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 061 • 1re SESSION • 42e LÉGISLATURE

TÉMOIGNAGES

Le mardi 16 mai 2017

Président

M. Blaine Calkins

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

Le mardi 16 mai 2017

● (1545)

[*Traduction*]

Le président (M. Blaine Calkins (Red Deer—Lacombe, PCC)): Bienvenue, chers collègues, à la 61e réunion du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, qui poursuit l'examen de l'étude de la Loi sur la protection des renseignements personnels et les documents électroniques, la LPRPDE.

Je prie les témoins d'excuser le retard du Comité aujourd'hui. Nous avons de bonnes raisons. Nous arrivons tout juste de la Chambre où les travaux ont été un peu plus longs que prévu après la période des questions.

Nous allons entrer directement dans le vif du sujet.

Il nous reste une heure et quarante minutes. Nous devrions donc pouvoir traiter le sujet sans problème.

Je suis heureux de la présence parmi nous aujourd'hui de M. Robert Watson, président-directeur général de l'Association canadienne de la technologie de l'information. Nous avons également M. André Leduc, vice-président aux Relations gouvernementales et politiques.

Du Conseil des consommateurs du Canada, nous avons M. Dennis Hogarth, vice-président.

De la Chambre de commerce du Canada, nous avons Scott Smith, directeur, Propriété intellectuelle et politique d'innovation.

Chaque organisation disposera d'une dizaine de minutes pour présenter ses observations préliminaires. Nous suivrons l'ordre dans lequel vous avez été présentés.

M. Watson, de l'Association canadienne de la technologie de l'information.

M. Robert Watson (président et directeur général, Association canadienne de la technologie de l'information): Je vous remercie, monsieur le président, mesdames et messieurs. C'est un privilège d'être ici aujourd'hui pour parler du monde en constante évolution de la technologie, des données et de la protection des renseignements personnels, au nom de l'Association canadienne de la technologie de l'information, l'ACTI.

L'ACTI est la voix nationale de l'industrie canadienne des technologies de l'information et des communications. L'industrie canadienne des TIC compte plus de 37 000 entreprises, créatrices de plus de 1,1 million d'emplois directs et indirects. De plus, l'industrie des TIC crée et fournit les biens et les services qui contribuent à rendre l'économie et la société plus productives, plus compétitives et plus novatrices. Dans cet esprit, nous nous réjouissons de pouvoir soutenir votre étude sur l'évolution du contexte de la protection de la vie privée au Canada.

Internet est devenu le moteur de croissance économique le plus puissant de l'histoire de l'humanité, dépassant la machine à vapeur et l'avènement de l'électricité. Les données se sont transformées en l'espace de quelques décennies en un produit précieux capable de résoudre des problèmes complexes et de générer d'immenses retombées et beaucoup de valeur pour les organisations, les particuliers et la société. *The Economist* soulignait dernièrement que le produit le plus précieux du monde n'est plus le pétrole, mais les données. Aujourd'hui, les entreprises de TIC utilisent des données pour améliorer la circulation, réduire le nombre d'accidents aux intersections, détecter des risques sanitaires, augmenter les rendements agricoles et améliorer la qualité de vie de tous les Canadiens. Nous espérons que cette discussion débouchera sur des recommandations qui renforceront le régime de protection de la vie privée du Canada de manière à promouvoir une utilisation responsable des données personnelles, tout en appuyant et en permettant l'innovation fondée sur des données qui favorisera la croissance continue du secteur canadien des TIC.

Je voudrais tout d'abord dire très clairement qu'un régime de protection de la vie privée strict permettant de conserver la confiance des Canadiens est tout à fait dans l'intérêt commercial de l'industrie des TIC. Il est essentiel pour les entreprises de garder la confiance des clients et cette confiance est cruciale quand un client confie des données personnelles à une entreprise. C'est encore plus vrai aujourd'hui que les données sont devenues les produits les plus précieux du monde. Les données, y compris les renseignements personnels des clients, deviennent aussi rapidement essentielles pour la plupart des activités des entreprises, que ce soit pour exécuter les commandes de clients, facturer, entretenir des relations avec la clientèle, gérer la chaîne d'approvisionnement ou faire du marketing. Par conséquent, la LPRPDE n'est pas seulement une loi sur la consommation, c'est aussi une loi sur l'économie. J'encourage le Comité à tenir compte dans ses délibérations des enjeux économiques importants, tandis qu'il réfléchit aux changements législatifs qu'il pourrait recommander.

Plusieurs parties ont souligné que les nouvelles technologies et les nouveaux modèles de gestion remettent en question la LPRPDE. Cependant son approche neutre sur le plan technologique et fondée sur des principes était supposée lui permettre de s'adapter au fil du temps. Elle comprend déjà un cadre réaliste pour gérer bon nombre des défis associés à des nouvelles technologies telles que l'analytique des données. La LPRPDE, si on ne l'interprète pas de façon trop restrictive, peut continuer d'être un cadre fondé sur des principes appropriés, capable de répondre aux préoccupations des Canadiens en matière de protection des renseignements personnels.

Au cours de l'année écoulée, l'ACTI a participé aux consultations organisées par le Commissariat à la protection de la vie privée, et j'aimerais présenter des remarques additionnelles sur trois aspects de ces consultations. Le premier concerne la protection de la réputation en ligne, le deuxième, la modernisation des méthodes de consentement, et le troisième vise à déterminer s'il est nécessaire de conférer au commissaire à la protection de la vie privée des pouvoirs d'exécution supplémentaires.

Pour ce qui est de la réputation en ligne ou de ce qu'on appelle le droit à l'oubli, le défi réside dans la permanence et la facilité de recherche de tout ce qui est affiché en ligne et dans les conséquences que peuvent avoir pour la réputation hors ligne d'un Canadien des choix regrettables ou des publications malveillantes.

Pour relever ces défis, le CPVP a avancé l'idée de nouveaux pouvoirs ou processus législatifs permettant de retirer d'Internet des renseignements concernant une personne. L'ACTI se demande si les nouvelles règles sont nécessaires à ce stade. En fait, elle recommande que le gouvernement concentre ses efforts sur l'éducation des Canadiens, surtout des jeunes Canadiens, pour qu'ils sachent comment se comporter de manière responsable en ligne et pour les inviter à réfléchir avant d'afficher quoi que ce soit.

Nous recommandons également que le gouvernement utilise le cadre juridique existant pour améliorer ses propres processus de demande de réparation aux tribunaux en cas de diffamation en ligne et pour faire en sorte que les simples citoyens aient plus facilement accès à ces recours juridiques. L'ACTI recommande de ne pas adopter comme dans l'UE un droit à l'oubli qui oblige les sociétés de moteur de recherche à modifier les résultats de recherche en fonction de plaintes individuelles.

● (1550)

Les entreprises du secteur d'Internet ont montré qu'elles sont disposées à retirer des contenus pour se conformer à des ordonnances de tribunal et à des obligations juridiques, mais aucune entreprise ne devrait se voir habiliter à décider de l'équilibre à trouver entre le respect de la vie privée d'une personne et la liberté d'expression. Il est préférable de laisser ces décisions aux tribunaux.

Vient ensuite la question du consentement. On a beaucoup parlé du fait qu'il est plus difficile pour tout un chacun, avec de nouvelles technologies comme l'analytique des données et l'Internet des objets, de donner un consentement éclairé. L'ACTI est très favorable à l'approche neutre sur le plan technologique et fondée sur des principes de la LPRPDE, mais ses membres trouvent que, dans son interprétation de la Loi, le Commissariat à la protection de la vie privée met trop l'accent sur le consentement exprès.

Dans le monde actuel du mobile et d'Internet où tout évolue rapidement, ralentir le transfert de l'information nécessaire à la conclusion de transactions pour obtenir le consentement exprès est une pratique qui comporte des limites importantes pour les clients comme pour les entreprises, y compris en ce qui concerne la volonté des personnes de lire ou comprendre ce à quoi elles consentent. Combien parmi les membres du Comité ont lu chaque mot de la politique de confidentialité d'iTunes?

La complicité technologique croissante signifie aussi que des organisations différentes ou multiples conservent, traitent et analysent peut-être les mêmes données, d'où la difficulté de se concentrer et d'expliquer pleinement aux personnes. Il existe aussi des situations où l'utilisation imprévue de données pourrait se révéler très bénéfique pour les utilisateurs, mais où il peut être difficile, voire impossible, d'obtenir des expressions de consentement renouvelées.

Compte tenu de ces difficultés, l'ACTI a proposé plusieurs changements qui régleront, selon elle, le problème du consentement, tout en permettant aux entreprises de se créer, de continuer d'innover et de produire une valeur économique à partir de données.

Tout d'abord, si le consentement exprès n'est pas toujours une option réaliste, des cadres devraient être mis en place pour élargir le consentement implicite dans des situations appropriées. Plus particulièrement, l'ACTI recommande d'adopter une nouvelle exemption afin d'autoriser le traitement de renseignements personnels fondé sur des intérêts ou des objectifs commerciaux légitimes conformes à ceux pour lesquels le consentement a été obtenu à l'origine. La LPRPDE contient déjà des dispositifs pour délimiter ces formes de consentement implicite, comme le critère de la personne raisonnable aux termes de l'article 5.3, et le CPVP peut formuler des conseils supplémentaires, au besoin.

L'ACTI propose également de mettre à jour l'exemption au consentement. Les exemptions actuellement prévues par les règlements pris en vertu de la LPRPDE, qui concernent pour l'essentiel les détails des annuaires téléphoniques, sont dépassées et ne correspondent pas au paysage des renseignements personnels aujourd'hui communiqués dans des espaces publics. Nous appuyant sur le modèle éprouvé de la LPRPDE elle-même, nous recommandons de définir une nouvelle exemption neutre sur le plan technologique et fondée sur des principes pour les renseignements accessibles au public qui puisse mieux s'adapter et évoluer avec le temps.

Enfin, l'ACTI est également d'avis que des pouvoirs d'exécution supplémentaires ne sont pas nécessaires à ce stade pour le CPVP. Des pouvoirs d'exécution renforcés lui ont déjà été conférés en 2015 par la Loi sur la protection des renseignements personnels numériques, et il faut du temps pour en déterminer l'efficacité. Dans le cadre actuel, le CPVP peut beaucoup faire pour renforcer et promouvoir la protection de la vie privée, y compris par sa fonction de sensibilisation du public. Le pouvoir de rendre des ordonnances risquerait de nuire à la relation de collaboration qui existe actuellement entre l'industrie et le CPVP et de rendre plus difficile une collaboration entre le gouvernement et l'industrie pour trouver ensemble des solutions dans ce domaine qui évolue rapidement.

Je vous remercie encore de m'avoir donné l'occasion de présenter ces observations aujourd'hui et je serai heureux de répondre à toute question.

● (1555)

Le président: Je vous remercie, monsieur Watson.

Je signale que personne n'a levé la main quand vous avez demandé combien lisent la politique de consentement et, comme cette réunion n'est pas télévisée, je dois m'assurer que cela figure dans l'enregistrement audio.

Monsieur Hogarth, du Conseil des consommateurs du Canada, vous avez la parole.

M. Dennis Hogarth (vice-président, Conseil des consommateurs du Canada): Je vous remercie, monsieur le président.

Je m'appelle Dennis Hogarth et je suis le vice-président bénévole du Conseil des consommateurs du Canada. Je tiens à dire que le Conseil est heureux de contribuer à cette étude.

Le Conseil des consommateurs du Canada est un organisme national sans but lucratif qui contribue à la protection et au renforcement des droits des consommateurs, qu'il sensibilise aussi à leurs responsabilités. Il travaille en collaboration avec les consommateurs, le gouvernement et les entreprises afin d'améliorer le marché. Les consommateurs ont un intérêt indéniable à la protection des renseignements personnels, à la mise en oeuvre de la Loi sur la protection des renseignements personnels et les documents électroniques et à toute amélioration apportée à la suite du présent examen.

Des questions importantes ont été soulevées au cours de cette étude. Elles reflètent la nécessité de clarifier les définitions et les interprétations dans les lois canadiennes en matière de protection des renseignements personnels.

Pour ce qui est du nouvel environnement électronique, d'ici 2020, plus de 50 milliards d'appareils connectés à Internet seront utilisés dans le monde, tous ayant la capacité de recueillir, analyser et communiquer des données provenant principalement des consommateurs. On collecte un nombre croissant et massif de points de données, qu'on appelle souvent « mégadonnées ».

Les données des consommateurs sont recueillies activement et en secret, à partir de recherches, des médias sociaux, des transactions effectuées avec des cartes de crédit et sur différents sites, comme Amazon, Expedia, etc. On recueille également des données plus passivement maintenant au moyen de dispositifs en apparence inoffensifs qui fournissent des renseignements sur l'emplacement, les habitudes de vie et les préférences personnelles. Toutes les connexions Internet enregistrent des données sur les utilisateurs. Bien qu'elles puissent être dissociées des renseignements personnels pour éviter des risques d'atteinte à la vie privée, lorsqu'elles s'inscrivent dans le contexte des mégadonnées et qu'elles sont analysées au moyen de logiciels perfectionnés, nous savons qu'il est possible à présent de connaître l'identité ou le profil des personnes.

Les lois en matière de protection de la vie privée sont en retard sur les utilisations avancées des renseignements personnels. L'accumulation de données personnelles crée un risque pour les organisations qui les détiennent autant que pour les consommateurs auxquels elles se rapportent.

Il ressort d'une étude réalisée en 2016 par PWC que nombre d'organisations ne comprennent pas encore tout à fait les risques de la cybercriminalité et ne savent pas comment gérer efficacement les incidents de cette nature et comment y réagir. Les problèmes vont de conseils d'administration qui comprennent mal les risques à la faiblesse des mesures de contrôle appliquées par des fournisseurs tiers externes. Alors que les consommateurs savaient autrefois quels renseignements ils fournissaient aux organisations et pourquoi ils les fournissaient, il est peu probable qu'ils sachent aujourd'hui quels renseignements les concernant sont conservés, où ils sont conservés et à quelles fins ils sont utilisés.

Ce qui nous amène à la question du consentement. Les techniques d'analyse de données sont de plus en plus poussées et permettent désormais d'accéder à d'immenses entrepôts de données. Les renseignements personnels sont recueillis, associés et utilisés de tellement de façons qu'il semble inconcevable que les modèles de consentement actuels demeurent possibles ou pertinents. Souvent, les politiques des organisations en matière de protection de la vie privée sont complexes, partiales et peu transparentes.

Pour donner un consentement éclairé, les consommateurs doivent savoir à quelles fins les données les concernant seront utilisées. Il est douteux que les consommateurs soient même capables de lire et de comprendre pleinement les politiques, mais ils doivent passer outre pour participer à un monde numérique inévitable.

Il a été question pour remédier à cette situation d'utiliser une échelle mobile de consentement. Les renseignements personnels sensibles feraient l'objet d'un consentement explicite, comme toujours, mais ceux de nature moins sensible pourraient faire l'objet d'un consentement implicite. Il faudrait pour cela élargir la définition des renseignements sensibles.

Il se peut que, de plus en plus, les mesures de protection de la vie privée ne soient plus autant axées sur l'organisation qui obtient les renseignements personnels que sur la façon dont ces renseignements sont conservés et mis à l'abri d'utilisations préjudiciables. Pour atténuer les risques, il faut que les organisations qui utilisent les renseignements personnels de façons complexes fassent l'objet de contrôles accrus. Elles doivent être soumises à une surveillance particulière pour s'assurer qu'elles utilisent les renseignements de manière appropriée.

Pour ce qui est des enfants et de la protection de la vie privée, le Conseil convient qu'il devrait être interdit de recueillir des renseignements auprès d'enfants de moins de 16 ans sans autorisation d'un tuteur légal. Cependant, il est difficile de vérifier l'âge d'une personne et les enfants peuvent duper les systèmes. Tant qu'il n'existe pas une sorte de système de registre fiable pour vérifier l'âge, il sera difficile de procéder à des contrôles sans créer de nouveaux problèmes de protection de la vie privée. Il faudrait, néanmoins, envisager la possibilité d'inclure dans les modifications prévues à la LPRPDE les mesures de protection énoncées dans le Règlement général sur la protection des données ou RGPD.

● (1600)

Quant au droit à l'oubli, la LPRPDE devrait, dans la mesure du possible, empêcher les organisations de conserver des renseignements personnels plus longtemps que le temps raisonnablement nécessaire pour le traitement ou de conserver des renseignements périmés ou dont elles ne peuvent confirmer l'exactitude. Les organisations responsables du traitement ou les sous-traitants qui en sont chargés devraient établir des limites raisonnables en ce qui concerne la conservation de certains types de renseignements personnels.

Les mégadonnées compliqueront davantage l'identification des données personnelles lorsque les consommateurs présenteront à des organisations des demandes relatives à des renseignements personnels. De même, il peut être difficile de déterminer quels sont les renseignements qui doivent être supprimés. Des solutions techniques, comme le métabalisage des données, peuvent être utiles à cette fin, mais le coût de ces systèmes pourrait dissuader les petites organisations de les utiliser.

En ce qui concerne l'application de la loi, les organisations ne se concentrent plus autant sur la protection de la vie privée. Leur conformité avec la LPRPDE demeure donc problématique, dans une large mesure parce que la non-conformité n'expose pas à grand-chose. Le Commissariat à la protection de la vie privée du Canada doit adopter des mesures d'application de la loi et imposer des sanctions rigoureuses et efficaces, y compris des amendes punitives et d'autres mesures en cas de non-conformité.

Selon nous, un modèle plus approprié prévoirait que le CPVP examine les pratiques et les politiques de confidentialité publiées des organisations, surtout lorsqu'elles sont connues pour beaucoup utiliser des renseignements personnels. Elles devraient, de plus, être tenues de s'inscrire auprès du CPVP et de lui fournir une description de la façon dont elles collectent, utilisent et protègent les renseignements personnels.

Des examens réguliers de la conformité devraient être faits par rapport aux politiques publiées et aux mesures de protection des données. Les résultats pourraient en être publiés en ligne afin que les consommateurs sachent comment leurs renseignements sont utilisés. La surveillance pourrait être renforcée en utilisant un modèle de réglementation qui fasse appel à des tiers indépendants

Pour ce qui est du respect des normes de l'Union européenne, le RGPD est actuellement considéré comme exemplaire dans le monde et il servira probablement de base à la révision future de nombreuses lois et pratiques nationales en matière de protection de la vie privée. Il se peut que l'harmonisation de la LPRPDE avec le RGPD demande plus d'efforts aux organisations canadiennes, mais se conformer à ce règlement offrirait une meilleure protection aux consommateurs et permettrait au Canada d'être plus concurrentiel que les pays qui ne s'y conforment pas, comme les États-Unis. Étant donné la vitesse à laquelle le monde électronique évolue, les entreprises canadiennes y gagneront à la longue. Par conséquent, nous recommandons au Comité d'examiner attentivement les mesures à prendre pour s'assurer que les lois canadiennes en matière de protection des renseignements personnels continuent d'être reconnues comme adéquates par l'Union européenne.

Enfin, sur la question des droits des consommateurs à la vie privée, ces droits ne sont pas appliqués uniformément au Canada. Le site Web du CPVP fait référence aux différents organismes fédéraux, provinciaux et autres concernés. Des lacunes et des chevauchements juridiques sèment la confusion et préoccuperont de plus en plus les consommateurs, qui veulent que les organisations qui utilisent leurs renseignements personnels soient soumises à des règles uniformes.

En février 2012, aux États-Unis, la Maison-Blanche a publié un rapport qui comprenait une déclaration des droits des consommateurs en matière de protection de la vie privée régissant la confidentialité des données des consommateurs. Ce rapport n'était pas juridiquement contraignant pour les organisations, mais il fournissait des directives appropriées sur les attentes relatives à la protection de la vie privée. Le Conseil est d'avis qu'il faudrait envisager la possibilité de mettre en oeuvre au Canada la déclaration claire quant aux droits et aux responsabilités en matière de protection de la vie privée qui se trouve dans le rapport de la Maison-Blanche.

Je vous remercie de m'avoir donné l'occasion de présenter cet exposé au nom du Conseil des consommateurs du Canada.

● (1605)

Le président: Merci beaucoup, monsieur Hogarth.

Notre dernier témoin aujourd'hui est M. Scott Smith, de la Chambre de commerce du Canada.

Monsieur, vous avez la parole.

M. Scott Smith (directeur, Propriété intellectuelle et politique d'innovation, Chambre de commerce du Canada): Je vous remercie infiniment, monsieur le président et les membres du Comité de me donner l'occasion de m'exprimer aujourd'hui.

Comme vous l'avez dit, je représente la Chambre de commerce du Canada. Nous sommes une association à but non lucratif et un lien vital entre les entreprises et le gouvernement. Nous avons un réseau de plus de 450 chambres de commerce réparties dans tout le pays. Vous connaissez probablement celle qui se trouve dans votre collectivité. Elles font toutes partie de la Chambre de commerce du Canada, qui est l'organisme-cadre. Nous représentons, par conséquent, près de 200 000 entreprises canadiennes de toutes tailles et de toutes les collectivités.

Je suis chargé à la Chambre de la propriété intellectuelle et de la politique d'innovation du point de vue de l'innovation. C'est ce dont je vais vous parler aujourd'hui dans mes observations. Je parlerai également de thèmes similaires à ceux des autres témoins. J'espère donc ne pas vous ennuyer.

Nous entendons beaucoup parler de l'omniprésence des mégadonnées ainsi que des gouvernements et des entreprises qui collectent des renseignements sur nous. Ce qu'on entend semble souvent négatif et laisse supposer une atteinte à la vie privée. C'est regrettable. Les données personnelles sont essentielles pour créer une gamme de produits novateurs et cruciales pour l'expérience utilisateur.

Il ressort d'une enquête réalisée en 2016 par Accenture auprès de 500 entreprises dans le monde que plus des trois quarts des répondants déclarent que les mégadonnées permettent d'offrir un service à la clientèle meilleur et plus personnalisé, et que plus de la moitié des répondants estiment qu'elles aident à renforcer la loyauté des clients. D'autres déclarent que l'information les aide à s'imposer sur de nouveaux marchés, à mieux cibler leur publicité et à fabriquer de meilleurs produits. Bref, les données permettent d'innover.

Si vous le permettez, j'aimerais attirer votre attention sur quelques exemples de ce qui fait que les données sont tellement importantes pour l'innovation et la compétitivité.

Tout d'abord, il s'agit de comprendre les clients. Les mégadonnées servent à mieux comprendre les clients, leurs comportements et leurs préférences. Pour garder un avantage concurrentiel, les entreprises vont au-delà des ensembles de données classiques et utilisent les médias sociaux et l'historique de navigation, ainsi que l'analyse de texte et les données de capteurs, pour obtenir un portait plus complet de leurs clients.

Le grand objectif dans bien des cas est de créer des modèles prédictifs qui ne correspondent pas à une personne en particulier. L'information collectée concerne certes des individus, mais ce ne sont pas tant les renseignements individuels que collectifs qui intéressent pour cerner dans l'immense quantité de données recueillies les modes de comportement.

L'utilisation des données dans les stations de ski en est une bonne illustration. Des étiquettes d'identification par radiofréquence sont insérées dans les billets de remontées. Cela permet de lutter contre la fraude et de réduire les temps d'attente aux remontées mécaniques, d'aider les stations de ski à comprendre la fréquentation des remontées et des pistes, à savoir lesquelles sont les plus populaires et à quels moments de la journée, et même à retracer les déplacements des différents skieurs, si jamais ils venaient à se perdre. Tout cela est à l'avantage du client dont l'expérience est plus agréable. Je sais que je serais heureux de recevoir un message qui m'annonce qu'il y a 60 centimètres de poudreuse sur ma piste préférée, même si mon employeur risque de ne pas vraiment apprécier que je disparaisse pour la journée.

Le deuxième thème est celui de l'optimisation des processus opérationnels.

Les détaillants sont capables d'optimiser leurs stocks en fonction des prévisions calculées à partir des données provenant des médias sociaux, des tendances des recherches sur Internet et des prévisions météorologiques. Les employeurs peuvent optimiser le flux de travail en surveillant les comportements et en adaptant les processus dès lors que ces comportements se révèlent très productifs.

Vient ensuite la quantification personnelle.

Nous sommes maintenant en mesure de tirer parti des données générées par les dispositifs portables. Combien parmi vous ont un Fitbit? Je vois une main se lever.

Cet appareil collecte des données sur notre consommation de calories, nos niveaux d'activité et notre sommeil. Ces données sont riches d'enseignements pour nous, mais ce qui est vraiment intéressant, c'est d'analyser les données collectives. L'analyse de décennies de données recueillies sur le sommeil au cours d'une nuit apportera de toutes nouvelles perspectives qui peuvent être utiles aux différents utilisateurs.

Il en va de même des sciences de la vie. Les essais cliniques de demain ne seront pas limités par la taille d'échantillons, mais pourraient inclure tout le monde.

Les mégadonnées sont utilisées pour faciliter la tâche des services de police, mais elles sont également utilisées par nos institutions financières. Les sociétés de cartes de crédit surveillent les comportements et lorsqu'ils dévient de normes prévues, les clients en sont avisés, ce qui aide à lutter contre la fraude et l'usurpation d'identité.

La LPRPDE a été adoptée avant l'apparition des médias sociaux, avant la diffusion de vidéos en temps réel et avant qu'il soit question de rançongiciels, dont nous avons tous entendu parler ces derniers jours. Et pourtant, elle est restée plutôt pertinente au fil de l'évolution de la technologie.

● (1610)

Comme elle repose sur des principes, le gouvernement n'a pas eu à réagir à l'évolution technologique. À maintes reprises, le contrôle judiciaire s'est révélé être un recours adéquat lorsqu'une organisation s'est écartée d'une utilisation raisonnable des données.

Néanmoins, des changements importants ont été apportés à la LPRPDE en 2015. Des changements législatifs à quelque chose d'aussi omniprésent que la loi sur la protection des renseignements personnels auront toujours des répercussions importantes sur les entreprises à cause de l'incertitude qu'ils suscitent dans l'économie. Certains des changements apportés en 2015 ne sont même pas encore en vigueur. Nous attendons toujours les détails expliquant comment les entreprises sont supposées se conformer aux exigences en ce qui concerne le signalement des atteintes à la protection des données et la conservation pour une durée indéfinie des dossiers concernant toutes ces atteintes. Nous ne savons pas vraiment pour le moment ce que cela voudra dire. La clarification de la définition du consentement ne fait guère plus que reconnaître une pratique exemplaire commune, mais les entreprises se sont interrogées à l'époque sur son objectif.

Nous devons certes suivre ce qui se passe dans d'autres pays pour faire en sorte que nos lois soient compatibles avec celles de nos partenaires commerciaux, pour garantir la libre circulation des données et la capacité d'innover, mais adopter des mesures de manière préemptive pourrait avoir des conséquences imprévues. Par exemple, des changements au Règlement général sur la protection des données sont imminents en Europe et l'équivalent au Canada pourrait être mis à l'épreuve. Cependant, nous devons comprendre que le RGPD va bien au-delà de la protection de la vie privée. Il vise autant le secteur public et la sécurité que la protection des renseignements personnels.

Par exemple, un commentaire a été fait sur les États-Unis et la surveillance américaine. C'est un facteur dont il faut tenir compte par rapport au RGPD. L'enjeu dépasse de loin notre loi sur la protection des renseignements personnels.

Le renforcement des contrôles auxquels sont soumises la collecte, l'utilisation et la communication de données personnelles n'aura probablement pas d'incidence positive sur la protection de la vie privée. La façon dont les données sont recueillies et le modèle de gestion qui repose sur cette collecte de données rendent intenables des contrôles renforcés, et nous parlons de comportements de base. Il est pratiquement impossible de créer un modèle de consentement autour de comportements.

Il faut avoir confiance pour communiquer des renseignements personnels et le maintien de cette confiance nécessite des pratiques exemplaires en matière de responsabilité numérique. Ainsi, il faut veiller à ce que la gestion des données personnelles réponde aux attentes des consommateurs, se montrer transparent sur la façon dont on se procure les renseignements personnels, donner aux gens plus de contrôle sur leurs données, expliquer aux consommateurs les avantages qu'ils retirent de la communication de renseignements, et utiliser les données pour apporter des améliorations sociales.

Les entreprises qui adoptent ces pratiques exemplaires seront celles qui prospéreront lorsque des technologies nouvelles telles que le chaînage des blocs évolueront et redonneront le contrôle des renseignements aux personnes concernées.

L'attaque menée la fin de semaine dernière par WannaCry à l'aide d'un rançongiciel ne visait peut-être pas les renseignements personnels, mais elle a certainement ouvert les yeux du monde entier sur la vulnérabilité de l'économie numérique. Cela veut également dire que nous devons réagir plus fermement aux problèmes de cybersécurité.

Je vais vous donner quelques statistiques récentes. Rien qu'au troisième trimestre de 2016, 18 millions d'échantillons de nouveaux maliciels ont été enregistrés. On a compté plus de 4 000 attaques de rançongiciels par jour depuis le début de 2016. La proportion de courriels d'hameçonnage contenant une forme de rançongiciel est passée à 97,25 % au troisième trimestre de 2016, alors qu'elle était de 92 % au premier trimestre. Bien que 78 % des internautes se déclarent conscients des risques que présentent les liens inconnus dans les courriels, ils n'en cliquent pas moins dessus.

Les données que les organisations collectent, conservent et utilisent sont extrêmement utiles, même si on n'en connaît pas encore toute l'utilité. Les gouvernements comme les organisations sont cependant à la merci d'attaques et on ferait mieux, à mon avis, d'utiliser les ressources dans une collaboration internationale contre les entreprises criminelles qui attaquent les bases de données que pour surveiller les organisations qui innovent et servent leurs clients.

Voilà qui conclut mes observations. Je vous remercie de votre attention.

● (1615)

Le président: Je vous remercie, monsieur Smith.

Nous allons passer à une série de questions de sept minutes.

Monsieur Ehsassi, vous avez la parole pour sept minutes.

M. Ali Ehsassi (Willowdale, Lib.): Merci beaucoup, messieurs, de votre témoignage. Il est très utile.

Je commencerai par M. Watson. J'ai eu le plaisir d'écouter vos observations. J'ai remarqué que vous aviez beaucoup à dire sur le consentement exprès, sur la nécessité de préserver les réputations et sur le pouvoir d'exécution. Je n'ai rien entendu au sujet de la pertinence et de son importance alors que nous examinons la possibilité de réviser la LPRPDE. Est-ce que c'est important? Selon vous, le modèle européen est-il exemplaire?

M. Robert Watson: Je vais répondre, et André prendra la suite.

Le modèle européen est, selon nous, très contraignant. Il y incombe, en fait, aux organisations de décider qui reste et qui est retiré. À notre avis, en règle générale, les personnes qui mettent des renseignements en ligne le font du fait de la prolifération des appareils intelligents. Or, dans ce processus, des mécanismes de contrôle interviennent tout du long, même dans les appareils.

On peut avoir un mécanisme de contrôle qui permet de décider si on veut une application dans son appareil et si on veut que cette application nous suive. On peut décider si on veut recevoir des courriels de telle organisation et, même si on ne les lit pas tous, on doit accepter les conditions d'achat sur le site.

On décide donc en toute connaissance de cause chaque fois qu'on progresse sur l'appareil, et si les organisations ont mis cela en place, c'est parce que, franchement, le risque pour la réputation si on fait quelque chose — de mal —à quelqu'un et que cela se sache dans le cyberespace n'en vaut pas la peine. Les organisations s'occupent de cet aspect et sont tout à fait disposées à travailler en collaboration avec le commissaire à la protection de la vie privée pour ne pas prendre de retard sur les organisations modernes.

André, avez-vous quelque chose à ajouter?

M. André Leduc (vice-président, Relations gouvernementales et politiques, Association canadienne de la technologie de l'information): La pertinence demeure très importante, surtout dans le cadre de l'accord commercial avec l'UE et de la libre circulation des données entre l'Europe et le Canada. Je n'irai pas jusqu'à dire que le RGPD est exemplaire. Il faudrait comparer les degrés de protection des renseignements personnels en Europe et au Canada.

Il est important de préserver la pertinence, et nous considérons que la LPRPDE en la forme actuelle nous permettra de maintenir cette pertinence et de conserver la libre circulation des données entre le Canada et l'Europe qui, répétons-le, sera encore plus importante une fois que nous pourrons mettre en oeuvre l'accord commercial entre l'UE et le Canada.

M. Ali Ehsassi: Diriez-vous également que le modèle européen est contraignant ou...?

M. André Leduc: Il n'y a guère de doute. Il suffit de voir l'exemple européen des témoins. En Europe, chaque fois qu'on va sur un site Web, un avertissement s'affiche d'abord.

Je ne suis pas certain que quiconque soit plus ou moins protégé par cette politique. Elle est contraignante pour les entreprises et pour les consommateurs qui, j'imagine, dans 99,99 % des cas cliquent pour autoriser les témoins sur le site Web afin d'obtenir l'information qu'ils cherchent.

Est-ce que ce type de règlement apporte vraiment quelque chose? Je demandais tout à l'heure si quelqu'un a déjà lu minutieusement les politiques de confidentialité affichées sur les sites Web ou si vous cliquez très rapidement pour faire ce que vous avez à faire. De nos jours, les consommateurs cliquent toujours pour entrer sur le site.

La Loi sur la protection des renseignements personnels prévoit également un système de mesures de contrôle. Il n'est pas dans l'intérêt d'une entreprise du secteur privé d'utiliser à mauvais escient les renseignements personnels de ses propres clients. Vous pouvez parler à T.J. Maxx, à Home Depot ou à Target des conséquences d'une atteinte importante à la sécurité des données. Ces entreprises ont été victimes de telles atteintes, de pirates qui sont entrés dans leur système et qui ont accédé aux renseignements personnels de leurs clients. Ce sont des victimes et elles le sont doublement quand un certain nombre de clients... Pour les grandes entreprises, pas de problème, elles survivront. Une PME canadienne, en revanche, perdra la moitié de ses clients, ce qui lui sera généralement fatal.

Il est donc dans l'intérêt des entreprises lorsqu'elles collectent des données... Vous voyez maintenant combien elles sont utiles. Comme nous l'avons souligné, elles ont supplanté le pétrole. Elles ont une valeur énorme et il est dans l'intérêt des entités du secteur privé de les protéger, de les conserver et de pouvoir les analyser.

● (1620)

M. Ali Ehsassi: Je vous remercie.

Monsieur Hogarth, je suppose que votre point de vue est très différent, puisque vous avez dit que le modèle européen est exemplaire. Pourquoi pensez-vous qu'il ne serait pas trop contraignant pour les entreprises canadiennes?

M. Dennis Hogarth: Je ne dis pas qu'il ne serait pas contraignant. Je dis que nous devrions comparer les principaux points du RGPD et de la LPRPDE pour nous assurer de maintenir la conformité dans la mesure du possible. Je ne dis pas de mettre en oeuvre en bloc le RGPD au Canada.

Je crois qu'on s'est entendu sur le fait qu'il faut examiner certains points clés, environ quatre, dont celui sur les renseignements personnels concernant les enfants, qui est le principal. Par exemple, à la caisse d'un magasin Staples, on a proposé à ma fille, qui avait 14 ans, de s'inscrire sous son adresse courriel. Le caissier avait probablement 17 ou 18 ans.

Certains éléments de notre infrastructure doivent être renforcés. Je ne crois pas que les gens soient convenablement formés dans les organisations, tout comme le public en général n'est probablement pas aussi informé qu'il le devrait.

Il est certain que nous devrions faire notre possible pour maintenir la conformité au RGPD, du moins dans la mesure où nous restons pertinents. Croyez-moi, j'ai été confronté à des situations où nous avons essayé de transférer des données aux États-Unis, et c'est très difficile si vous devez procéder entreprise par entreprise.

M. Ali Ehsassi: Dans votre témoignage, vous mentionniez que les mégadonnées et la collecte de données pourraient présenter un risque pour les entreprises. Il me semble que la seule référence que vous ayez faite est à la cybercriminalité. Y a-t-il d'autres choses dont les entreprises devraient se préoccuper?

M. Dennis Hogarth: Il est certain que lorsqu'on se trouve dans un environnement où de plus en plus de données finissent dans des bases de données, elles ne resteront pas dans une seule organisation. Elles franchiront les limites organisationnelles et on en perdra la trace. C'est pourquoi je dis, en somme, que nous devrions adopter une norme.

Le consentement exprès est très peu pratique. Il nous faut un environnement où les organisations sont soumises à des tests, où quelqu'un d'autre examine les politiques de confidentialité parce que nous ne pouvons pas tout faire, comme quelqu'un l'a fait remarquer. Personne ici n'a probablement examiné plus d'une ou deux des politiques de confidentialité qui régissent nos vies, et il en existe peut-être 20, 30 ou 40. Elles devraient être soumises à un examen indépendant et être évaluées par rapport à une norme.

Le président: Merci beaucoup.

Nous allons passer à M. Jeneroux. Vous avez la parole.

M. Matt Jeneroux (Edmonton Riverbend, PCC): Je remercie les témoins de leur présence aujourd'hui.

Je voudrais simplement commencer par récapituler.

Monsieur Watson, vous dites non au pouvoir de rendre des ordonnances.

Monsieur Hogarth, vous êtes en faveur du pouvoir de rendre des ordonnances, n'est-ce pas?

Monsieur Smith, je n'ai pas compris votre position sur la question. Avez-vous un commentaire rapide?

M. Scott Smith: Le pouvoir de rendre des ordonnances est inutile, c'est pourquoi je renvoie dans mes observations au système judiciaire et au fait qu'il se montre très compétent dans toute affaire où des entreprises ont franchi les limites.

M. Matt Jeneroux: Très bien.

À ce sujet, le dernier examen législatif de cette loi remonte à 2007. À l'époque, de l'avis de MM. Watson et Smith, aucun pouvoir de rendre des ordonnances n'était nécessaire. Cependant, depuis lors, le Comité a examiné la Loi sur l'accès à l'information et la Loi sur la protection des renseignements personnels, et nous avons suggéré d'inclure dans les deux le pouvoir de rendre des ordonnances. Sachant cela, pensez-vous qu'il serait nécessaire que les dispositions relatives au pouvoir de rendre des ordonnances soient similaires dans toutes les lois ou est-ce que cela ne vous fait pas du tout changer d'avis?

Je commencerai par M. Hogarth.

● (1625)

M. Dennis Hogarth: Quand vous parlez de toutes les lois, à quelles lois faites-vous référence?

M. Matt Jeneroux: Désolé. Lors de son examen de la Loi sur l'accès à l'information et de la Loi sur la protection des renseignements personnels, le Comité a recommandé de conférer au commissaire le pouvoir de rendre des ordonnances. Les deux lois allant dans ce sens, seriez-vous aussi de cet avis?

M. Dennis Hogarth: Le pouvoir de rendre des ordonnances sera essentiel pour obtenir une conformité. Comme je l'ai dit dans mon témoignage, le problème est que ces organisations ne prennent pas les mesures voulues parce qu'elles voient qu'elles prennent peu de risques à ne pas se conformer. Si elles doivent dépenser 50 000 $ pour se conformer ou prendre le risque de ne pas se conformer sans guère s'exposer à une amende ou à une sanction, elles choisiront la solution de facilité.

M. Matt Jeneroux: D'accord.

Monsieur Smith?

M. Dennis Hogarth: Je l'ai en fait vu faire.

M. Scott Smith: Mes craintes à propos du pouvoir de rendre des ordonnances remontent à l'expérience que vivent certaines entreprises avec la Loi canadienne anti-pourriel, par exemple, aux termes de laquelle le pouvoir de rendre des ordonnances, l'organisme chargé de la conformité et l'organisme supposé dispenser des conseils ne font qu'un. Cela crée une situation difficile pour les entreprises. Aujourd'hui, cela changerait les relations entre le CPVP et les entreprises, qui sont amicales. Je craindrais qu'elles ne le soient plus.

M. Matt Jeneroux: D'accord.

M. Robert Watson: Nous disons que le pouvoir de rendre des ordonnances n'est pas nécessaire à l'heure actuelle, que le CPVP et l'industrie entretiennent de bonnes relations de travail.

Je ne suis pas tout à fait d'accord avec M. Hogarth en ceci que le coût de la non-conformité est élevé pour les entreprises et qu'elles le savent.

Il faut bien savoir aussi que ce dont nous parlons aujourd'hui n'arrêtera pas la cybercriminalité. Les cybercriminels continueront de sévir. C'est un tout autre sujet. Si quelqu'un veut voler vos données personnelles, ce n'est pas d'encore plus de règlements dont vous avez besoin. Ce qu'il vous faut, c'est installer d'autres applications pour l'en empêcher.

M. Matt Jeneroux: Je reviens donc à vous, monsieur Watson, sur un autre sujet, le droit à l'oubli et le droit à l'effacement. Vous avez parlé de la nécessité d'éduquer et pas nécessairement de légiférer sur ces aspects.

Nous avons du mal au Comité à déterminer quel type d'incident donnerait le droit à l'oubli et le droit à l'effacement. Autrement dit, mes collègues de l'autre côté de la table ne sont pas nécessairement du même avis que moi sur ce que tout le monde devrait oublier.

Étant donné ces différences d'opinions, comment formulez-vous cette éducation pour qu'elle soit utile et fructueuse?

M. Robert Watson: Là encore, je commencerai et André prendra la suite.

Pour ce qui est du droit à l'oubli, tout d'abord, avant qu'on nous oublie, nous devrions nous rappeler les différents types de personnes — et je veux dire de groupes d'âge —qui utilisent Internet. Leur attitude peut évoluer, mais à l'heure actuelle, peu importe les renseignements qu'ils donnent, et ils les donnent volontiers.

Si vous faites des affaires avec quelqu'un, le commissaire à la protection de la vie privée et les lois sur la protection des renseignements personnels vous donnent le droit de ne pas voir divulguer des données personnelles vous concernant. C'est entendu. Mais le droit à l'oubli... Je comprends l'idée. Je pense juste qu'essayer de l'inscrire dans un règlement renvoie exactement à ce que vous disiez: il existe tellement d'applications et de situations différentes qu'il sera très compliqué pour quiconque d'essayer de s'y conformer ou même de s'y adapter.

M. Matt Jeneroux: En effet.

M. Robert Watson: Là est le problème.

M. André Leduc: Vous ne verrez pas d'absence de conformité de l'industrie à une ordonnance judiciaire. Nous avons des procédures judiciaires en place, si un juge décide que le contenu d'un site Web doit être supprimé. L'entreprise ou l'hébergeur Web le supprimeront sans problème. En revanche, que se passe-t-il si le site est hébergé au Brésil?

Ajouter des règlements n'est donc pas forcément la meilleure solution. Nous avons déjà des lois pour régler cette question et les ordonnances judiciaires sont déjà suivies d'effet en ce qui concerne la suppression de contenu. La crainte serait qu'on charge l'industrie des fournisseurs de services Internet de réagir à ces situations. Si un consommateur déclare qu'il souhaite qu'on supprime des données qui le concernent, combien de fois ce type de demande se répétera-t-il?

Il existe une procédure judiciaire pour cela.

La question soulevée par Robert est que le commissaire à la protection de la vie privée est peut-être le plus apte à s'occuper de l'éducation, en tant qu'ombudsman mieux placé pour sensibiliser et travailler de concert avec les provinces en passant par le système scolaire pour informer les jeunes du risque que tout ce qu'on affiche en ligne y reste à tout jamais. Ce qu'on y verse n'est pas supprimé instantanément et quand on voit de jeunes filles afficher des photos d'elles-mêmes nues ou quoi que ce soit d'autre, une fois que ces photos se retrouvent sur un site Web, elles sont recopiées sur tout un tas d'autres.

La meilleure façon de contrôler la situation est d'informer les jeunes des dangers qu'elle comporte. Essayer d'imposer par règlement à tous ces sites Web de supprimer ce contenu ne peut être qu'une solution temporaire et jamais suffisante.

● (1630)

Le président: Très bien. Merci beaucoup.

[*Français*]

Monsieur Choquette, vous avez la parole pour sept minutes.

M. François Choquette (Drummond, NPD): Merci beaucoup, monsieur le président.

Je vais revenir au droit à l'oubli. C'est une question importante à laquelle tout le monde peut faire face un jour ou l'autre. Dans le rapport du commissaire à la protection de la vie privée intitulé « Réputation en ligne - Que dit-on à mon sujet? », on parle d'un citoyen espagnol au sujet duquel un renseignement circulait sur le Web — il avait une dette et celle-ci n'était pas remboursée. Cette information était facile à retracer: il s'agissait simplement de faire une recherche au moyen d'un moteur de recherche comme Google.

La cause de cette personne a finalement été entendue et le renseignement a été retiré, non pas de la page même où il se trouvait, mais du mécanisme de recherche sur le Web. Il y a cette question, mais il y a aussi celle que vous avez mentionnée, à savoir les personnes vulnérables.

De plus en plus, on demande aux enfants des renseignements personnels, notamment leur adresse courriel. De la même façon, on ne peut plus magasiner sans qu'on nous la demande également. On reçoit ensuite toutes sortes de messages publicitaires.

J'ai une fille qui aura bientôt 15 ans. Elle est sollicitée de toute part et me demande souvent ma carte de crédit pour acheter des produits en ligne. Ces questions sont importantes.

Quelles sont vos recommandations concernant le droit à l'oubli?

[*Traduction*]

Le président: Monsieur Smith, vous avez la parole.

M. Scott Smith: Certains commentaires faits plus tôt concernaient le droit à l'oubli. D'un point de vue réglementaire, il est pratiquement impossible pour le gouvernement du Canada, par exemple — ou pour tout gouvernement dans le monde — de supprimer l'empreinte numérique d'un affichage particulier. On ne peut pas agir à l'échelle mondiale.

En fait, il y a eu un cas dernièrement en Colombie-Britannique où quelqu'un volait de la propriété intellectuelle et la vendait sur Internet, et on a essayé de faire supprimer cette référence dans le monde entier. L'entreprise concernée a résisté et déclaré que le tribunal britanno-colombien n'était pas compétent pour statuer à l'échelle mondiale. C'est un véritable problème.

La question devrait porter davantage sur ce que font les entreprises pour régler ce problème. Les entreprises respectables et qui tiennent à leur réputation accèdent à ce type de demande, en particulier lorsqu'elles concernent des enfants. En essayant de réglementer et de dire qu'une chose est visée et pas une autre, on va au-devant de problèmes, car on risque d'oublier quelque chose ou d'aller trop loin. Il est pratiquement impossible de trouver un parfait équilibre.

[*Français*]

M. François Choquette: Monsieur Hogarth, qu'en pensez-vous?

● (1635)

[*Traduction*]

M. Dennis Hogarth: Je conviens qu'il est très difficile aujourd'hui de retracer l'information une fois qu'elle est mise sur Internet.

Je crois que nous mettons trop l'accent sur les enfants qui abusent d'Internet. Il y a plus en jeu que cela: des choses comme des renseignements médicaux personnels, des choses qui sont versées dans des bases de données à la suite d'achats par carte de crédit, et les données que les entreprises contrôlent très bien, mais qu'elles conservent bien plus longtemps qu'elles ne le devraient, surtout dans le cas des jeunes. Si on sait qu'on a affaire à des moins de 16 ans, il faut leur donner la possibilité de faire effacer ces données quand ils grandissent.

Il existe différentes catégories d'information. Je conviens qu'il est difficile de récupérer quelque chose une fois que c'est sur Internet, mais nous perdons de vue quantité d'autres données en nous concentrant toujours sur l'information qui se trouve sur Internet. Vraiment, beaucoup de données dans les bases de données deviennent périmées et inutiles, et il faudrait, en fait, les éliminer.

[*Français*]

M. François Choquette: Vous avez parlé de moderniser l'approche en matière de consentement. Je ne me souviens plus qui a demandé si nous avions déjà lu la page complète consacrée au consentement, rédigée en lettres minuscules, afin de savoir à quoi nous consentions. J'avoue pour ma part que, comme tout le monde, j'accepte les conditions et je passe à la prochaine étape. Nous ne pouvons pas refuser les conditions parce qu'autrement, nous ne pouvons pas accéder aux services que nous voulons obtenir.

Comment pourrait-on moderniser l'approche en matière de consentement?

[*Traduction*]

M. Robert Watson: Pour ce qui est du principe sur lequel reposent le droit à l'oubli et le droit de vérifier qu'on sait ce qu'on signe, il existe des lois au Canada. Si des renseignements personnels se trouvent sur une page Web, des lois permettent déjà de les faire retirer de cette page. Elles existent et elles suffisent en l'occurrence. Chercher une autre solution pour faire supprimer des renseignements d'une page Web parce qu'on a décidé de faire autrement... C'est de toute façon impossible. Nous ne pouvons donc pas ajouter de règlement.

Quant au droit relatif au consentement, les documents sont longs. Et s'ils sont aussi longs, c'est parce que leur préparation résulte de nombreuses interactions entre les gouvernements, les avocats des gouvernements et les avocats des organisations. Croyez-moi, les organisations préféreraient qu'ils soient aussi courts que possible. S'ils sont aussi longs, c'est pour qu'elles soient certaines non seulement de se protéger en tant qu'organisations, mais également de protéger le consommateur, parce que, si jamais on les traîne en justice, elles devront avoir l'assurance d'avoir donné au consommateur les droits voulus quand il a acheté le produit. C'est écrit noir sur blanc, elles doivent s'en assurer, parce qu'on ne peut pas, comme organisation où que ce soit dans le monde, et surtout au Canada, duper un consommateur: on ne survivrait pas au passage devant des tribunaux.

C'est donc écrit noir sur blanc. Il est inutile d'essayer d'élaborer un règlement qui dit qu'il faut veiller à savoir ce qu'on signe. C'est quelque chose qui existe déjà...

[*Français*]

M. François Choquette: J'aimerais entendre les commentaires de M. Hogarth à ce sujet.

[*Traduction*]

Le président: Pardon, monsieur Choquette, les sept minutes sont écoulées, mais nous reviendrons à vous dans quelques minutes.

Monsieur Saini, vous avez la parole.

M. Raj Saini (Kitchener-Centre, Lib.): Bonjour, messieurs. Merci beaucoup de vos exposés.

J'aimerais parler de quelque chose qu'on n'a pas vraiment examiné à propos du consentement.

Monsieur Hogarth, vous avez adressé un mémoire au Comité et vous y parlez d'une échelle mobile de consentement, d'un consentement qui devrait être explicite ou implicite. Je sais que l'an dernier, en août, l'ACTI a proposé, en réponse à un appel à consultation du CPVP, comme le mentionne votre mémoire, une nouvelle exception au consentement pour des intérêts commerciaux légitimes.

À présent que nous examinons la LPRPDE, et aussi étant donné que dans un an, le RGPD s'appliquera, que devrions-nous faire, selon vous, en ce qui concerne le consentement? Quel est votre avis sur la question?

Monsieur Smith, je ne sais pas ce que vous en pensez. Vous voudrez peut-être nous donner votre avis sur la question également.

M. Scott Smith: Si vous le voulez bien, je commencerai.

Des changements ont été apportés au consentement il y a moins de deux ans afin de le clarifier. Il me semble que les commentaires sur un consentement exprès sont un peu erronés en ceci que les données que les entreprises collectent ne sont pas identifiables. Pour l'essentiel, elles collectent des données sur le comportement qui leur permettent de créer des modèles prédictifs. L'idée qu'elles vont consacrer du temps et de l'argent à fusionner des fichiers de données pour identifier une personne en particulier... est irréaliste. Elles n'en retireraient aucun avantage. Elles n'ont aucun intérêt à le faire. Ce sont les données agrégées et les modèles prédictifs qu'elles permettent de créer qui présentent un réel intérêt.

L'idée que nous allons créer un nouveau modèle de consentement en vertu duquel les données qui proviennent de votre FitBit, qui sont ensuite vendues à des fabricants de médicaments, par exemple... On ne vend pas de données personnelles. Il s'agit de données agrégées et c'est l'intérêt qu'elles présentent qui est vendu.

● (1640)

M. Robert Watson: Le concept de degré de consentement est intéressant. Il y a le consentement absolu qui dit que la personne doit absolument consentir à toute interaction qui se produira, et c'est très peu pratique, jusqu'au fait que...

Je ne sais pas si vous avez vu qu'à Toronto, un membre du conseil a proposé que la capacité de fréquence FM de tous les téléphones cellulaires devrait être activée afin qu'en cas d'urgence, tous captent un éventuel message radiodiffusé. On peut penser qu'il s'agit d'un consentement socialement responsable. Certainement, puisque, peu importe où vous êtes dans la région et où on vous trouve, c'est pour le bien commun, parce qu'il peut se produire une urgence telle qu'il faut vous trouver — ce type de consentement.

Il existe aussi le consentement en vertu duquel vous passez simplement un contrat avec un fournisseur de services cellulaires pour utiliser ses services et grâce à cela — il doit évidemment savoir où vous vous trouvez —, il peut améliorer son réseau.

La question est donc celle du degré de consentement.

M. André Leduc: J'aimerais ajouter quelque chose. Dans ses observations préliminaires, Robert a attiré l'attention sur le critère de la personne raisonnable. Pour ce qui est de savoir si le consentement est le bon instrument, vous vous penchez actuellement sur la question. Mais, il s'agit de savoir si le consentement est éclairé. Est-ce que les gens se contentent de cliquer sans jamais rien lire? Est-ce que c'est ce qui se produit presque tout le temps? Je me risquerais à dire que oui, c'est ce qui se passe.

Si on veut s'assurer que les entreprises, y compris le secteur public, utilisent les données personnelles de façon responsable, il faudrait, à mon sens, ajouter ce critère de la personne raisonnable. Est-ce qu'un Canadien raisonnable penserait qu'il s'agit d'une utilisation appropriée de ses renseignements personnels ou pas? Voilà 100 ans qu'on invoque dans les tribunaux le critère de la personne raisonnable. Il me semble que dans notre monde trépidant, prendre le temps de lire et de comprendre ce à quoi on consent... L'entreprise essaie d'être transparente. C'est pourquoi ces politiques de confidentialité et les ententes juridiques sur l'utilisation finale sont tellement longues. C'est parce que nous avons ajouté la responsabilité juridique au scénario, entre autres. Leurs avocats disent qu'il « faut se prémunir contre la responsabilité juridique par ces documents », mais personne ne les lit.

S'agit-il d'un consentement éclairé? Je dirais que probablement pas dans 99,9 % des cas. Il vaudrait mieux déterminer ce qui constitue une utilisation raisonnable et responsable des renseignements personnels des Canadiens lorsqu'on les collecte.

M. Raj Saini: Monsieur Hogarth.

M. Dennis Hogarth: Je suis d'accord que personne ne lit les politiques de confidentialité. Elles sont trop compliquées et juridiques. C'est pourquoi je pense qu'il devrait y en avoir une évaluation indépendante, afin que les consommateurs puissent être avertis s'il est important qu'ils soient au courant de certaines conditions ou de certaines politiques en la matière. Quelqu'un pourrait avoir un site Web qui rende compte des principales questions et caractéristiques de ces différentes politiques de confidentialité.

En ce qui concerne le consentement, nous sommes tout à fait d'accord qu'il est impossible de donner un consentement pleinement éclairé dans le monde actuel. C'est pourquoi vous devriez probablement, selon nous, élargir la définition des données sensibles en ce qui concerne les choses pour lesquelles il faut obtenir un consentement explicite et un consentement implicite pour le reste. Le consommateur et le public ont besoin d'un point de référence en ce qui a trait à ces politiques pour déterminer si elles sont bonnes, mauvaises ou indifférentes.

● (1645)

M. Raj Saini: Je poursuivrai avec vous, monsieur Hogarth.

Dans votre mémoire, vous écrivez également que les organisations ne devraient pas conserver les données plus longtemps qu'il n'est raisonnablement nécessaire. Cela correspond en partie à ce que mes collègues mentionnaient à propos du droit à l'effacement à l'article 17 du RGPD.

Pouvez-vous nous donner quelques exemples de la façon dont nous devrions procéder en la matière, en particulier en cette ère des mégadonnées?

M. Dennis Hogarth: À l'ère des mégadonnées, et même avant, la question est, au fond, que les organisations devraient fixer un délai durant lequel il est raisonnable de conserver des données. Même dans un environnement de mégadonnées, il existe des outils qui peuvent baliser les données et fixer une date limite ou d'autres critères à leur égard. L'utilisation des mégadonnées va nous obliger à entrer dans ce monde. Mais nous ne pouvons pas entrer dans un monde de mégadonnées où règne une totale anarchie. Il existe des outils technologiques qui permettent d'utiliser des mégadonnées et de constituer des bases de mégadonnées. Il existe aussi des outils qui permettent de maîtriser les mégadonnées et il faut les utiliser.

Le président: Je vous remercie.

Nous allons passer à une série de cinq minutes et commencer par M. Kelly.

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

Je commencerai par vous, monsieur Hogarth.

Vous avez parlé des différents types de consentement et de la nécessité de faire la distinction entre ce qui est particulièrement sensible et ce qui l'est peut-être moins.

La LPRPDE présente-t-elle, en l'état, des lacunes particulières auxquelles il faut remédier? Dans les questions que vous avez soulevées, quelles sont les lacunes actuelles qui empêchent les types de meilleur traitement de l'information et différents types de consentement?

M. Dennis Hogarth: Je ne pense pas que ce soit une affaire de meilleur traitement. La LPRPDE est très explicite au sujet des données sensibles. À vrai dire, il faudrait que je réfléchisse aux éléments et aspects qui devraient sans doute être ajoutés.

Il va sans dire que certaines personnes estiment que leur adresse est confidentielle, tout comme leur numéro de cellulaire et, de plus en plus, l'information qui permet de les reconnaître, comme l'identificateur de leur cellulaire. La façon dont on peut retracer votre cellulaire pourrait être considérée comme une information sensible.

M. Pat Kelly: D'accord. Y a-t-il quelque chose de particulier que vous souhaiteriez voir arriver? Quel est le changement que vous voudriez voir apporter aux termes de la LPRPDE?

M. Dennis Hogarth: J'aimerais prendre le temps d'y réfléchir, si vous voulez bien.

M. Pat Kelly: Très bien. Peut-être que si j'obtiens les cinq prochaines minutes, je réessayerai, mais si vous pouviez y penser...

M. Robert Watson: Excusez-moi, est-ce que je peux...

M. Pat Kelly: Je vous en prie.

M. Robert Watson: À propos de votre dernière question au sujet des numéros de cellulaire et des adresses électroniques, les gens veulent les garder à vie pour des raisons pratiques. Il est possible maintenant de conserver son numéro de cellulaire dans tout le Canada. Vous pouvez le conserver avec n'importe quel autre fournisseur, si vous le souhaitez. Vos données doivent rester chez le fournisseur original et chez le nouveau fournisseur. C'est comme cela que cela fonctionne. Quoi qu'il arrive, votre adresse courriel et l'information que vous voulez conserver comme étant votre adresse courriel doivent rester chez le fournisseur de courriel original et chez le nouveau fournisseur de courriel. Voilà une application pratique de cette idée de consentement.

M. Pat Kelly: D'accord. Nous étudions la LPRPDE et nous arriverons, j'ose l'espérer, à un rapport qui recommandera des changements. Existe-t-il un obstacle? Ou y a-t-il des changements qui vous paraissent nécessaires à la loi en sa forme actuelle pour qu'on soit en mesure de répondre aux attentes des clients et pour permettre aux entreprises de se conformer?

● (1650)

M. André Leduc: Il me semble que, quand elle a été rédigée en 1999 et déposée à la Chambre, puis jusqu'à son adoption en 2001, nous cliquions sur des sites Web et nous n'utilisions pas autant ces appareils. J'irais jusqu'à dire que nous vivions à un rythme un peu plus lent.

Je crois que la question clé est celle que nous étudions; à savoir: le consentement est-il le bon moyen? S'il est une chose qui vaut la peine d'être examinée à propos de la LPRPDE, c'est quel est l'intérêt de donner son consentement en cliquant sans savoir ce à quoi on consent. Est-ce que nous devrions étudier un autre modèle qui supprime cette étape du processus pour lui préférer le critère de « l'utilisation raisonnable » et de la « personne raisonnable » pour évaluer ce que nous devrions collecter ou pas, ou ce que nous pouvons collecter, ainsi que l'utilisation et la communication de ces données par la suite?

M. Pat Kelly: D'accord.

Avec le temps qui me reste, je vais passer à un tout autre sujet et vous demander, monsieur Watson, de parler de ce que vous avez mentionné plus tôt, à savoir qu'il est important de faire la distinction entre l'activité criminelle et l'utilisation que les entreprises font des données. Vous avez dit que, quelle que soit la réglementation qu'on met en place pour protéger les entreprises, qui ont elles-mêmes intérêt, entre autres, à se conformer aux exigences pour éviter de ternir leur propre réputation, comme activité distincte de celle des pirates et des personnes qui se moquent de tout ce qui précède... Je vous laisserai en dire plus à ce sujet parce que cela me paraît important... La LPRPDE n'est pas le Code criminel. Ce n'est sans doute pas là que nous réprimons certaines des activités qui portent atteinte à la vie privée.

Le président: M. Kelly a utilisé tout son temps pour cette question. Je vous demanderai donc de répondre très succinctement, monsieur Watson.

M. Robert Watson: C'est simple. La cybersécurité ou la cybercriminalité se produisent de deux façons. Elles visent des données existantes qui se trouvent quelque part, mais de plus en plus maintenant, c'est au moment où vous effectuez la transaction qu'on vous cible. Il ne s'agit pas de données historiques.

Le président: Très bien.

Monsieur Long, je vous en prie, si vous pouvez être bref.

M. Wayne Long (Saint John—Rothesay, Lib.): Merci à nos témoins de cet après-midi. Une fois encore, vos témoignages étaient très intéressants. Plus nous en entendons, plus nous en apprenons, et plus de questions nous avons, me semble-t-il.

Je crois que ma première expérience en ce qui concerne le droit à l'oubli — et je promets qu'il ne s'agit pas de mon histoire de punaises avec les Sea Dogs de Saint John — remonte à 2005-2006, à l'époque où un joueur a fait une déclaration qui a été reprise aux nouvelles nationales. Il en a été question à *Hockey Night in Canada*, et j'ai dû faire certaines choses pour essayer de limiter les dégâts. Je ne jouais pas sur mon téléphone à l'instant, je le promets, mais pendant que vous parliez, j'ai cherché son nom sur Google et la première chose qui s'est affichée, c'est cette histoire, qui remonte pourtant à 11 ans.

J'adresse cette question à tout le groupe et vous répondrez en premier, monsieur Leduc et monsieur Watson. Pouvons-nous oublier le droit à l'oubli?

M. André Leduc: Je ne vous suggérerai pas de l'oublier. Vous devez aussi revenir en arrière, au monde d'avant Internet. Si quelque chose se retrouve dans un journal, c'est transféré sur microfiche et toujours accessible. C'est juste la façon d'accéder à l'information qui change. Nous utilisons un moteur de recherche et nous allons sur Internet, ce qui fait que nous y avons plus facilement accès qu'avant.

D'un point de vue juridique, les règles ne devraient pas changer parce que nous avons Internet. La personne a fait ces déclarations et ce qui serait intéressant de savoir, c'est si un juge lui accorderait le droit à l'oubli dans ces circonstances. C'est pourquoi nous renvoyons toujours à... Quand nous parlons d'un examen indépendant, il peut être fait par un juge qui décidera si cette personne a ou n'a pas le droit. Il ne s'agit pas d'une simple demande par laquelle je dis souhaiter que cette information disparaisse du site Web...

M. Wayne Long: C'est vrai.

M. André Leduc: Le recours existe déjà. Il existait avant l'arrivée d'Internet et il reste applicable aujourd'hui.

M. Wayne Long: Monsieur Watson.

M. Robert Watson: L'avantage d'Internet, qui est de permettre à tout le monde d'obtenir la même information — à condition, évidemment, d'avoir la bonne connexion —, en est aussi le problème. Tout le monde commet des erreurs et maintenant, l'erreur est là... On n'empêchera pas les gens de faire des erreurs...

M. Wayne Long: C'est exact. J'ajouterai que ce jeune homme, qui a maintenant 27 ans, passe des entrevues d'emploi et ses employeurs potentiels interrogent Internet. Là encore, la première chose qui s'affiche, c'est cet incident.

M. Robert Watson: Oui, immédiatement. Je le répète, c'est l'avantage d'Internet. C'est instantané. Autrefois, il aurait fallu attendre. La personne aurait probablement été employée depuis deux ou trois mois, quelqu'un aurait trouvé l'information et, alors, ç'en aurait été fini d'elle.

C'est une question de temps. Les gens commettront toujours des erreurs ou regretteront d'avoir dit des choses ou je ne sais quoi. Nous ne pouvons pas être sans arrêt à réglementer pour essayer de les protéger de leurs propres bêtises.

● (1655)

M. Wayne Long: Monsieur Smith.

M. Scott Smith: Je suis enclin à être d'accord avec cela. Nous parlons essentiellement de données historiques. Si les nouvelles reprennent l'information, alors elle existe sous une forme ou une autre. Ce n'est pas parce qu'on l'a supprimée d'Internet... Comme le soulignait André, elle continuera d'exister quelque part sous une autre forme. Même si ce n'est pas en ligne, on pourra probablement continuer de la trouver ailleurs. Quelqu'un sera capable de la consulter. On ne nous oublie jamais vraiment.

M. Wayne Long: Monsieur Hogarth, avez-vous quelque chose à ajouter à cela?

M. Dennis Hogarth: Prenons, par exemple, quelqu'un qui est accusé d'un crime, mais qui est finalement innocenté. Dix ans plus tard, les articles de presse sont toujours là et on les trouve si on les cherche. C'est le type d'information qu'il faudrait probablement oublier d'une certaine façon. Si quelqu'un est déclaré innocent, mais que l'accusation circule encore sur Internet ou que les articles de presse existent toujours, cela aura un impact sur sa carrière et sur sa vie future.

M. Wayne Long: Très bien. Je vous remercie.

Nous avons des FitBit. Notre famille en a. Nous sommes allés en acheter il y a quelques mois. Des amis qui ont de jeunes enfants sont venus. Je me suis inscrit sur le site de FitBit, fait ce que j'avais à faire, suis allé sur mon iPhone, et j'ai cliqué sur approuver, approuver, approuver... Hier, j'ai fait 15 168 pas, mon pouls au repos est à 59, j'ai parcouru sept kilomètres et j'ai dormi quatre heures quarante-cinq minutes.

Cela me convient tout à fait. J'ai cliqué sur toutes les notifications et appuyé sur tous les boutons. Mais que faisons-nous pour protéger nos enfants? Je crois que 70 % des enfants de 14 ans ont un téléphone aujourd'hui. Que faisons-nous explicitement pour les protéger? Le jeune de 14 ans qui a un FitBit a fait la même chose que moi en répondant oui à tout. Comment protégeons-nous les enfants dans le cadre de la LPRPDE? Que faisons-nous au sujet du consentement exprès?

Monsieur Leduc.

M. André Leduc: Des changements ont été apportés à la Loi sur la protection des renseignements personnels numériques pour mettre l'accent sur la protection des mineurs — pas les gars avec un chapeau qui vivent dans des grottes, mais les enfants dont nous devons nous occuper — et l'approche doit être équilibrée.

Robert a souligné que nous devons mieux informer. On parle de l'arrivée d'Internet. Ce n'est pas une mince affaire. Qu'il s'agisse des systèmes scolaires, des parents ou des groupes communautaires, nous devons éduquer les enfants au sujet des dangers potentiels.

Avec quelque chose comme FitBit, qui suit votre rythme cardiaque et tout le reste, il n'y a guère de risque. Ce dont nous parlons, dans le milieu des mégadonnées — et c'est intéressant —, c'est de la possibilité qu'un jour, on puisse vous avertir par message texte une demi-heure à l'avance de l'imminence d'une crise cardiaque. C'est vers cela que nous allons. C'est dans ce sens que va l'analyse des mégadonnées.

Pour ce qui est de protéger les mineurs, il est très difficile d'imposer la responsabilité aux entreprises qui collectent ces données, en dehors du fait qu'elles doivent vous demander si vous avez moins de 18 ans, moins de 19 ans ou moins de 21 ans, et si tel est le cas, vous dire que vous devez obtenir le consentement de vos parents pour fournir ces renseignements.

Il n'y a pas grand-chose d'autre. Combien de jeunes de 14 ans iront demander à leurs parents l'autorisation de fournir les renseignements sur le FitBit? Combien de parents les enverront promener?

Là encore, je sais que je me répète, si vous regardez le critère de l'utilisation raisonnable, du lien raisonnable et de la personne raisonnable pour évaluer ce qui est correct et ce qui ne l'est pas, vous voyez qu'il est beaucoup plus facile de l'utiliser que d'essayer de réglementer un régime de consentement qui ne présente peut-être aucun intérêt. On n'obtient pas vraiment de consentement éclairé et on ne peut pas vraiment jurer de l'âge de la personne dont on collecte les données, car je serais porté à croire que la plupart des jeunes de 14 ans passeront outre et, convaincus qu'on ne les laissera pas aller plus loin s'ils disent leur âge, ils cliquent sur 18 ans pour poursuivre.

Le président: Je vous remercie, monsieur Long. J'en ai conscience.

Je vais prendre cinq minutes sur la série des conservateurs, si mes collègues n'y voient pas d'inconvénient.

En tant qu'ancien professionnel des TI, je comprends tout à fait ce que vous dites quand vous expliquez que les données sont le bien le plus précieux des entreprises. Il en est ainsi depuis un moment en cette ère de l'information et, maintenant, comme vous le disiez, les données deviennent plus précieuses que le pétrole, ce qui est intéressant.

Monsieur Smith, je m'adresse à vous, car je vais revenir sur la question de M. Long. Les données deviennent extrêmement utiles. En fait, c'est l'information qui est le plus utile. Les données sont des faits bruts, tandis que l'information réunie est intéressante et utile.

Voici ma question, monsieur Smith. Vous avez expliqué très clairement que ce sont les données, les données anonymisées, qui permettent de prévoir des tendances et ainsi de suite, de prédire qu'un utilisateur ou un groupe d'utilisateurs particuliers appartenant à un certain groupe d'âge — ou présentant certaines caractéristiques — pourraient être intéressés, de sorte que nous pouvons avoir des modèles prédictifs aux fins de ventes et de commerce. Je ne pense pas que cela dérange grand monde.

Personnellement, j'apprécie le fait que mon iPad sache de temps en temps mieux que moi ce que je pense. C'est sans conséquence, mais dans le cas du FitBit, qu'arrivera-t-il si les données sur le sommeil, le pouls au repos et tout autre aspect de la santé qu'il recueille finissent entre les mains d'un employeur potentiel avant une entrevue? Qu'arrivera-t-il si les données n'ont pas été anonymisées, si nous savons qui elles concernent et que cela devient un problème, comme la discrimination génétique au sujet de laquelle un projet de loi vient d'être adopté au Parlement? Qu'arrivera-t-il si cela pose un problème qui empêche une personne de décrocher un emploi possible? Peut-être que FitBit calcule son poids et mesure d'autres habitudes et que ces données pourraient lui porter préjudice lorsqu'elle postulera à un emploi.

J'aimerais connaître le point de vue de M. Hogarth et de M. Smith sur le sujet.

● (1700)

M. Scott Smith: Je crois en avoir parlé dans mes observations, mais je ne me rappelle pas. Ma réponse à ce sujet est la suivante: quel serait le préjudice pour la réputation d'une entreprise comme FitBit si on apprenait qu'elle vend des données aux employeurs, aux sociétés d'assurances ou à je ne sais qui d'autre? Elle serait rapidement acculée à la faillite.

Cette information est, en effet, intéressante, et il est peut-être même tentant de la vendre à des employeurs potentiels, par exemple, mais la probabilité qu'une entreprise qui veut continuer d'exister franchisse le pas...

Le président: Et si l'employeur en question est FitBit?

M. Scott Smith: Là encore, on revient, je pense, aux politiques de confidentialité déjà en place et au fait que FitBit ne collecte pas du tout de données personnelles identifiables.

Est-ce que cela pourrait arriver? Certainement. Est-ce une probabilité? Non.

Le président: D'accord. Je vous crois.

Monsieur Hogarth.

M. Dennis Hogarth: J'ai une simple question. Les données de FitBit sont-elles des données sur la santé? Auquel cas elles appartiennent aux catégories sensibles pour lesquelles il faut un consentement explicite. C'est aussi simple que cela. Un consentement explicite est obligatoire pour qu'un tiers puisse les utiliser. Si ces données concernent un mineur, le consentement des parents est exigé.

Le président: Très bien, je comprends.

J'ai une question pour M. Watson ou M. Leduc.

En ce qui concerne le seuil de conformité, les sanctions pécuniaires, nous avons évoqué les différences.

Monsieur Leduc, ou peut-être monsieur Watson... Je pense que vous avez dit que Target s'en sortirait, que l'entreprise survivrait. Target survivra parce que l'entreprise est assez grande, mais une petite ou une moyenne entreprise pourrait ne pas survivre en cas d'atteinte à la protection de ses données et si les changements à la loi que le Comité pourrait recommander prévoient des sanctions pécuniaires.

Devrait-il y avoir un seuil? Je ne suis pas tellement pour qu'on trace des lignes arbitraires dans le sable sur le plan législatif, mais devrait-il y avoir un seuil de sorte que les petites entreprises qui n'ont pas nécessairement d'employé chargé de la protection des renseignements personnels...?

J'avais ma propre entreprise de TI avant d'être député. Je travaillais seul. J'étais mon propre consultant en protection des données personnelles. Que faisons-nous pour les petites entreprises? Devrions-nous avoir une exemption de sorte qu'elles ne soient pas touchées de la même façon qu'une grande société, ou est-ce que ce serait foncièrement inéquitable ou injuste?

M. André Leduc: Je ne l'ai pas mentionné dans mes observations préliminaires, mais ma thèse de MBA portait sur les PME, le respect de la LPRPDE et de la Loi canadienne anti-pourriel, et les conséquences pour les PME. J'ai même réalisé un sondage auprès de PME et organisé des groupes de réflexion.

Vous avez parlé du problème qui se posera. Une grande société pourra survivre. Si on lui inflige une sanction de 100 000 $, elle peut payer et continuer ses activités. Une petite entreprise risque d'être acculée à la faillite si elle se voit infliger une telle sanction.

En cas d'atteinte à la protection des données, l'entreprise est victime d'un pirate qui a infiltré son système et supprimé des données pour lui nuire ou collecter des renseignements personnels sur ses clients. Pour ce qui est de mettre en place des règlements pour faire comprendre aux entreprises qu'elles doivent conserver en lieu sûr les données qu'elles recueillent, elles le comprennent déjà.

Pénaliser une petite entreprise victime d'une atteinte à la protection de données n'est probablement pas la meilleure solution. Mieux vaut probablement la faire venir et demander au CPVP de lui expliquer ce qui s'est passé dans le piratage, faire l'enquête — elle comprendra la mécanique du piratage.

C'est le système actuel. On fait venir les petites et moyennes entreprises pour leur expliquer quels étaient les problèmes et pour s'assurer qu'elles se conformeront aux règles à l'avenir.

● (1705)

M. Robert Watson: Puis-je ajouter quelque chose?

Le président: Très rapidement, s'il vous plaît.

M. Robert Watson: Je serai bref. L'impact sur les grandes entreprises serait encore plus important que sur les petites entreprises, là encore à cause de leur réputation.

Je peux vous assurer que tous les conseils d'administration examinent maintenant très sérieusement le moindre incident qui a à voir avec les médias sociaux. Regardez ce qui est arrivé à la société de prêts hypothécaires de Toronto qui n'a pas fait attention à quelques déclarations inexactes, il y a trois ou quatre ans. Ce n'est pas comme si elle était insolvable, mais tous ses investisseurs ont retiré leurs fonds.

Le président: Monsieur Watson, personne autour de cette table ne comprend que quelque chose que nous avons dit il y a quatre ans puisse se retourner maintenant contre nous.

Monsieur Dubourg, vous avez cinq minutes. Je vous en prie.

[*Français*]

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

Je voudrais saluer les témoins qui sont parmi nous cet après-midi.

Je vous remercie de nous avoir livré votre présentation et de nous avoir soumis votre mémoire.

Ma première question s'adresse à M. Watson.

La position que vous faites valoir dans votre mémoire est qu'il n'y a pas lieu de changer la loi, que celle-ci demeure d'actualité. Malgré les avancées technologiques, vous considérez qu'il ne devrait pas y avoir de modifications législatives.

Est-ce bien ce que vous dites?

[*Traduction*]

M. Robert Watson: Nous pensons qu'une évolution est en marche, assurément. Internet évolue et vite. Cela ne fait aucun doute.

Nous sommes d'avis que la loi en vigueur est bonne. Ce qui devrait se passer, c'est que le CPVP devrait être davantage comme un ombudsman qui dispense des conseils, travaille en collaboration avec l'industrie, propose des changements. L'industrie sera d'accord. C'est certain. Il n'y a pas de manque de volonté à cet égard. Elle redoute seulement que si on commence à multiplier les règlements, cela ne s'arrêtera jamais. Les choses se compliqueront, c'est tout.

M. Emmanuel Dubourg: Je suis d'accord.

[*Français*]

L'autre aspect a trait aux pénalités. Vous êtes toujours sur la même longueur d'onde. Vous avez dit qu'on ne devrait pas accorder plus de pouvoirs au commissaire parce que l'approche collaborative fonctionne très bien, n'est-ce pas?

[*Traduction*]

M. Robert Watson: Je suis d'accord. Il peut venir dire que cette entreprise ne coopère pas et il le faut. S'il fait une déclaration, conciliante ou pas, l'entreprise ne la prendra pas à la légère, et je ne connais pas d'entreprise qui la prendrait à la légère.

[*Français*]

M. Emmanuel Dubourg: D'accord.

Je vais maintenant m'adresser à vous, monsieur Hogarth.

Votre rapport contient plusieurs mises en garde par rapport aux métadonnées. Vous dites qu'en 2020, il y aura plus de 50 milliards d'appareils connectés à Internet et que plusieurs renseignements seront obtenus de façon secrète, si je puis dire.

Vous portez le titre de Fellow de l'Ordre des comptables agréés.

Premièrement, y a-t-il des mesures de contrôle semblables à celles que vous suggérez que nous pourrions examiner pour améliorer ce projet de loi?

Deuxièmement, pouvez-vous faire des commentaires sur ce qu'a dit M. Leduc? En réponse à une question, il a dit qu'il serait difficile de mettre en place des mesures de contrôle dans le cas d'un enfant de 14 ou de 16 ans. Que peut-on mettre en place pour s'assurer que les données recueillies sont acceptables?

[*Traduction*]

M. Dennis Hogarth: Tout d'abord, une des choses que je souligne dans mon mémoire, c'est que c'est l'authentification qui est le problème et qu'elle deviendra de plus en plus problématique, non seulement en ce qui concerne les mineurs, mais aussi en ce qui nous concerne tous. Comment établissez-vous que vous êtes vraiment la personne qui donne son consentement ou qui donne accès à vos données? Ce point doit être examiné en détail. Il faudra, de toute façon, faire intervenir la technologie.

Votre premier point était?

● (1710)

M. Emmanuel Dubourg: Il concernait le contrôle.

[*Français*]

Peut-on mettre en place plus de mesures de contrôle pour s'assurer que les renseignements recueillis sont appropriés?

[*Traduction*]

M. Dennis Hogarth: Le contrôle des mégadonnées... Très souvent, quand je dis que les données sont collectées en secret, c'est un peu comme votre thermostat à la maison qui collecte un tas d'éléments d'information sur la façon dont vous faites tourner votre foyer. Il est question maintenant de réfrigérateurs qui recueillent des données sur tout, y compris sur ce qu'on y met.

Vous avez des automobiles qui fournissent des données qui pourraient être très utiles aux assureurs. Je ne crois pas que vous autorisiez votre voiture à dire que vous pouvez ou pas fournir toutes ces données.

De plus en plus, nous allons devoir trouver des moyens de nous pencher sur ces industries, pas nécessairement par rapport à un modèle de consentement, mais du point de vue d'un examen ou d'un audit de leur utilisation de l'information pour déterminer si elle est, en fait, raisonnable? Est-ce qu'elles satisfont au critère de ce qui est raisonnable?

M. Emmanuel Dubourg: Je vous remercie.

Le président: Merci beaucoup, monsieur Dubourg.

Le dernier député à poser des questions sera M. Choquette, qui dispose de trois minutes. Je demanderai ensuite aux témoins de quitter la salle, car nous poursuivrons les travaux du Comité à huis clos.

Je tiens à vous remercier de votre témoignage aujourd'hui.

Monsieur Choquette.

[*Français*]

M. François Choquette: Merci, monsieur le président.

J'aimerais revenir au mécanisme de résolution des différends. Lorsque le Commissariat à la protection de la vie privée du Canada fait enquête, il peut avoir recours à un mécanisme de résolution des différends, mais il ne peut pas imposer une amende ou une ordonnance. Par contre, les lois de l'Alberta et de la Colombie-Britannique en matière de protection des renseignements personnels qui s'appliquent au secteur privé confèrent au commissaire à l'information des pouvoirs d'ordonnance.

Avez-vous connu des cas particuliers où des pouvoirs d'ordonnance ont été exercés par le commissariat à la protection de la vie privée de l'Alberta ou celui de la Colombie-Britannique? Les résultats ont-ils été positifs ou négatifs? Comment les évalueriez-vous?

[*Traduction*]

M. Scott Smith: Je n'ai pas d'expérience directe du pouvoir de rendre des ordonnances en Alberta. Je le connais, au fond, par ouï-dire. Je répéterai ce qui a été dit plus tôt, qu'il crée un fossé entre les entreprises aux prises avec ces processus et le commissaire. Ce que je dirai à propos de la LPRPDE, c'est que je ne pense pas que quiconque puisse donner un exemple où le commissaire ait fait enquête, où la justice se soit prononcée et où il n'en soit pas résulté une mise en conformité.

Est-il nécessaire que le commissaire ait le pouvoir de rendre des ordonnances? À mon avis, non. Le système fonctionne fort bien à l'heure actuelle et le modifier changerait la dynamique.

M. Dennis Hogarth: Je souligne dans mon mémoire qu'il y a un risque d'incohérence entre les lois fédérales et provinciales qui nuirait certainement à beaucoup d'entreprises nationales.

Si vous devez examiner le succès ou l'échec des capacités de rendre des ordonnances, je crois que vous regarderez probablement ce qui se passe dans des pays qui ont mis en oeuvre ce type de programme, comme le Royaume-Uni et la France. Ils peuvent sembler un peu extrêmes, mais ils sont très efficaces pour ce qui est d'obtenir la conformité avec les exigences.

M. Robert Watson: Nous n'avons aucune expérience en ce qui concerne le pouvoir de rendre des ordonnances.

[*Français*]

M. François Choquette: D'accord.

[*Traduction*]

Le président: D'accord.

Nous sommes à peu près à trois minutes. Je remercie de nouveau les témoins d'avoir pris le temps de venir nous faire profiter de leurs compétences.

Je vais suspendre brièvement la réunion et nous reprendrons à huis clos. Nous avons à parler de quelques activités du Comité.

Merci beaucoup.

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