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 054 • 1re SESSION • 42e LÉGISLATURE

TÉMOIGNAGES

Le mardi 4 avril 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 4 avril 2017

● (1610)

[*Traduction*]

Le vice-président (M. Daniel Blaikie (Elmwood—Transcona, NPD)): La séance est ouverte.

Je tiens à expliquer aux témoins la situation, qui pourrait créer de la confusion. Je préside la réunion d'aujourd'hui. Je suis le deuxième vice-président, et le seul député du NPD à siéger au Comité. Ainsi, lorsque ce sera au tour du NPD de poser des questions, je vais changer de place et un autre membre du Comité assurera la présidence. Ce sera le jeu de la chaise musicale. Je voulais m'assurer que tout le monde comprenne pourquoi il en est ainsi.

Je vous remercie de votre présence. Nous recevons aujourd'hui David Young, directeur de David Young Law, Robert G. Parker, expert-conseil pour Risk Masters International Inc., Ian Kerr, professeur et titulaire de la Chaire de recherche du Canada en éthique, en droit et en technologie à l'Université d'Ottawa et Vincent Gautrais, professeur titulaire et directeur du Centre de recherche en droit public de la faculté de droit de l'Université de Montréal.

Merci à tous de témoigner devant nous aujourd'hui. Nous avons commencé en retard, alors nous allons tout de suite passer aux déclarations préliminaires.

Maître Young, voulez-vous commencer? Vous disposez de 10 minutes pour chaque exposé. Nous allons entendre les quatre témoins, puis nous passerons aux séries de questions.

M. David Young (directeur, David Young Law, à titre personnel): Bonjour monsieur le président, mesdames et messieurs les membres du Comité.

Je vous remercie de m'avoir invité à témoigner devant vous et à exposer mon opinion relativement à votre étude de la Loi sur la protection des renseignements personnels et les documents électroniques, la LPRPDE. Je vous ai fourni un mémoire, qui traite en profondeur des commentaires que je ferai aujourd'hui, et qui abordent d'autres sujets, notamment le droit à l'oubli et l'exigence du caractère adéquat de l'Union européenne. Je vous prie de lire mon mémoire pour connaître mon opinion sur ces deux sujets.

Je vais d'abord me présenter. Je suis directeur chez David Young Law, une société de conseils juridiques en lois et règlements sur la vie privée. À titre d'avocat en droit de la vie privée, je donnais des conseils aux membres du secteur public et du secteur privé, de même qu'aux particuliers, avant l'entrée en vigueur de la LPRPDE. Je fais partie de la Section nationale du droit de la vie privée et de l'accès à l'information de l'Association du Barreau canadien, et j'ai formulé certaines observations au présent Comité sur la révision précédente de la loi et sur la présente révision. Je tiens toutefois à souligner que je présente mon mémoire à titre personnel.

Cette révision de la LPRPDE survient à un moment particulièrement bien choisi. Dans notre monde numérique actuel, les problèmes entourant la vie privée se trouvent au coeur de nos réflexions. Je vous propose de traiter de deux enjeux précis: le consentement et le contrôle d'application.

Tout d'abord, la question du consentement. Le consentement constitue le principe clé des lois canadiennes sur la vie privée dans le secteur privé. Suivant ce principe, chacun a le droit de contrôler la collecte, l'utilisation et la divulgation de ses renseignements personnels, sous réserve d'un nombre limité d'exceptions. À mon avis, la formulation de la règle du consentement que l'on trouve dans la LPRPDE ne devrait pas faire l'objet d'une modification ou d'une limitation puisque son application dans diverses circonstances évoluera en pratique de manière à s'adapter aux constants changements dans la façon d'utiliser les renseignements.

Il serait très difficile d'exprimer, par l'entremise d'une modification à la LPRPDE, les besoins et les mécanismes précis pour prévoir d'une quelconque façon les impératifs d'un monde numérique qui évolue rapidement.

La présente consultation du Commissariat à la protection de la vie privée sur le consentement arrive à point nommé. À la suite de cette consultation, le CPVP devrait pouvoir proposer des balises et élaborer des principes pour veiller à ce que le consentement demeure une règle clé de la LPRPDE. Il importe de souligner que les tribunaux, notamment la Cour suprême du Canada, ont examiné les problèmes soulevés par le consentement et ont précisé que cette règle faisait l'objet d'importantes restrictions, telles que la liberté d'expression et l'application raisonnable du consentement présumé.

Certains des ajustements proposés affaibliraient la rigueur de cette règle et ouvriraient possiblement la porte à une plus grande collecte de renseignements personnels que ce qui se fait aujourd'hui. À mon avis, le commissaire à la protection de la vie privée en arrivera vraisemblablement à la même conclusion. De surcroît, cet affaiblissement pourrait compromettre notre capacité de nous conformer à l'exigence du caractère adéquat de la nouvelle règle en matière de vie privée de l'Union européenne, le Règlement général sur la protection des données, ou RGPD, dont vous avez beaucoup entendu parler.

À mon avis, la règle du consentement actuelle de la LPRPDE est suffisamment flexible pour répondre aux changements dans les pratiques de traitement de l'information et à l'innovation, et ne devrait pas être modifiée. L'objectif principal est de veiller à ce que les personnes aient le droit de contrôler et de protéger leurs renseignements personnels.

Le deuxième sujet que je veux aborder est le modèle de contrôle d'application. On a beaucoup parlé d'accroître les pouvoirs d'application du commissaire à la protection de la vie privée. Nous savons que, présentement, le rôle du commissaire correspond à celui d'un médiateur. Les dispositions réparatrices de la LPRPDE l'enjoignent à enquêter et à déposer un rapport sur les plaintes reçues.

Pour le moment, ces articles ne l'habilitent pas à ordonner à une organisation de prendre les mesures réparatrices nécessaires. Je crois qu'il a exercé l'autorité qui lui a été confiée à travers ce mécanisme de manière très efficace. Le commissaire exerce ses pouvoirs sous forme d'ordonnances: il présente ses conclusions, procède à des vérifications sur des organisations, fait des recommandations et, en vertu des récentes modifications apportées à la LPRPDE, il pourra conclure des accords de conformité et les faire respecter.

● (1615)

De plus, le commissaire peut rendre publiques les atteintes à la vie privée et nommer les parties en tort. Ce modèle a été essentiellement repris par les législateurs provinciaux en matière de vie privée, à l'exception d'un pouvoir formel permettant de rendre des ordonnances. En ce qui concerne l'efficacité de la mise en application, je pense que ce modèle fonctionne bien.

Cela dit, s'il est établi que le présent modèle n'offre pas les outils nécessaires pour assurer un contrôle d'application efficace, je crois qu'il serait possible d'ajouter aux pouvoirs du commissaire celui de faire des recommandations exécutoires (autrement dit, des ordonnances). Ce pouvoir ne devrait pas affaiblir le cadre régissant le rôle du commissaire en matière de résolution des plaintes, lequel est essentiellement axé sur la conformité.

Une autre suggestion mentionne que le commissaire devrait pouvoir imposer des amendes. Vous savez que ce pouvoir existe en vertu des compétences provinciales en matière de protection des renseignements personnels, ainsi que partout dans le monde. Premièrement, je vous signale que des amendes sont imposées en ce moment en vertu de certaines dispositions de la LPRPDE. Après l'entrée en vigueur des modifications proposées actuellement, une telle peine sera également imposée pour avoir omis de déclarer une atteinte. Deuxièmement, les organismes de réglementation ne sont pas habilités à imposer des amendes ou des sanctions pécuniaires en vertu des dispositions des lois provinciales en matière de protection des renseignements personnels dans le secteur privé. Dans certains cas (par exemple celui de la loi albertaine régissant le secteur privé), le législateur a prévu une infraction passible d'une amende pour les personnes ayant intentionnellement enfreint la loi. En fait, je crois que la loi albertaine est la seule à renfermer cette disposition précise. Selon celle-ci, la poursuite pénale pour une telle infraction relève des autorités provinciales responsables de l'application de la loi, et non de l'organisme de réglementation.

Sur la scène internationale, la législation diffère: par exemple, nous savons qu'en Europe, les organismes de réglementation peuvent imposer des sanctions pécuniaires pour les atteintes à la vie privée, ce qu'ils ont fait. Dans certains cas, ces amendes s'élèvent à plusieurs millions de dollars.

Au Canada, certaines lois imposent de telles sanctions pécuniaires, en particulier la Loi sur la concurrence et la Loi canadienne anti-pourriel. Cependant, je crois comprendre que, jusqu'à maintenant, les atteintes à la vie privée ne correspondent pas aux types de violations que le législateur tentait d'enrayer par ces lois.

Habiliter le commissaire à la protection de la vie privée à imposer des sanctions pécuniaires dénaturerait considérablement ses pouvoirs actuels et ne cadrerait pas avec le modèle de l'ombudsman. Cependant, si on le juge à propos, il serait possible d'arrondir les dispositions pénales de la LPRPDE afin de prévoir des sanctions pécuniaires pour des infractions comme une violation intentionnelle de la loi. Une telle disposition s'harmoniserait avec la nouvelle infraction prévue dans les cas où l'on ne se conforme pas à l'obligation de déclarer les atteintes.

Je dirais pour conclure que je conviens que l'étude du Comité devrait inclure un renvoi au nouveau règlement de l'UE sur la protection des données, c'est-à-dire le RGPD. Toutefois, dans l'état actuel des choses, il serait prématuré d'apporter d'importantes modifications à la LPRPDE en réaction au RGPD. Lorsque nous aurons travaillé plus longuement avec le RGPD et son processus d'examen du caractère adéquat du degré de protection transfrontalier, nous en aurons une opinion plus précise. Compte tenu de l'accent accru que le RGPD met sur les organismes d'application de la loi et les organismes de sécurité nationale, il est possible qu'il nous faille renforcer les mécanismes de protection des bases de données canadiennes auxquelles ces organismes ont accès.

Comme la LPRPDE est fondée sur un code rédigé à l'origine pour encourager la conformité volontaire, et qu'elle repose, par le fait même, sur des principes plutôt que des règles normatives, j'ai entendu bon nombre de gens déclarer au début de sa mise en oeuvre que la loi n'était pas bien conçue pour fournir des directives juridiques claires. Toutefois, la loi a clairement résisté à l'épreuve du temps et, à mon avis, son origine inhabituelle lui donne la souplesse requise pour faire face aux besoins en constante évolution de la technologie et du milieu numérique d'aujourd'hui. Cette compréhension a une grande incidence sur mon opinion par rapport aux modifications qui devraient être prises en considération au cours de la présente étude.

Je vous remercie encore une fois de l'occasion qui m'a été donnée de présenter mes points de vue.

● (1620)

M. Daniel Blaikie: Merci beaucoup, monsieur Young.

Monsieur Parker.

M. Robert Parker (expert-conseil, Risk Masters International Inc., à titre personnel): Merci.

Je m'appelle Robert Parker, et je suis un partenaire retraité de Deloitte & Touche. J'ai été mêlé pour la première fois à la protection de la vie privée en 1995 dans le cadre de ma participation à un groupe de travail de l'ISO sur la protection de la vie privée. Par la suite, en 2000, j'ai pris part au lancement du groupe de travail canado-américain sur la protection de la vie privée, qui a élaboré les principes généralement reconnus en matière de protection de la vie privée et, beaucoup plus récemment, le modèle d'évolution des pratiques en matière de protection des renseignements personnels.

J'ai fondé un service spécialisé en protection de la vie privée à Deloitte & Touche et, lorsque j'ai pris ma retraite en 2005, il comptait 40 employés, dont 15 à temps plein et 25 à temps partiel.

Comme cela a été mentionné, je suis maintenant au service de Risk Masters International Inc. Le groupe est composé de quatre partenaires retraités, dont trois qui travaillent aux États-Unis et moi-même, au Canada. Nous oeuvrons dans le domaine de la gestion des risques, qui comprend la protection des renseignements personnels, et nous avons élaboré un cours portant sur la protection des renseignements personnels que nous offrons aux États-Unis et qui traite des exigences en matière de protection des renseignements personnels liés aux soins de santé aux États-Unis.

Je vous remercie de l'occasion qui m'est donnée de présenter aux membres du Comité certaines de mes réflexions, et je suis impatient de participer à la discussion qui suivra.

J'ai répertorié sept enjeux dignes d'intérêt, et j'ai conscience que c'est un peu plus que les deux cernés par David. Toutefois, j'aimerais mettre l'accent sur seulement quatre d'entre eux.

Je vais laisser de côté l'avis d'atteinte à la vie privée. Je crois que nous devons accélérer l'exécution du travail à accomplir pour définir les exigences et les règles en matière d'avis d'atteinte à la vie privée, et pour préciser les obligations et les droits de l'une ou l'autre des parties en cas d'atteinte à la vie privée. Dans le cadre de mon travail avec une entreprise américaine, qui est également une société internationale, je me suis occupé de la façon dont elle gérait les atteintes à la vie privée liées à des documents papier et des documents électroniques.

La question du consentement valable est abordée dans un certain nombre de documents. Les problèmes à cet égard semblent mettre en valeur le contraste entre le bureau d'accueil et le bureau administratif. Le Centre for Democracy and Information a mené une étude qui a révélé un décalage complet entre ce que vous cochez sur le formulaire — ou ce sur quoi vous cliquez dans un site Web — et ce qui se passe dans le bureau administratif. Le personnel du bureau administratif doit modifier les bases de données afin de pouvoir enregistrer ce consentement. Il doit modifier toutes les applications qui consultent les bases de données afin qu'elles vérifient la présence ou non du consentement et qu'elles agissent en conséquence. Il s'agit là d'une énorme tâche et d'une étape que de nombreuses organisations ont simplement sautée, et c'est la raison pour laquelle il y a un décalage entre ce à quoi les gens ont consenti et le service qu'ils reçoivent souvent.

Le dernier élément est la propriété des renseignements non fournis. Il y a quelques années, un procès a eu lieu en Ontario — et je précise que je ne suis pas avocat. Il s'agissait d'une affaire très pointue qui, par conséquent, n'a pas permis d'établir un précédent, mais elle avait trait à des tissus humains. Dans le cadre de l'affaire, il a été dit que, dès leur prélèvement, les tissus humains appartiennent à l'hôpital, et non à la personne sur laquelle ils ont été prélevés. Je pense qu'il serait utile de clarifier des questions de non-consentement comme celle-là.

Des quatre enjeux dont je souhaite discuter, le premier est la collecte par rapport à la conservation, l'utilisation et la divulgation. Compte tenu de l'évolution actuelle de la société, un certain nombre de personnes et de jeunes de la génération du millénaire fournissent volontairement tous leurs renseignements. Ils affichent sur Facebook ce qu'ils ont mangé pour déjeuner, et ils utilisent Twitter. Ils sont très ouverts en ce qui concerne leur information. Ils ne perçoivent pas certains des problèmes que d'autres groupes de la société ou d'autres générations discernent. Il se peut que la question ou le problème ne soit pas lié tant à la collecte qu'à la conservation, l'utilisation, la divulgation et la façon dont l'information est sécurisée.

En 2005, après les attentats à la bombe dans le métro de Londres, les détectives ont été autorisés à enquêter sur les personnes que les gens avaient rencontrées jusqu'à six mois plus tôt. Ils ont retrouvé tous ces gens et ont réussi à identifier un certain nombre des responsables.

En Ontario, la décision rendue initialement autorisait la TTC à conserver les renseignements pendant 72 heures. Si elle n'en avait plus besoin après 72 heures.... J'ai conscience que, dans toutes les mesures législatives, il y a une clause relative à la sécurité nationale qui vous permet de conserver les renseignements plus longtemps, mais un grand nombre de gens le font de toute manière. Ils les recueillent et les conservent pendant une longue période de temps, qui peut remonter à de nombreuses années dans le cas d'un courriel ou d'une pièce de correspondance.

● (1625)

Si l'on tient compte de cela, la collecte n'est peut-être pas aussi problématique que la conservation, l'utilisation, la divulgation et la façon dont nous sécurisons très rigoureusement l'information, de manière à ce qu'elle ne soit pas utilisée d'une façon inappropriée. Le premier important enjeu est donc la collecte, l'utilisation et la divulgation.

Le deuxième est l'Internet des objets, c'est-à-dire lorsque nous utilisons le protocole IP pour faire marcher ses « objets ». Il peut s'agir d'objets mécaniques ou de systèmes, peu importe.

Je vais vous donner quelques exemples. Si votre voiture est assez neuve, elle est dotée d'un module de gestion du moteur. Ce module enregistre de nombreuses données, dont les taux d'accélération et de décélération, la vitesse à laquelle vous conduisez, entre autres choses. Ces renseignements sont-ils personnels? Votre voiture pourrait-elle renseigner les gens? Le mécanicien est en mesure d'avoir accès à ces renseignements, mais cela vaut aussi pour des services de police. En fait, une société d'assurances américaine affirme qu'elle réduira vos cotisations si vous lui donnez accès à ces renseignements, parce qu'elle croit que vous ne partirez pas en trombe, que vous ne freinerez pas brusquement et que vous ne conduirez pas à une vitesse excessive si elle peut consulter ces renseignements. Ces données sont-elles personnelles? Voilà un exemple concret.

Votre caméra pour tableau de bord est un autre exemple. L'information qu'elle collecte est-elle personnelle? Les services de police peuvent-ils la saisir? Ont-ils besoin, entre autres, d'une ordonnance du tribunal? Il y a beaucoup d'aspects de l'Internet des objets que, selon moi, nous ne devrions pas perdre de vue lorsque nous examinons la mesure législative.

Les données numériques dérivées sont le troisième des quatre enjeux. Les « données numériques dérivées » désignent au sens large l'information qui reste après avoir allumé les appareils. Lorsque vous effectuez une transaction sur Internet, des données numériques dérivées sont produites, comme l'heure à laquelle la transaction a eu lieu, ce qui s'est produit ici et là, les personnes qui ont participé à la transaction, leur adresse postale et tous les renseignements de ce genre. Cette information peut être revendue, et certaines personnes la revendent aux États-Unis. Au cours du week-end, vous avez peut-être remarqué le problème géré par la Federal Communications Commission, qui est en partie lié à cette question.

Nous sommes donc en présence de données numériques dérivées, c'est-à-dire de renseignements secondaires sur la transaction. Cette information vous appartient-elle? Appartient-elle à l'organisation qui a recueilli ses renseignements sur vous? Quels sont vos droits par rapport à leur utilisation et, en particulier, à leur revente à d'autres parties qui pourraient déterminer vos tendances comportementales et d'autres questions que vous ne souhaitez peut-être pas qu'elles cernent?

Le quatrième enjeu est le caractère adéquat de la sécurité. Lorsque nous avons examiné le premier enjeu ayant trait à la nécessité de bien protéger tous ces renseignements si nous planifions d'en recueillir davantage, nous avons parlé de la nécessité de prévoir des mesures de sécurité. Le problème, c'est que, bien que nous construisions des murs plus hauts et plus épais et que nous creusions des fossés plus profonds et plus larges, ces mesures ne fonctionnent pas. Les malfaiteurs réussissent tout de même à s'introduire dans les systèmes, et des atteintes à la protection des données surviennent.

Aux États-Unis, deux ou trois partenaires de Pricewaterhouse suggèrent que nous changions de paradigme, c'est-à-dire que nous permettions à tout le monde d'entrer. Vous connaissez le dicton : « Soyez proches de vos amis, et plus encore de vos ennemis ». Ainsi, vous établiriez un profil pour tous les visiteurs de votre site Web dans lequel vous analyseriez leurs activités et le modèle des anticipations. En ajoutant des mégadonnées à cette information, vous pourriez créer le profil de ces gens et, lorsqu'ils s'écarteraient de leur profil, vous pourriez les arrêter immédiatement.

Nous n'avons pas une mentalité de forteresse. Pour examiner ces données, nous devons changer de paradigme, mais cela signifie que nous devons recueillir des renseignements sur des personnes identifiables et établir des profils pour chacune d'entre elles. Est-ce une approche que nous souhaitons adopter, ou préférons-nous que la LPRPDE s'en occupe? Quoi qu'il en soit, ce changement de paradigme en matière de sécurité se produira dans les années à venir.

Voilà les quatre principaux sujets que je souhaitais aborder. C'est avec plaisir que je répondrai à la fin de la séance à toutes les questions concernant les trois sous-sujets.

● (1630)

J'aimerais mentionner les principes généralement reconnus en matière de protection des renseignements personnels qui ont été élaborés par un groupe de travail mixte Canada-États-Unis. Étant donné que le Canada y participe, ces principes sont heureusement publiés dans les deux langues officielles; il est donc facile d'y avoir accès, et je peux les faire parvenir au Comité. Il y a 10 principes et 72 critères, et c'est très contraignant. Cela concerne les atteintes à la protection des renseignements personnels, les avis, etc. C'est un document contraignant à un très grand degré. Étant donné que c'était très contraignant, nous avons opté pour le modèle d'évolution des pratiques en matière de protection des renseignements personnels. Nous avons pris le modèle de maturité de la capacité — du Carnegie Mellon et du département américain de la Défense — et avons créé le modèle d'évolution des pratiques en matière de protection des renseignements personnels qui explique comment un organisme doit agir... Je peux également vous le faire parvenir.

Je vous remercie de votre temps. Je sais que j'ai parlé 10 minutes et quelques secondes, mais je vous suis reconnaissant de m'avoir donné l'occasion de prendre la parole. Comme vous êtes à même de le constater, la protection des renseignements personnels me passionne.

Le vice-président (M. Daniel Blaikie): Merci beaucoup.

Passons maintenant à M. Kerr.

M. Ian Kerr (professeur et titulaire de la Chaire de recherche du Canada en éthique, en droit et en technologie, Université d'Ottawa, à titre personnel): Monsieur le président, messieurs les membres du Comité, merci et bonjour. Je vous remercie de me donner l'occasion de témoigner devant vous aujourd'hui dans le cadre de votre examen de la Loi sur la protection des renseignements personnels et les documents électroniques, soit une loi qui a désespérément besoin d'une réforme.

Je m'appelle Ian Kerr et je suis professeur à l'Université d'Ottawa, où j'occupe un poste qui touche à quatre sphères: la Faculté de droit, la Faculté de médecine, l'École des sciences de l'information et le Département de philosophie. Depuis 17 ans, je suis titulaire de la Chaire de recherche du Canada en éthique, en droit et en technologie. Les chaires de recherche du Canada sont détenues par « des chercheurs exceptionnels reconnus par leurs pairs comme des chefs de file mondiaux dans leur domaine ».

Je témoigne aujourd'hui devant vous à titre personnel.

J'aimerais tout d'abord renforcer certains points que d'autres témoins ont déjà fait valoir.

Premièrement, je suis en désaccord avec mon collègue David Young, parce que je crois qu'il est maintenant évident qu'il faut réclamer une application plus stricte des mesures et accorder au Commissariat à la protection de la vie privée le pouvoir de rendre des ordonnances et la capacité d'imposer de lourdes pénalités, y compris des amendes.

Comme Micheal Vonn de l'Assocciation des libertés civiles de la Colombie-Britannique l'a récemment dit devant le Comité: « Il n'y a plus d'arguments crédibles justifiant le maintien du modèle de l'ombudsman ». Cette idée a déjà été reconnue par le commissaire Therrien, l'ancienne commissaire Stoddart et la commissaire adjointe Bernier et a été renforcée par les témoignages de commissaires d'autres provinces qui ont déjà le pouvoir de rendre des ordonnances, ce que les commissaires Clayton et McArthur ont qualifié d'avantageux devant le Comité. De véritables pouvoirs d'enquête et le pouvoir de rendre des ordonnances sont nécessaires pour une application efficace des lois sur la protection des renseignements personnels, en particulier dans un contexte mondial. Faisons-le.

Deuxièmement, je suis d'accord avec l'ancienne commissaire Stoddart et le témoignage de Valerie Steeves qui ont toutes les deux affirmé que le libellé de la Loi doit être renforcé de manière à réaffirmer son objectif de protéger les droits de la personne. Comme Mme Steeves le souligne, il n'est plus possible de résumer les droits relatifs à la protection des renseignements personnels à la simple protection des données, et la protection des données ne se résume pas non plus à trouver un équilibre entre divers intérêts. L'établissement de la protection des renseignements personnels comme un droit de la personne, comme le fait la Loi, traduit un ensemble sous-jacent de valeurs démocratiques et d'engagements profonds et essentiels. Les droits relatifs à la protection des renseignements personnels ne sont pas que de simples compromis à l'intention des entreprises privées ou du gouvernement. Il faut renforcer le libellé de la Loi pour mettre davantage l'accent sur les droits de la personne.

Maintenant que j'ai insisté sur ces points, la majorité de mes commentaires porteront sur deux principaux thèmes que soulève votre étude: la transparence et le consentement valable. Je vais utiliser ces cadres pour orienter vos réflexions, mais il serait nécessaire à vrai dire d'approfondir ces deux concepts en raison de l'évolution rapide des technologies.

Lorsque la Loi a été adoptée, la principale métaphore concernait le roman *1984* de George Orwell et la maxime « Big Brother vous regarde ». Des droits bien établis relatifs à la protection des renseignements personnels étaient vus comme un antidote à la nouvelle possibilité qu'offraient la surveillance des données et l'utilisation des technologies de l'information par le gouvernement et l'industrie pour regarder, suivre et surveiller les gens en inspectant les données qu'ils laissent derrière eux durant leurs activités. Même si elle n'était pas un remède miracle, la tentative de limiter la collecte, l'utilisation et la divulgation de données par une loi neutre sur le plan technologique était vue comme une mesure corrective suffisante.

Cependant, les progrès technologiques depuis 17 ans, soit depuis la création de la Loi, permettent de faire beaucoup plus que seulement regarder. J'aimerais mettre l'accent aujourd'hui sur un seul exemple, soit l'utilisation de l'intelligence artificielle pour évaluer les risques et prendre des décisions de manière déléguée. Les humains sont remplacés par des machines. Au lieu d'être surveillés par Big Brother, nous nous dirigeons vers ce que Daniel Solove qualifie de:

> [...] une indifférence bureaucratique encore plus irréfléchie, des erreurs arbitraires et une déshumanisation, un monde où les gens se sentent impuissants et vulnérables, sans aucune forme de participation concrète dans la collecte et l'utilisation de leurs renseignements.

Il ne s'agit pas du roman *1984* de George Orwell; c'est le procès de Joseph K. de Franz Kafka.

Depuis la création de la Loi, le monde actuel permet l'utilisation de l'intelligence artificielle, qui est complexe et inscrutable, pour prendre des décisions importantes qui influent sur les chances et les possibilités qui s'offrent à nous dans la vie. Ces décisions sont souvent mises en oeuvre sans consulter les personnes touchées ou en les consultant peu et sans expliquer comment ces décisions ont été prises ou sans fournir suffisamment d'explications. De telles décisions peuvent être troublantes, injustes, non sécuritaires, imprévisibles, irresponsables et inconstitutionnelles. Elles nuisent aux droits fondamentaux, y compris les droits à l'application régulière de la loi et même à la présomption d'innocence.

Cela vaut la peine de nous pencher sur certains exemples réels. H&R Block se sert du programme Watson d'IBM pour prendre des décisions professionnelles concernant les impôts des gens. Parallèlement, les gouvernements utilisent l'intelligence artificielle pour trouver les personnes qui fraudent le fisc.

● (1635)

De grands cabinets d'avocats utilisent ROSS pour aider leurs clients à éviter des risques juridiques. Parallèlement, les organismes d'application de la loi ont recours à des programmes similaires pour repérer les personnes qui commettront des crimes et les détenus qui récidiveront. Les banques utilisent l'intelligence artificielle pour déterminer les personnes qui n'arriveront pas à rembourser leur prêt. Les universités utilisent l'intelligence artificielle pour décider des étudiants qui devraient y être admis. Des employeurs utilisent l'intelligence artificielle pour décider des personnes à embaucher, etc.

Cependant, voici où le bât blesse. La manière dont sont conçus ces programmes d'intelligence artificielle soulève des problèmes uniques en matière de protection des renseignements personnels. Beaucoup de personnes utilisent l'apprentissage automatique pour devenir excellentes à prendre des décisions. Cela signifie que l'intelligence artificielle peut aller au-delà de sa programmation initiale pour trouver des éléments dans les données que les décideurs humains ne verraient pas ou ne comprendraient pas.

Ce nouveau comportement est ce qui rend très utile l'intelligence artificielle, mais c'est aussi ce qui la rend inscrutable. L'apprentissage automatique, la découverte de connaissances dans les banques de données et d'autres techniques relatives à l'intelligence artificielle produisent des modèles décisionnels qui sont si radicalement différents de la manière dont les décisions sont prises par des humains que nous n'arrivons pas à les comprendre. Fait ironique, l'intelligence artificielle fait preuve d'une précision incroyable, mais ceux qui s'en servent et même leurs programmeurs ne savent souvent pas exactement comment et pourquoi.

Si nous permettons de telles décisions sans être en mesure de les comprendre, cela peut avoir l'effet d'éliminer les obstacles essentiels à la primauté du droit. Lorsqu'une institution utilise vos renseignements personnels et des données à votre sujet pour décider que votre prêt vous est refusé, que votre quartier fait l'objet d'une plus grande surveillance policière, que vous n'êtes pas admis à l'université, que vous n'obtenez pas l'emploi et que vous ne pouvez pas être remis en liberté et que personne ne peut vraiment expliquer ces décisions, de telles utilisations de vos données nuisent à vos droits relatifs à la protection des renseignements personnels.

À mon avis, c'est notamment la raison pour laquelle des spécialistes ont témoigné devant vous pour vous parler de ce qu'ils appellent la transparence des algorithmes, mais je tiens à faire valoir dans mon mémoire que la transparence ne va pas assez loin. C'est insuffisant de seulement demander aux gouvernements et aux entreprises de divulguer les renseignements utilisés ou recueillis lorsqu'une intelligence artificielle nuit aux chances et aux possibilités qui s'offrent à nous dans la vie. Ceux qui ont recours à l'intelligence artificielle ont l'obligation d'expliquer ces décisions de manière à nous permettre de remettre en question le processus décisionnel en soi. C'est un principe de base en matière de protection des renseignements personnels qui est inclus dans les mesures liées à la protection des données dans le monde.

J'affirme donc que la Loi exige d'expliquer les décisions prises par des machines. L'obligation d'expliquer vise la transparence et le consentement et va encore plus loin en vue de garantir les droits fondamentaux à l'application régulière de la loi et à la présomption d'innocence. C'est l'approche adoptée dans le Règlement général sur la protection des données. J'irais même encore plus loin. À la lumière de l'article 22 du Règlement général sur la protection des données de l'Union européenne, je suggère que la Loi sur la protection des renseignements personnels et les documents électroniques inclut aussi « le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé ».

La Loi a été adoptée pour protéger les humains et empêcher la technologie d'empiéter sur leurs droits. Les humains doivent donc continuer d'exercer un certain contrôle sur les décisions concernant les gens. La Loi devrait interdire la prise de décisions entièrement automatisée qui ne peut pas être comprise par les humains ou qui ne permet pas l'intervention des humains. À titre de précision, je ne propose pas cela pour arrimer nos pratiques à celles de l'Union européenne; je le fais, parce que c'est nécessaire en vue de protéger les droits de la personne.

Ma maman m'a bien élevé. Elle m'a entre autres appris qu'il ne faut pas accepter une invitation à souper pour ensuite se plaindre aux hôtes de ce qui est servi. En dépit des judicieux conseils de ma maman, j'aimerais conclure mon exposé en faisant deux observations désagréables.

Premièrement, je témoigne devant vous aujourd'hui, et je crois qu'il est juste de dire que j'ai raison d'avoir un sentiment de déjà vu. À l'exception de quelques nouveaux points, comme ma recommandation concernant l'obligation d'expliquer, la majorité des points que j'ai fait valoir et des points que tous les autres témoins ont fait valoir devant le Comité ont déjà été mentionnés auparavant.

Même si ces questions sont nouvelles pour de nombreux membres du Comité, ceux qui ont fait leur devoir se sont certainement rendu compte que nous avons déjà fait tout ce processus lors des réunions concernant le projet de loi S-4, le projet de loi C-13 et la Loi sur la protection des renseignements personnels, des réunions sur la protection des renseignements personnels et les médias sociaux et, bien entendu, de l'examen de 2006 de la Loi sur la protection des renseignements personnels et les documents électroniques. Or, nous constatons très peu de changements législatifs importants.

Même si l'étude en cours est importante, je vous dis en tout respect que vous n'êtes pas des conducteurs de Zamboni. Il faut arrêter de tourner en rond sur la même patinoire. Le temps est venu d'apporter des changements législatifs importants.

Deuxièmement, pendant que je me prépare aux séries de questions, je regarde autour de la table et je vois uniquement des hommes. Pour une raison que je n'arrive pas à m'expliquer, le Comité se compose uniquement d'hommes. Je suis conscient que vous avez convoqué un certain nombre de femmes à venir témoigner devant le Comité dans le cadre de l'étude. C'est évidemment logique. Après tout, une grande majorité des professionnels dans le domaine de la protection des renseignements personnels sont des femmes. Je crois en fait qu'il est juste de dire que les sommités mondiales dans le domaine de la protection des renseignements personnels sont majoritairement des femmes.

● (1640)

Je trouve renversant et injustifié qu'aucune femme ne siège au Comité; à mon avis, c'est une décision aussi incompréhensible que bon nombre de celles prises par des algorithmes.

Je me sens obligé de conclure mon exposé en faisant valoir ce point aux fins du compte rendu.

Merci d'avoir porté une attention particulière à mon exposé. J'ai hâte de répondre à vos questions.

Le vice-président (M. Daniel Blaikie): Merci beaucoup.

[*Français*]

Nous allons maintenant entendre la présentation de M. Gautrais, professeur titulaire et directeur du Centre de recherche en droit public à la Faculté de droit de l'Université de Montréal.

M. Vincent Gautrais (professeur titulaire, directeur du Centre de recherche en droit public, Faculté de droit, Université de Montréal, à titre personnel): Merci beaucoup, messieurs les membres du Comité.

Je m'appelle Vincent Gautrais. Je suis professeur de droit, avocat, directeur du Centre de recherche en droit public à l'Université de Montréal et titulaire de la Chaire L. R. Wilson en droit des technologies de l'information et du commerce électronique.

C'est évidemment un réel plaisir d'intervenir pour la seconde fois devant ce comité, relativement aux questions en lien avec la Loi sur la protection des renseignements personnels et les documents électroniques, et de participer comme Canadien à cet exercice démocratique.

À la différence de la dernière fois, en juin 2012, où le Comité nous invitait à réagir à cette loi de façon générale, cette fois, la lettre de M. Therrien, datée du 2 décembre 2016, nous guide sur certains éléments sujets à réflexion. Ainsi, je me permettrai de calquer les quatre thématiques qui ont été présentées dans son document, et c'est sur le premier point en lien avec le consentement que je vais utiliser une bonne partie de mes 10 minutes. En effet, j'ai particulièrement travaillé sur le sujet du contrat électronique, sujet sur lequel a porté ma thèse de doctorat, dans un autre siècle, il y a près de 25 ans.

Selon moi, et avec l'égard pour certaines propositions qui ont été présentées avant, il me semble que la situation actuelle est relativement ridicule. Ce constat malheureux est partagé par beaucoup. Il n'y a quasiment pas de débat. On le sait, personne ne lit les contrats en matière de vie privée, personne n'a raisonnablement la possibilité d'en prendre connaissance. Le contenu contractuel sur un écran ne dispose d'aucune limite d'espace. Les contrats sont donc infiniment longs. La Cour suprême, pourtant proactive et créative en bien des cas, n'a pas saisi l'occasion de lutter contre cette pratique clairement pathologique, en 2007, lors de l'affaire Dell Computer. C'est dommage.

C'est dommage, car avec le temps, le consentement est sorti de sa fonction initiale, de son but initial, alors qu'il visait au début à protéger l'individu afin de lui assurer un certain contrôle de ses propres données. Il est, au contraire, devenu le moyen de protéger les entreprises qui l'utilisent. Effectivement, les entreprises peuvent désormais totalement s'affranchir de tout contrat en noyant leurs obligations, leurs manières de faire, dans des pages et des pages. L'information, c'est comme l'oxygène, c'est nécessaire, oui, mais lorsqu'il y en a trop, on ne respire plus.

Devant ce constat d'échec, que fait-on? J'aimerais sur ce point vous présenter trois éléments. Le premier est bien la forme. Il est possible de croire que la situation serait bien meilleure, plus protectrice pour l'individu, pour le citoyen, si celui-ci devait manifester formellement son intention, si l'usager devait accepter au préalable une situation de fait. C'est le débat qui a déjà été présenté devant vous, devant ce comité, entre l'*opt out* versus l'*opt in* . Ce débat stigmatise bien, je crois, l'opposition classique sur le sujet, le second terme, l'*opt in*, étant plus protecteur que le premier.

Je crains malheureusement, après des années à avoir aimé cette idée, que la solution de l'*opt in* ait néanmoins quelques limites. Même clair, un contrat demeure inaccessible pour le commun des mortels. Il est inaccessible par sa longueur, par le fait qu'on ne lit pas de la même manière sur un écran, par les termes juridiques très compliqués que l'on y trouve, par les liens hypertextes qui constituent autant d'invitations à « sortir » du contrat et ainsi de suite. Le processus va vite et les internautes s'attendent à cette même vitesse. De plus, le taux d'analphabétisme fonctionnel rend la lecture des clauses contractuelles souvent bien illusoire. La mise en avant de la solution de l'*opt in* passe d'abord et avant tout par une attention particulière laissée sur la manifestation du consentement et dans une moindre mesure, en amont, sur la lisibilité du contrat.

Récemment, une chercheuse américaine montrait que le *clickwrap*, c'est-à-dire le fait de cliquer sur un bouton « J'accepte », plutôt que le fréquent *browsewrap*, qui est le fait de disposer quelque part, sur le site Web de l'entreprise, la politique sur la vie privée, n'avait quasiment aucune incidence sur la lecture d'un document. Elle montrait que seulement 0,36 % des personnes lisaient davantage le contrat, ce qui est, encore une fois, négligeable.

De la même manière, l'apparition de la pratique des bandeaux — vous avez tous vu cela — en bas des pages Web qui signifient l'acceptation des témoins, soit les fameux *cookies*, est davantage vue comme un irritant à la lecture plutôt qu'un outil qui permet de protéger l'individu.

● (1645)

Cette suspicion vis-à-vis du consentement se vérifie également en deuxième lieu sur le fond, et je ne crois pas que l'on puisse consentir à tout. Si, dans le droit des contrats en général, on dispose de règles sur les clauses abusives, par exemple, on ne vérifie que rarement cette réalité en matière de protection des renseignements personnels. Les clauses de consentement actuellement disponibles sur le Web sont truffées de stipulations qui sont clairement attentatoires aux intérêts des individus et rares sont les cas où le juge va contrôler ces clauses.

Que fait-on lorsqu'une entreprise demande à un candidat à un stage — c'est déjà arrivé dans un bureau d'avocats — de consentir à transmettre son mot de passe Facebook pour savoir ce qu'il a écrit sur son profil? Une étude réelle a montré que 48 % des usagers seraient prêts à donner leur mot de passe contre une barre de chocolat, mais on ne peut consentir à tout et il est important d'avoir un contrôle, me semble-t-il, sur certains éléments du contrat.

En troisième et dernier lieu sur le consentement, il existe des situations où le consentement ne peut, en pratique, être donné. C'est vrai en matière d'intelligence artificielle. Je mets au défi une entreprise d'expliquer convenablement à ses usagers l'utilisation qui est faite de leurs renseignements personnels dans le cadre du « *big data* ». Toujours dans une optique de déconstruction de ce réflexe contractuel, c'est la raison pour laquelle il y a lieu de multiplier les cas où le consentement n'est pas nécessaire ou requis. À titre d'exemple, les articles 67 et 68 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels du Québec font mention de cas où ce qu'on appelle des « ententes de communication » permettent d'utiliser des renseignements personnels sans le consentement des intéressés. Donc, il y a une entente entre les deux instances quant à l'utilisation des données.

Plutôt que demander un consentement presque fictif, mieux vaut présenter le dossier à des représentants du Commissariat, des spécialistes, des experts de la protection de la vie privée qui sont mieux à même de juger des garanties que l'entreprise souhaite offrir pour compenser l'utilisation de ces données. Cette solution des ententes de communication a d'ailleurs été proposée par votre comité en ce qui concerne la loi pour le secteur public, soit la Loi sur la protection des renseignements personnels, dans un récent rapport de décembre 2016, au paragraphe 2.2, recommandations 4, 5 et 6.

Par ces trois questionnements, soit la forme, le fond et les cas d'exonération du consentement, nous avons tenté de désacraliser le consentement. Comme le signalait un auteur britannique, il faut sortir du « fétichisme contractuel ».

Cela m'amène au deuxième point, qui sera beaucoup plus bref, faute de temps. Vous l'avez compris, j'ai tendance à penser que la capacité de contrôle de l'usager est limitée. L'individu ne peut pas faire grand-chose, sinon un peu en ce qui concerne le contrat, mais pas tant que cela. Aussi, où ce contrôle doit-il s'exercer?

Comme cela a été dit par plusieurs de mes prédécesseurs, on ne peut évidemment pas se passer — c'est un *no-brainer*, comme l'a dit M. Kerr — d'un commissariat à la protection de la vie privée qui bénéficie de prérogatives bien plus importantes que celles dont le commissaire dispose actuellement. Même si le Commissariat a la capacité de négocier des changements d'attitude auprès d'acteurs internationaux — ce qu'il a d'ailleurs très bien fait auprès de Google et de Facebook —, la loi actuelle se distingue par une incapacité d'action incroyable de la part du Commissariat, quand on la compare à la loi d'autres instances.

Il me semble donc que le sens de l'histoire passe par une hausse des prérogatives du Commissariat, hausse qui doit immanquablement passer par une capacité d'imposer des sanctions financières, comme cela a été dit déjà par plusieurs personnes. Ces sanctions pourraient se faire sentir d'une façon plus ponctuelle sur la réputation. Il est surprenant que, à la différence de l'immense majorité des décisions de justice au Canada, les décisions du Commissariat soient anonymes et que les noms des entreprises ne soient même pas présents, qu'ils soient caviardés et dissimulés.

Je ne traiterai pas du troisième point sur la réputation en ligne. D'abord, cela a été largement commenté, ensuite, j'ai moi-même pu, lors de ma précédente intervention en 2012, évoquer les réticences vis-à-vis de la notion de droit à l'oubli, qui mérite en effet une grande suspicion tant quant à son application que sur les conséquences qu'elle génère par rapport à d'autres libertés et droits fondamentaux.

Enfin, je souhaite dire quelques mots sur le caractère adéquat des articles 25 et 26 de la directive européenne de 1995 et maintenant des articles 44 et suivants du règlement européen de 2016.

● (1650)

Certes, il importe d'envisager les rapprochements avec nos partenaires européens. Cette région considère la vie privée d'une façon qui est digne d'intérêt. Je crois en revanche qu'il ne faut pas être trop ébloui par la perception de la vie privée qu'on a en Europe. La vie privée est une affaire de culture et cette perception diffère de la nôtre. Nous pouvons considérer ce qui se passe en Europe, mais il faut conserver notre spécificité canadienne.

En résumé, il s'agit d'intégrer davantage la nouveauté technologique, de désacraliser le consentement, d'assurer la spécificité canadienne et de faire en sorte que la loi soit un peu moins « décorative » en matière de sanctions.

Le vice-président (M. Daniel Blaikie): Merci beaucoup.

[*Traduction*]

Monsieur Bratina, vous avez la parole.

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

Mon cerveau tourne à plein régime, parce que je ne sais pas si nous arriverons à nous entendre sur un ensemble simple de faits sur lesquels nous pouvons nous appuyer pour aller de l'avant. Nous avons déjà une divergence d'opinions, comme l'a exprimé M. Kerr.

Monsieur Young, j'aimerais vous donner l'occasion de défendre votre point de vue par rapport à ce qu'a dit M. Kerr.

M. David Young: Merci. Je pensais justement à cela pendant qu'Ian présentait ses arguments.

Il y a certains éléments. Je ne crois pas que nous sommes en désaccord en ce qui a trait à l'essence de l'éthique que nous recherchons, c'est-à-dire le contrôle. J'utilise cette expression. C'est l'objectif actuel de notre loi; c'est le contrôle de vos renseignements personnels. Nous pourrions dire que le principe est violé aujourd'hui à certains égards. En fait, nous pourrions faire valoir que le principe est souvent violé en ce qui concerne les mégadonnées. Dans mon exposé et mon mémoire, j'ai donné des exemples, et une grande partie de ce dont parlait Ian concernant l'intelligence artificielle et d'autres travaux qu'il a réalisés portent vraiment sur les mégadonnées. Quel en est-il de l'aspect pratique de la chose?

Je dirais... et je crois ne pas être en gros désaccord avec la majorité de ce qu'a dit notre collègue de l'Université de Montréal. Nous devons le protéger. Je suis par contre en désaccord avec le professeur. Je sais que vous m'avez demandé de répondre aux arguments formulés par Ian, mais un avis n'est pas la solution. C'est la règle dans le secteur public. C'est l'élément auquel a fait allusion le professeur. Il suffit d'aviser les gens, puis vous pouvez faire tout ce que vous voulez.

C'est ce que nous avons actuellement avec la prétendue possibilité de nous y soustraire. Un avis est envoyé, et vous pouvez vous y soustraire, si cela ne vous convient pas. Cependant, si l'avis est inadéquat, vous n'aurez peut-être pas suffisamment de renseignements pour vous y soustraire ou vous n'aurez peut-être pas l'occasion de le faire.

Pour revenir à votre question, je crois que la règle du consentement que nous avons actuellement est très solide et devrait vraiment être appliquée. Comme je l'ai fait valoir, je ne dis pas qu'il serait impossible d'intégrer à la Loi des mécanismes pour améliorer cette règle ou nous attaquer à certains enjeux liés à l'apprentissage automatique qu'a soulevés Ian, mais je crois que la manière réaliste d'y arriver est de laisser le Commissariat à la protection de la vie privée orienter les intervenants. Le commissaire a accompli un excellent travail. Nous avons en fait au Canada des lignes directrices. Je n'essaye pas du tout de rabaisser notre organisme, mais la Federal Trade Commission aux États-Unis, où il n'y a aucune loi sur la protection des renseignements personnels ou aucune loi générale sur la protection des renseignements personnels, réalise un travail phénoménal, et nous l'écoutons et nous nous en servons pour nous orienter. Le Commissariat s'en sert pour s'orienter.

En toute honnêteté, j'élaborerais des mécanismes pour m'attaquer aux enjeux soulevés par Ian. Je conviens que vous ne devriez pas obtenir des résultats imprévisibles parce que vos données ont été regroupées avec celles des autres et que cela fait en sorte que les entreprises déterminent quelque chose à votre sujet auquel vous ne vous attendiez pas. Je suis tout à fait d'accord avec cela. Bref, je ne crois pas que c'est une règle que nous pourrions inclure dans la Loi.

● (1655)

M. Ian Kerr: Monsieur Bratina, si j'ai bien compris votre question, vous nous demandiez de parler de notre divergence d'opinions concernant la question de l'application des mesures...

M. Bob Bratina: Oui.

M. Ian Kerr: ... en ce qui concerne la question des pouvoirs. Je vais donc dire quelques mots à ce sujet.

M. Bob Bratina: D'accord.

M. Ian Kerr: Je crois que je vais également parler de la question du consentement qui a été soulevée.

M. Young signale — et avec raison, selon moi — que la FTC réalise un travail phénoménal, même si elle s'occupe de secteurs très précis, au lieu d'avoir une mesure législative omnibus, comme c'est le cas au Canada. L'une des principales raisons pour lesquelles la FTC accomplit un travail si spectaculaire, c'est qu'elle dispose de pouvoirs importants — le pouvoir de rendre des ordonnances et la capacité d'appliquer des mesures, y compris la capacité d'imposer des amendes.

J'aimerais vous donner un exemple. Je crois que cela rejoint aussi la question du consentement, car, si j'ai bien compris M. Gautrais, on doit dissiper certains des mythes entourant le consentement et les problèmes liés à la protection de la vie privée selon le modèle du consentement contractuel.

En 2009, les étudiants de la clinique en droit de la technologie de mon université ont déposé une plainte au Commissariat à la protection de la vie privée du Canada. La plainte concernait plus particulièrement Facebook et ses pratiques relatives aux renseignements personnels. La commissaire a donc effectué une enquête complète, qui a débouché sur une décision et des recommandations. Bien entendu, n'ayant pas le pouvoir de rendre des ordonnances ni la capacité d'imposer des amendes, elle ne pouvait que faire des recommandations.

Curieusement, alors que le monde entier attendait de voir la réponse de Facebook, le géant américain a décidé, par voie de conséquence ou, du moins, par pure coïncidence, d'établir des paramètres de confidentialité pour la toute première fois. C'était en 2010. Le monde était frappé de voir Facebook réagir à ces quelques plaintes relatives à la protection de la vie privée par l'instauration de paramètres de confidentialité, permettant ainsi aux gens de modifier leurs paramètres à leur guise. On semblait donner aux gens le pouvoir de contrôler leur vie privée.

Or, fait intéressant, voici ce qui s'est réellement passé: Facebook, qui emploie de nombreux psychologues, s'est rendu compte qu'entre 88 et 92 % de ses usagers ne changeraient jamais leurs paramètres de confidentialité. Par conséquent, l'établissement de ces paramètres de confidentialité est le fruit de la plus importante mainmise de données de l'histoire, et je crois qu'on n'a jamais rien vu de pareil depuis. Tout reposait sur le consentement et le contrôle.

Selon moi, ce genre de situations nous révèlent que le Commissariat à la protection de la vie privée du Canada, ou ses équivalents dans le monde entier, ne coordonnaient pas leurs interventions en misant sur le pouvoir de rendre des ordonnances et la capacité d'imposer des amendes, comme c'est de plus en plus le cas aujourd'hui. C'est précisément pour cette raison que Facebook pouvait s'en tirer.

Il est important de souligner que Mark Zuckerberg n'adhère pas aux mêmes paramètres que ceux qu'il a établis pour le reste du monde. Il a changé ses paramètres de confidentialité, sachant qu'il ferait partie des quelque 18 % de personnes disposées à modifier leurs paramètres de confidentialité. Je crois que cela en dit long, tant sur le pouvoir de rendre des ordonnances que sur l'illusion de contrôle et de consentement qui existe dans le droit relatif au respect de la vie privée.

● (1700)

M. Bob Bratina: J'allais vous poser une question sur la différence entre un principe et une interdiction; en fait, je me demande si nous devons tout simplement adopter une loi qui ressemble un peu aux 10 commandements, au lieu de nous occuper de détails sur lesquels nous ne semblons jamais nous entendre.

M. David Young: La LPRPDE se veut déjà cela. Elle compte 10 principes. Elle donne des explications supplémentaires utiles, qui servent maintenant de directives.

M. Daniel Blaikie: Monsieur Jeneroux.

M. Matt Jeneroux (Edmonton Riverbend, PCC): Merci, monsieur le président, et merci à vous tous d'être des nôtres, y compris M. Gautrais, qui est avec nous de façon virtuelle.

Monsieur Gautrais, je vais commencer par vous, si vous me le permettez. Je vais également insister sur certaines des observations que vous avez faites vers la fin de votre exposé. Lors de votre comparution devant notre comité en 2012, vous aviez dit ceci:

> [...] développer une approche strictement minimaliste sur le plan législatif, sans développer, me semble-t-il, de nouveaux concepts. D'ailleurs, on a pu voir de tels concepts en Europe, notamment, le « droit à l'oubli », qui a été développé dans plusieurs travaux européens et qui m'apparaît excessivement difficile à appliquer.

Un certain temps s'est écoulé depuis 2012. Plus précisément, nous savons que le règlement général sur la protection des données de l'Union européenne entrera en vigueur en 2018. Avez-vous changé d'avis à ce sujet? Vous en avez parlé un peu, mais j'espérais obtenir un peu plus de détails.

[*Français*]

M. Vincent Gautrais: Je vois que vous êtes très bien préparé, parce que vous avez fait des comparaisons. Merci de mentionner cela. Je crois honnêtement qu'il n'y a pas de changement de position parce qu'en matière de vie privée, mais aussi dans les autres domaines touchés par le numérique, chaque fois qu'on a changé les lois, on s'est retrouvé dans une situation très problématique. Cela a déjà été dit, notamment par M. Young.

Je pense effectivement que l'approche de principe que l'on trouve dans la loi est assez intéressante. Cela dit, en ce qui concerne le renforcement des pouvoirs de sanction d'un organisme de contrôle, comme peut l'être le Commissariat à la protection de la vie privée, je n'ai pas évoqué cette possibilité il y a cinq ans, parce que le Commissariat a effectivement fait un assez bon travail pour réussir à faire changer les choses, comme dans le cas de Facebook en 2009. En 2009, le Commissariat canadien a changé les pratiques dans le monde entier, ce qui est quand même incroyable si l'on considère que la Loi est très peu sévère et contient très peu de contraintes. Je crois quand même qu'on pourrait faciliter les choses, parce que la vie privée est devenue plus importante, parce que les risques sont plus importants. Le changement principal, effectivement, serait lié au fait qu'il faudrait renforcer les pouvoirs d'une instance. Je dirais que c'est le seul changement principal que je crois important. Cependant, l'approche de principe, à part le consentement, m'apparaît toujours applicable. Cela se voit notamment dans le texte du commissaire à la protection de la vie privée, M. Therrien, qui considère qu'il faut garder cette même approche.

[*Traduction*]

M. Matt Jeneroux: Très bien.

À la lumière de ces faits, surtout compte tenu de l'entrée en vigueur du règlement européen sur la protection des données en 2018, selon vous, y a-t-il des mesures urgentes que nous devrions prendre dès maintenant pour harmoniser nos pratiques avec celles de l'Union européenne?

Vous avez déjà effleuré la question, monsieur Gautrais, mais j'aimerais également inviter M. Parker à intervenir. Si vous avez quelque chose à ajouter en premier, monsieur Gautrais... ensuite, je vais céder la parole à M. Parker.

[*Français*]

M. Vincent Gautrais: Relativement à l'Europe, je crois vraiment, justement, qu'il n'y a pas d'urgence. C'est important d'être connecté, mais l'approche européenne me semble utile culturellement. Je la connais assez bien. Cela fait 25 ans que je suis au Canada, mais je suis venu de l'Europe. J'ai commencé mon droit en Europe, et il y a une différence culturelle très forte en matière de vie privée. On n'a pas la même perception et il ne faut donc pas être ébloui, comme je l'ai mentionné, par l'approche européenne. Il faut savoir garder notre spécificité canadienne, qui est très nord-américaine.

À mon avis, il n'y a pas d'urgence. Il ne faut pas être aveuglé non plus par la crainte. À mon avis, il est tout à fait possible de ne pas obtenir un avis de conformité, comme celui que nous avons reçu en 2001. Je crois que c'est effectivement possible qu'on ne l'obtienne pas, parce qu'il y a des nouveaux principes dans le règlement européen. Je crois aussi que le Groupe 29 en Europe, qui vérifie la conformité des pays étrangers, a durci ses positions. Je vais vous donner un exemple: en 2014, la loi québécoise sur la protection de la vie privée a été reconnue comme non conforme. On a demandé des précisions, alors que la loi canadienne est sans doute plus exigeante que celle de 2001. Je crois donc qu'il va y avoir des différences d'opinions, mais qu'il faut garder la spécificité canadienne qui existe dans la loi actuelle.

● (1705)

[*Traduction*]

M. Matt Jeneroux: Monsieur Parker, est-il urgent d'agir, sachant que le règlement sur la protection des données entrera en vigueur en 2018 en Europe? Je suis curieux d'entendre vos observations, surtout en ce qui concerne le « droit à l'oubli ».

M. Robert Parker: J'ai peut-être une opinion différente de celle d'autres personnes, mais je pense que le droit à l'oubli serait utile. Selon moi, les gens aimeraient avoir la possibilité d'extraire leurs renseignements. Par contre, j'ignore à quel point ce serait réalisable sur le plan technologique.

Pour vous donner un exemple, lorsqu'on sauvegarde des données sur des DVD — ce n'est plus une pratique très populaire de nos jours —, on ne peut pas en extraire un nom. Il faut réenregistrer tout le DVD; il est donc impossible de retirer les renseignements d'une personne.

Par ailleurs, il s'agit de déterminer l'emplacement de cette information au sein de l'organisation. Ainsi, les données pourraient être recueillies en un seul endroit et diffusées dans l'ensemble de l'organisation. Il pourrait être très difficile de repérer toutes les occurrences de l'information visée et de procéder de manière entièrement conforme au droit à l'oubli.

En principe, c'est une bonne idée, mais cela pose certains problèmes technologiques.

Le président suppléant (M. Pat Kelly (Calgary Rocky Ridge, PCC)): Il ne reste que 10 secondes, alors je vais céder la parole à M. Blaikie.

M. Daniel Blaikie: Merci beaucoup.

J'aimerais d'abord revenir sur un point soulevé par M. Young, à savoir l'idée d'établir un lien entre, d'une part, les amendes et les sanctions imposées en cas de violation de la loi sur la protection des renseignements personnels et, d'autre part, la preuve de l'intention. Je me demande si c'est bien ce que vous vouliez dire ou si...

M. David Young: Désolé, veuillez répéter la...

M. Daniel Blaikie: Il faut prouver l'intention d'enfreindre la loi avant de pouvoir imposer des sanctions, et je me demande si...

M. David Young: Comment fait-on pour vérifier l'intention? C'est ce que vous cherchez à savoir?

M. Daniel Blaikie: Je me demande s'il s'agit là d'un seuil trop élevé. Qu'en pensez-vous?

M. David Young: Non, pas vraiment. En fait, certains de mes collègues estiment qu'il s'agit peut-être d'un seuil trop faible.

Voici un exemple de cette hypothèse: les organisations prennent intentionnellement des mesures pour se conformer aux lois sur la protection des renseignements personnels. Elles élaborent des politiques en la matière, des procédures et toute une infrastructure. Si le commissaire finit par conclure que ces mesures ne sont pas conformes, s'agit-il d'une infraction intentionnelle? Les organisations en avaient-elles l'intention?

C'est très facile à dire... et, bien franchement, je pense qu'il faut un élément intentionnel lorsqu'on parle d'amendes. On n'impose pas d'amendes à quelqu'un pour cause de négligence, à moins qu'il s'agisse d'une négligence grave.

M. Daniel Blaikie: Ce que j'essaie de comprendre, c'est lorsque vous dites, par exemple, que les organismes d'application de la loi doivent être chargés de l'enquête et qu'ils doivent ensuite prouver l'intention. Je reconnais que, dans le cas d'une entreprise qui essaie, de bonne foi et en toute honnêteté, de respecter la vie privée des gens et qui met au point un système, lequel s'avère, au bout du compte, inadéquat, l'imposition de l'amende maximale risque de ne pas être un traitement équitable.

● (1710)

M. David Young: C'est cela.

M. Daniel Blaikie: Mais ne serait-il pas important, à ce moment-là, d'essayer de dissocier l'infraction — celle d'avoir un système inadéquat — de la sanction? Ne serait-il pas plus logique...

M. David Young: De leur imposer...

M. Daniel Blaikie: ... d'examiner l'intention en vue d'évaluer l'amende, plutôt que de déterminer s'il y a eu infraction ou si l'entreprise dispose d'un régime approprié?

M. David Young: J'ai sorti la loi de l'Alberta, et c'est ce qui est indiqué dans son libellé actuel: enfreindre intentionnellement les dispositions de la loi. Je ne suis pas sûr de la loi du Québec, mais à part cela, il s'agit de la seule loi au Canada qui impose des amendes en cas d'infraction.

M. Daniel Blaikie: C'est exact. Par exemple, je sais que dans d'autres domaines, comme la sécurité ferroviaire, il existe des lois à cet égard. Voici une partie du problème: si on invoque rarement ces dispositions législatives ou s'il n'y a pas beaucoup de causes gagnées en vertu d'une telle loi — peu importe les manquements à la sécurité dont il est question —, c'est parce que le fait d'essayer de prouver que l'entreprise avait l'intention de causer du tort est tout simplement un seuil trop élevé à atteindre.

M. David Young: Tout à fait.

M. Daniel Blaikie: Ne risquerions-nous pas de répéter quelque chose de semblable si c'était ainsi que nous...

M. David Young: Si on n'utilise pas le critère de l'intention, sur quoi allons-nous nous appuyer?

Nous sommes déjà sur le point d'ériger en infraction le défaut de signaler une atteinte, et il s'agit simplement d'un défaut de signaler une atteinte.

À certains égards, la réponse à ce que vous avez décrit réside dans la portée considérable de la diligence raisonnable. Ce principe fait partie du droit pénal et du droit réglementaire. On n'a pas besoin de l'énoncer par écrit, mais c'est écrit dans... Songez, par exemple, à la loi anti-pourriel.

En ce qui concerne l'exemple que vous avez donné, je crois que ce serait la meilleure façon de répondre.

J'espère que le Comité aura compris que, selon moi, le système fonctionne bien... et, abstraction faite de l'exemple donné par Ian concernant la réponse de Facebook. Il n'a pas aimé la façon dont Facebook a réagi. Alors, comment un pouvoir de rendre des ordonnances pourrait-il régler le problème? Facebook a continué de faire ce qu'elle faisait, mais elle a ajouté un avis de confidentialité, et tout le tralala.

Le système a fait ses preuves, à mon avis. Toutefois, je suis conscient des pressions en faveur de pouvoirs accrus en matière d'application de la loi. Là où je veux en venir, c'est que, dans le modèle actuel, le commissaire pourrait très facilement convertir son pouvoir de recommandation ou y ajouter un pouvoir de rendre des ordonnances. Au fond, c'est déjà ce qu'il fait actuellement. Il procède vraiment de cette façon, et ce, beaucoup plus qu'en 2007.

M. Daniel Blaikie: Comme mon temps est limité, je me demande si nous pouvons entendre maintenant l'avis de M. Kerr sur ce point et, ensuite, nous laisserons M. Parker intervenir à ce sujet.

M. Ian Kerr: Volontiers, et je vais essayer d'être bref.

Pour ce qui est de votre question de savoir si le critère de l'intention est une norme trop élevée, j'ai tendance à être d'accord là-dessus. Si nous fixons une norme de preuve si élevée — et ce genre de choses sont difficiles à établir —, au point d'en faire presque une norme de preuve en matière criminelle, et nous savons que les normes applicables en matière criminelle sont plus strictes... M. Young a posé une question, je crois, de nature rhétorique: si nous n'utilisons pas la norme de l'intention, quel critère allons-nous appliquer? Je dirais que nous pourrions suivre l'approche générale concernant l'attente raisonnable en matière de respect de la vie privée, qui est une norme objective fondée sur la notion du caractère raisonnable, et il y a tout un domaine du droit privé qui régit les préjudices causés aux personnes en fonction de la prévisibilité raisonnable et des autres aspects liés à une norme objective; bref, nous pourrions certainement trouver une façon de relever des fautes sans tenir compte de l'intention, comme vous le suggérez.

M. Daniel Blaikie: Merci.

Monsieur Parker.

M. Robert Parker: Relativement à la question de savoir s'il faut tenir compte de l'intention ou de l'incident, nous pouvons examiner certaines des décisions rendues par la FTC, surtout dans l'affaire mettant en cause CVS Pharmacy. Dans une des pharmacies, on n'avait pas bien formé les employés, si bien que ceux-ci avaient refusé de donner aux patients un accès à leurs propres renseignements médicaux. Résultat: une amende de 4,5 millions de dollars pour 53 incidents.

Par conséquent, dans cette affaire, la FTC semble avoir appliqué le critère de l'incident, et non celui de l'intention.

M. Daniel Blaikie: D'accord.

Pour ma dernière question, j'aimerais revenir sur la question des données numériques dérivées; si j'ai bien compris, lorsque je transmets mes renseignements à une entreprise dans un cadre général, celle-ci en devient propriétaire. Que peut-elle faire avec ces renseignements? Peut-elle les vendre à une autre organisation?

M. Robert Parker: Oui.

M. Daniel Blaikie: J'ai peut-être mal compris le concept, mais...

M. Robert Parker: Les données numériques dérivées, c'est ce qu'il reste après une transaction. Une fois que vous avez terminé la transaction et acheté les produits, vous laissez une marque d'horodatage qui indique quand la transaction a eu lieu. Vous laissez également des renseignements concernant votre carte de crédit ou peu importe le mode de paiement, notamment par PayPal. L'entreprise peut donc vendre tous ces autres éléments d'information.

● (1715)

M. Daniel Blaikie: Dans le contexte du modèle contractuel, cela signifie-t-il vraiment qu'on aura affaire à un formulaire et à un document de consentement plus longs? Ou y a-t-il une autre façon de s'y prendre, sans alourdir le formulaire de consentement?

Le président suppléant (M. Pat Kelly): Il vous reste juste assez de temps pour une courte réponse.

M. Robert Parker: Je crois que le modèle de consentement serait très difficile à établir. L'idée même de rendre le formulaire plus long, avec de plus en plus d'éléments de consentement...

M. David Young: Puis-je répondre en 15 secondes?

Le président suppléant (M. Pat Kelly): Nous avons dépassé le temps alloué. Je suis désolé. Nous pourrons peut-être y revenir dans une autre intervention.

C'est maintenant au tour de M. Saini.

M. Raj Saini (Kitchener-Centre, Lib.): Merci beaucoup, à vous tous, d'être des nôtres aujourd'hui.

Je voudrais revenir sur la question du droit à l'oubli. Il y a eu beaucoup de discussions à ce sujet, même au cours des séances antérieures. Certains ont dit que cette mesure ne résisterait pas à une contestation fondée sur la Charte.

Si nous laissons de côté la prémisse principale, quelle est votre opinion sur le droit à l'oubli pour les enfants? Croyez-vous qu'il devrait y avoir une disposition imposant une limite d'âge, au cas où des enfants mettraient des choses en ligne? Qu'en pensez-vous? Devrions-nous ajouter une disposition à cet égard?

La question s'adresse à vous tous.

M. Ian Kerr: Tout d'abord, une chose qui n'a pas été mentionnée aujourd'hui, mais qui, je le crois, a été évoquée lors de témoignages antérieurs, c'est que même si nous mettons de côté le droit pompeux d'être oublié dans le sens européen du terme, la LPRPDE et les lois sur la protection des renseignements personnels dans l'ensemble du Canada, ces principes auxquels nous avons si souvent fait allusion comprennent déjà quelque chose au sujet de l'exactitude des données. Dans les situations où des données seraient fausses ou trompeuses, je crois que le droit en matière de vie privée propose déjà qu'il devrait y avoir une certaine forme de réparation.

Comme l'ont mentionné, je crois, le professeur Florian Martin-Bariteau et la professeure Teresa Scassa, l'idée du droit d'effacer de l'information erronée qui aurait été mise en ligne pourrait être renforcée. Selon moi, c'est quelque chose qui est déjà couvert par les principes existants. Toutefois, dans le contexte des médias sociaux et des jeunes, il serait peut-être de bon conseil d'utiliser cela comme ancrage pour parler de quelque chose de beaucoup moins pompeux et vague que le droit d'être oublié, pour parler de quelque chose de beaucoup plus précis qui pourrait protéger nos enfants. Je crois que c'est ce que nous devrions faire.

M. David Young: Je serais assurément d'accord avec la possibilité d'instaurer un droit à l'oubli amélioré ou concevable à l'intention des enfants. Comme je le dis dans mon mémoire, je crois que nous avons un droit à l'oubli. Nous n'en connaissons pas encore la portée, mais la Cour suprême sera saisie de deux affaires en la matière au cours de la prochaine année, ce qui permettra de préciser les choses. C'est pour cette raison que nous devons être très prudents avec les dispositions générales du droit, car, bien franchement, je crois que nous avons déjà ce droit. Ian a mentionné la question de l'exactitude des renseignements. Il est possible de retirer son consentement. Le retrait du consentement est le droit de dire à quelqu'un qu'il ne peut plus utiliser et conserver vos renseignements, et qu'il doit les effacer.

La réponse simple à votre question est « oui ». Pour une foule de raison, nous avons eu des difficultés d'ordre constitutionnel lorsque nous avons dû légiférer au sujet du droit des enfants, mais je ne crois pas que c'est un problème insurmontable.

M. Robert Parker: Je souscris au retrait du consentement ainsi qu'au droit à l'oubli. En ce qui concerne les enfants, je n'ai pas regardé cela en détail, mais aux États-Unis, la COPPA — la « loi sur la protection des enfants en ligne » — fournit une certaine protection aux enfants de 13 ans et moins quant aux renseignements qu'ils fournissent ou qu'ils sont susceptibles de fournir à un fournisseur d'accès Internet.

Comme je l'ai dit, il est difficile d'éliminer de l'ensemble de l'organisation toutes les occurrences de l'information visée, surtout si les données ont été vendues à d'autres organisations. Je crois que c'est une bonne idée de permettre le retrait du consentement et d'avoir aussi le droit d'être oublié. Je vois toutefois des problèmes d'ordre technique.

[*Français*]

M. Vincent Gautrais: Si je peux me permettre, je ne suis pas sûr d'être très favorable à un droit particulier pour les enfants, comme viennent de l'accorder les Européens. En effet, le droit permet déjà de retirer certaines données lorsque les dommages sont plus grands. La situation des enfants est plus sensible, il est vrai. C'est donc déjà possible de le faire dans certains cas.

Je dirais aussi qu'il y a des solutions. Facebook, par exemple, est très réactif et arrive déjà très bien à retirer des images et des vidéos problématiques. Cette compagnie est extrêmement efficace car elle contrôle, contrairement à ce qu'elle affirme, les médias sociaux. Elle peut donc déjà limiter les dommages en retirant elle-même les données et les images des enfants. Ce n'est pas une situation qui pose problème.

● (1720)

[*Traduction*]

M. Raj Saini: J'avais une autre question à vous poser.

À l'heure actuelle, les sites Web que nous utilisons sont indexés automatiquement et ils ne peuvent être désindexés que sur demande. Croyez-vous que nous pourrions prévoir certaines dispositions pour faire l'inverse, c'est-à-dire d'avoir un système où vous auriez à décider de l'inclusion de vos renseignements plutôt qu'avoir à demander leur exclusion? Croyez-vous que c'est une bonne idée, un scénario idéal?

M. Ian Kerr: Je crois que c'est l'un des enjeux sur lesquels on peut de se faire une opinion de principe et dont la mise en oeuvre technique risquerait de saper l'idéalisme que ses défenseurs pourraient avoir, alors ma réponse prendra une autre tangente.

En général, je crois que tout réglage par défaut devrait être axé sur la protection des renseignements personnels. C'est le problème qui s'est produit lorsque Facebook a instauré ses réglages en la matière. Je crois que cela est particulièrement vrai dans le contexte de l'Internet, qui se souvient toujours de tout. Le premier ouvrage écrit par un universitaire à ce sujet s'intitulait *Delete* et il y était question de l'importance, à l'ère de l'information, de trouver des mandataires dont la fonction serait d'oublier.

Votre proposition ferait beaucoup pour nous rapprocher de cela, mais je crois aussi que cela rendrait l'environnement en ligne quasiment inutilisable. Je ne sais pas comment il serait possible de mettre cela en place par l'intermédiaire d'une prescription. Cette sorte de prescription serait un exemple de la façon dont la loi pourrait vraiment gâcher l'autre sorte de code — le code de logiciel.

Cela dit, je pense qu'il est absolument essentiel, dans le cadre des délibérations du Comité, que vous réfléchissiez bien à la façon de faire en sorte que ces réglages par défaut soient axés sur la protection des renseignements personnels. Ce serait un moyen d'essayer de faire cela.

Le vice-président (M. Daniel Blaikie): Il reste environ 30 secondes si quelqu'un d'autre voulait s'en prévaloir.

M. David Young: Pour en revenir à ce que Ian disait, aux États-Unis, il y a un idiome qui fait son chemin depuis un certain nombre d'années, le « do not track » — ou « ne pas suivre » —, qui est un réglage par défaut. Essentiellement, cela signifie que toute cette collecte de données que vous... Chaque fois que vous allez sur un site Web, des données sont colligées, tant celles que vous fournissez sciemment que celles qui sont transmises à votre insu. La règle actuelle est celle du choix de refuser: pour peu qu'on vous informe que c'est ce qui se passe, vous avez la possibilité de refuser cette collecte de renseignements. L'option contraire est celle de « ne pas suivre », et c'est vraiment la règle la mieux en mesure de protéger...

Le vice-président (M. Daniel Blaikie): Je crains bien que ce soit tout le temps de parole qu'avait M. Saini.

Nous voulons nous assurer que M. Kelly aura la totalité de ses cinq minutes pour poser des questions avant la fin de la séance.

M. Pat Kelly: Merci, monsieur Blaikie.

Monsieur Kerr, j'aimerais revenir aux passages les plus provocateurs de votre témoignage et, peut-être, demander aux autres témoins de nous dire ce qu'ils en pensent.

Vous avez pris une bonne partie de votre exposé pour parler des aspects potentiellement apeurants des prises de décision que pourrait prendre une intelligence artificielle. Comme l'ont fait d'autres, vous avez évoqué Orwell pour souligner le pouvoir de connaître et de suivre les activités des gens. Il y a cependant une importante distinction à faire — et qui n'a certainement pas échappé à Orwell — entre le scénario où l'information est recueillie, suivie ou utilisée à des fins malveillantes par un État et celui où des intervenants du secteur privé feraient la même chose, mais, vraisemblablement, avec le consentement des personnes concernées. Nous avons entendu parler abondamment de tous les différents problèmes associés au modèle de consentement, notamment lorsqu'il s'agit d'enfants.

Vous avez parlé du « devoir d'expliquer ». J'ai cru comprendre qu'une bonne partie des problèmes que certains voient relativement aux défis que vous avez mentionnés pourraient être résolus en... Lorsqu'il est question d'entreprises et d'intervenants du secteur privé, le simple fait qu'il y ait un choix — à condition qu'il y en ait un — ne suffit-il pas à apaiser les craintes que l'on pourrait avoir?

Je vais demander aux autres de me dire ce qu'ils pensent de cela, c'est-à-dire de la distinction qu'ils font entre un État qui collige de l'information sur les gens et qui traite avec désinvolture de leur vie privée, et des entreprises avec lesquelles on pourrait choisir de ne pas traiter.

● (1725)

M. Ian Kerr: Aurai-je aussi la possibilité de me prononcer là-dessus?

M. Pat Kelly: Bien sûr.

Je vais laisser les autres parler en premier, et nous allons tenter de nous assurer d'avoir assez de temps pour vous.

M. Robert Parker: Si vous pensez au modèle fondé sur le choix, oui, vous avez un certain contrôle, et cela devrait vous permettre de refuser que des renseignements soient utilisés d'une certaine façon ou conservés en votre nom. Je crois que c'est un très bon modèle, mais il ne fonctionne pas pour tous les scénarios.

Un autre exemple — vous n'avez qu'à remonter un peu plus loin —, c'est le fait qu'il est impossible de se faire oublier sur Internet. J'utilise Facebook avec parcimonie. Je n'y affiche pas de photos. Pourtant, ma photo est là et on y a ajouté mon nom. C'est quelqu'un d'autre qui a fait cela. Je suis désormais partout. Vous pouvez retirer certaines choses de là, mais peu importe ce que vous choisissez de retirer, soyez assurés qu'elle est quelque part dans le cyberespace.

M. David Young: Je crois que le problème le plus grave en ce qui concerne le choix à l'état pur, c'est que cela se résume à la possibilité de se retirer. Habituellement, on a le choix. Les options sont offertes. Celle de se retirer y est peut-être clairement indiquée, mais si vous ne la cochez pas, vous êtes pris dans l'engrenage.

Je peux vous assurer que c'est ce qui se passe dans le secteur privé. La réalité c'est qu'il faut signaler son retrait, sa non-participation, pas son consentement. Pour peu que l'on se fasse suffisamment avertir, pour peu que le procédé soit transparent et clair — c'est la thèse de Ian, et je ne m'y oppose pas —, alors il devrait être tout à fait possible de choisir. Je suis d'accord avec cela.

Cependant, je ne crois pas que c'est effectivement ce qui se passe dans la réalité. C'est ce qui est évoqué lorsqu'il est question de consentement valable. Je sais que vous avez entendu cela des milliers de fois. C'est un défi de taille, mais pas insurmontable. Ce ne sera jamais parfait, mais ce n'est pas un défi insurmontable.

[*Français*]

Le vice-président (M. Daniel Blaikie): Monsieur Gautrais, si vous voulez participer à la discussion, vous êtes le bienvenu.

M. Vincent Gautrais: Concernant le modèle de consentement, je répéterai simplement qu'à mon avis, la question n'est pas forcément de choisir entre l'*opt in* et l'*opt out*, bien que cela puisse fonctionner dans certains cas. Cette question n'est pas sans intérêt, mais il reste qu'on se fonde trop souvent sur un modèle basé sur le consentement alors que ce consentement est fictif. Il y a d'autres solutions, notamment un contrôle exercé par un organisme comme le Commissariat.

[*Traduction*]

M. Pat Kelly: M. Kerr voulait avoir un instant.

Le vice-président (M. Daniel Blaikie): Je sais, mais nous lui avons déjà donné un peu plus de temps.

Nous allons laisser la parole à M. Long jusqu'à la fin de la séance, ce qui lui laisse environ deux minutes.

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

J'aimerais approfondir cette question du consentement valable. Je reviens encore avec cette notion que j'évoque pour toutes mes questions, mais en ce qui concerne les enfants et le consentement valable, j'ai lu qu'à certains endroits, en bas de 13 ans, il faut le consentement d'un parent, qu'entre 13 et 15 ans, c'est un mélange de conditions, puis qu'il y a la catégorie des 15 ans et plus.

Monsieur Young, pouvez-vous nous dire en quoi consisterait pour vous un consentement valable?

M. David Young: Je crois qu'un consentement valable serait... et bien, ce serait de comprendre, point à la ligne. En fait, vous pouvez jeter un coup d'oeil aux modifications qui ont été apportées en 2015 à la Loi sur la protection des renseignements personnels et les documents électroniques. Il y est question d'un soi-disant consentement amélioré, alors je vous conseille de le lire. Je l'ai précisément sous les yeux. C'est une très bonne description de ce qu'est un consentement valable. Il s'agit de comprendre ce à quoi vous consentez.

J'aimerais apporter une précision à propos des enfants. Même s'il y a des règles très utiles comme la COPPA des États-Unis, la loi sur la protection des enfants en ligne, et une règle d'application volontaire à peu près pareille au Canada — elle est pilotée par l'Association canadienne du marketing —, je persiste à croire qu'un mineur ne peut pas donner son consentement.

Vous pouvez traiter cela comme un consentement, mais lorsque les enfants atteignent 18 ou 19 ans, ils ont le droit de retirer tout consentement donné antérieurement. Elle n'est pas exercée, mais je crois que c'est la règle juridique qui s'applique. Les enfants ont donc la possibilité de réévaluer leur consentement. Je crois que cela pourrait fonctionner pour ce « droit à l'oubli » pour les enfants, par exemple. Ils devraient avoir la possibilité de réévaluer leur consentement lorsqu'ils atteignent 18 ans.

● (1730)

M. Wayne Long: Monsieur Parker, avez-vous quoi que ce soit à dire au sujet de...

Le vice-président (M. Daniel Blaikie): Il ne reste que 20 secondes.

M. Robert Parker: Le consentement est ce que la personne donne. Alors vous consentez à ce qu'ils utilisent vos renseignements. C'est comme dans un bureau, lorsque vous vous présentez au comptoir et qu'il y a tous ces formulaires et tout le reste. Pour ce qui se passe dans l'arrière-boutique, il faut suffisamment de granularité pour que vos choix soient acheminés correctement — disons les formulaires A, B et D, mais pas C et E —, mais ce n'est pas ce qui se passe. La plupart du temps, les organisations qui font la collecte de ces renseignements ne changeront pas le système de l'arrière-boutique qui permettra ce degré de granularité. Alors, peu importe ce à quoi vous aurez consenti, vous allez vous retrouver avec tout ou rien.

M. Daniel Blaikie: Merci beaucoup, monsieur Parker.

C'est tout le temps que nous avions.

Merci beaucoup à nos témoins d'être venus, bien entendu, mais aussi d'avoir été patients durant les votes qui se sont tenus à la Chambre des communes.

Je tiens à mentionner, au cas où vous ne le sauriez pas, que si vous avez d'autres observations à présenter au Comité, vous pouvez nous les faire parvenir par écrit. De la même façon, si vous souhaitez apporter une réponse plus étoffée à une question qui aurait été soulevée aujourd'hui, nous vous invitons à communiquer avec le greffier afin de lui transmettre le fruit de vos réflexions.

Encore une fois, merci à tous.

La séance est levée.