M. Raj Saini: Merci.

Le président: Nous entendrons M. Massé et ensuite, brièvement, M. Bratina.

[Français]

M. Rémi Massé: Merci, monsieur le président.

Plus tôt, j'ai oublié de vous demander quelque chose, monsieur Martin-Bariteau.

Dans votre conclusion, vous avez fait état d'un court document bilingue contenant des exemples et des recommandations et vous n'avez pas eu le temps de terminer vos propos à ce sujet. Nous serions très intéressés à ce que vous nous fassiez parvenir ce document et vos recommandations.

M. Florian Martin-Bariteau: Je le ferai avec plaisir.

[Traduction]

Le président: Merci beaucoup.

Monsieur Bratina, vous avez la parole.

M. Bob Bratina: Merci.

Monsieur Karanicolas, votre travail porte principalement sur les droits et libertés d'expression en ligne. Concernant le journalisme et la protection des renseignements personnels en ce qui a trait aux journalistes et aux fausses nouvelles, le sujet de l'heure, la distribution se fait principalement par voie électronique. Selon vous, quelle est la responsabilité des organes de presse quant à la réception, à la publication ou à la diffusion de renseignements reçus, disons, par voie numérique?

La seule façon pour moi d'aborder le sujet est de vous demander si le public devrait avoir le droit de savoir quelles sources les organes de presse utilisent pour publier leurs nouvelles.

M. Michael Karanicolas: La protection des sources journalistiques est un principe très important de la liberté d'expression et il doit être protégé. Nous nous éloignons de la LPRPDE, mais, à mon avis, la loi canadienne devrait être plus rigoureuse. Les journalistes ne doivent pas être tenus de révéler leurs sources. Cette règle fondamentale doit être protégée.

Au sujet des fausses nouvelles, dès que ce problème est apparu, beaucoup de défenseurs de la liberté d'expression se sont inquiétés, car ils ont compris dans quelle direction allait la discussion. Nous avons besoin d'initiatives solides pour promouvoir le bon sens au sein du lectorat et le journalisme responsable, mais l'expression « fausses nouvelles » est souvent utilisée par les gouvernements du monde pour interdire l'expression d'opinions contraires aux leurs. Dès que cette conversation s'est amorcée, beaucoup se sont inquiétés et je crois, malheureusement, que c'est dans cette direction que se dirige cette conversation, et ce, à l'échelle mondiale.

M. Bob Bratina: Merci. Je voulais simplement avoir votre opinion sur la question.

Le président: Je ne suis pas vraiment convaincu de la pertinence de cette question pour notre étude, mais c'est important.

M. Bob Bratina: Si vous me laissez une heure, j'arriverai à changer votre opinion.

Des voix: Ah, ah!

Le président: Chers collègues, si vous me le permettez, j'aimerais poser une question aux témoins.

Nonobstant le fait que les données recueillies par l'entremise de logiciels malveillants, de logiciels espions et d'agents numériques, notamment, soient protégées en vertu de différentes lois canadiennes, ces données peuvent être jumelées à d'autres recueillies de façon légitime, par exemple, par ceux qui respectent les dispositions de la LPRPDE. Compte tenu de la fluidité des données et du Web et du fait que l'on ne sait pas avec certitude où les données sont stockées, le stockage et le traitement des données se faisant un peu partout dans le monde, à quel point est-ce important d'harmoniser la législation et les règles relatives à la protection des renseignements personnels tout en évitant d'effrayer les entreprises technologiques canadiennes qui souhaitent investir, mener des recherches et stimuler

l'innovation grâce à ces données? Que faire pour trouver un juste équilibre?

Je m'adresse à n'importe lequel d'entre vous.

Comme personne ne semble vouloir s'aventurer, je vais choisir M. Karanicolas.

• (1705)

M. Michael Karanicolas: Concernant l'harmonisation des règles, compte tenu de la façon dont les règles sont établies ailleurs, il s'agit d'un processus extrêmement important, mais aussi extrêmement difficile. Les opinions diffèrent énormément d'un endroit à l'autre sur la vie privée et les limites appropriées à la vie privée, y compris le traitement des renseignements personnels. Il est donc très difficile de convenir d'une norme commune sur des questions comme la vie privée ou la protection des données.

Toutefois, je suis tout à fait d'accord avec vous: l'opacité de ces flux de données est très problématique. Nous pourrions nous concentrer sur l'endroit où sont stockés les renseignements, mais, à mon avis, il est plus important de savoir qui sont les intervenants. Il y a un autre problème important. Après avoir lu et accepté les conditions d'utilisation de Google et de Facebook, par exemple — même si elles sont difficiles à comprendre, on peut au moins les consulter —, ces sociétés peuvent partager vos renseignements personnels avec des courtiers en données. De là, c'est un vrai trou noir.

Les sociétés doivent absolument être plus transparentes sur ce qu'elles font des renseignements personnels des utilisateurs et fournir plus d'information sur la façon dont les données sont traitées en coulisse.

Mme Teresa Scassa: Je suis d'accord avec mon collègue. La transparence, à ce niveau, sera un problème majeur.

Je crois, également, que la protection des données devient de plus en plus une responsabilité interdisciplinaire. Prenons, par exemple, le droit relatif à la portabilité des données souligné dans la nouvelle directive européenne. Nous en avons parlé un peu plus tôt. À mon avis, il s'agit davantage d'une loi sur la concurrence que d'une loi sur la protection des données. Cela a peu d'importance en ce qui a trait à la réglementation du milieu, mais je crois qu'il y a beaucoup de chevauchement. À mon avis, les grands enjeux liés aux données sont aussi liés aux droits de la personne ou à la non-discrimination, alors que d'autres sont liés à la protection du consommateur.

Habituellement, différents enjeux sont abordés dans différentes lois au sein de différents ministères. Il y a une convergence accrue vers la pertinence de ces dispositions sur la protection des données ou de la protection des données par rapport à la pertinence de ces enjeux. C'est donc un problème, à mon avis. Je partage cet avis.

[Français]

M. Florian Martin-Bariteau: Je suis d'accord avec ce qui a été dit.

[Traduction]

Le président: D'accord.

Au Comité, tout comme lorsque j'étais administrateur de base de données, mes questions concernant les données sont un peu techniques, mais il y a tout un débat en ce moment sur la suppression et la désactivation, deux choses totalement différentes. Nous n'avons pas eu l'occasion d'avoir une bonne discussion sur ces sujets.

Une chose dont nous devrions parler davantage au Comité, à mon avis, est le libellé, la simplicité du langage utilisé, l'utilisation d'un langage courant dans les conditions d'utilisation que nous signons, car, comme vous l'avez souligné, la monnaie d'échange, dans la plupart des cas, ce sont les données et renseignements personnels que nous fournissons lorsque nous ouvrons une session ou lorsque nous utilisons une application, qu'elle soit gratuite ou non.

Je sais que cela soulève beaucoup de questions. Je suis un mordu de l'informatique, disons, et je ne connais personne qui lit jusqu'à la fin les contrats de licence de 65 pages truffés de jargon de juristes. Auriez-vous des recommandations à faire au Comité pour simplifier l'expérience du consommateur?

Mme Teresa Scassa: Michael, voulez-vous répondre d'abord?

M. Michael Karanicolas: Concernant les droits du consommateur à la suppression des données et à la compréhension des conditions, encore une fois, la transparence joue un rôle important à ce chapitre. Les utilisateurs devraient être en mesure de comprendre lesquels de leurs renseignements personnels la société conserve et de demander à ce que ces renseignements soient supprimés ou éliminés lorsqu'ils n'utilisent plus le service associé, ou de demander à ce que ces renseignements soient corrigés. Ce sont des points importants à examiner.

Concernant la simplification des conditions d'utilisation, il existe un problème fondamental, soit que ces conditions doivent être juridiquement contraignantes. Elles sont rédigées par des avocats. Elles doivent être précises et rédigées en utilisant un libellé bien particulier. Habituellement, nous proposons d'accompagner les conditions d'utilisation d'une version simplifiée de celles-ci pour faciliter la compréhension. C'est possible. Certaines initiatives ont été mises à l'essai avec beaucoup de succès pour fournir des explications en langage clair.

Le CPVP a un rôle à jouer dans la promotion de modèles de conditions d'utilisation. Encore une fois, c'est possible. Il est possible de rédiger une entente normalisée pouvant être adaptée selon le contexte. C'est une option qu'il faudrait examiner davantage.

● (1710)

Le président: Merci beaucoup.

Chers collègues, merci. Je ne lèverai pas la séance tout de suite. Nous allons plutôt suspendre la séance pour passer à huis clos, car nous avons une question à aborder.

Je tiens à remercier nos témoins de leur aide dans le cadre de notre étude sur la LPRPDE. Nous savons que nous pourrions compter à nouveau sur votre expertise, au besoin.

Chers collègues, nous allons suspendre la séance quelques instants et nous poursuivrons ensuite à huis clos.

[La séance se poursuit à huis clos.]

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

PERMISSION DU PRÉSIDENT

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

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

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

Aussi disponible sur le site Web du Parlement du Canada à l'adresse suivante : <http://www.parl.gc.ca>

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

SPEAKER'S PERMISSION

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

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

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

Also available on the Parliament of Canada Web Site at the following address: <http://www.parl.gc.ca>