CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

44e LÉGISLATURE, 1re SESSION

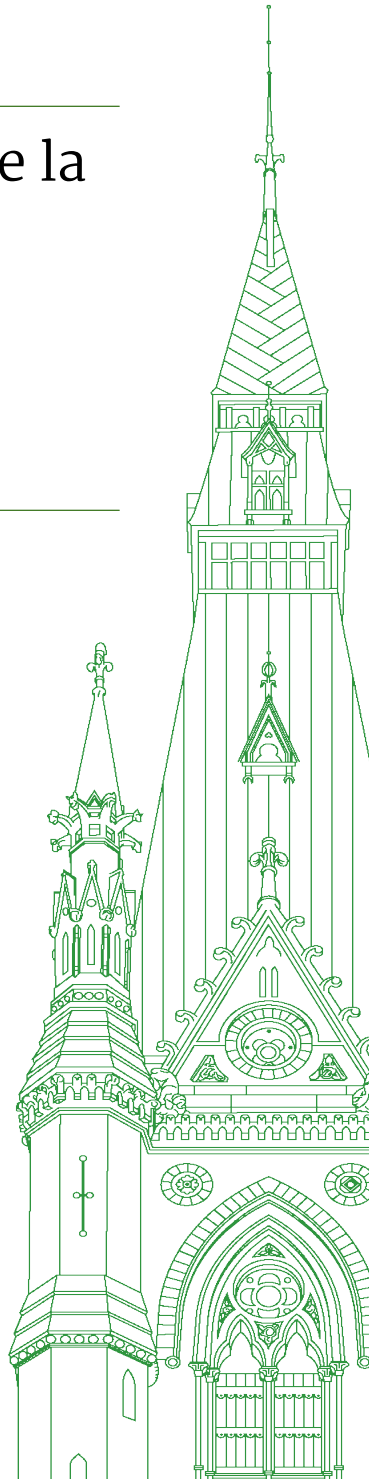
Comité permanent de l'industrie et de la technologie

TÉMOIGNAGES

NUMÉRO 100

PARTIE PUBLIQUE SEULEMENT - PUBLIC PART ONLY

Le jeudi 30 novembre 2023



Président : M. Joël Lightbound

Comité permanent de l'industrie et de la technologie

Le jeudi 30 novembre 2023

● (1555)

[*Français*]

Le président (M. Joël Lightbound (Louis-Hébert, Lib.)): Je déclare la séance ouverte.

Bonjour à tous et à toutes. Bienvenue à la 100e réunion du Comité permanent de l'industrie et de la technologie au cours de cette législature. C'est quand même une occasion spéciale.

Je tiens aussi à souligner que c'est l'anniversaire de notre analyste, Mme Alexandra Savoie. Nous lui souhaitons un joyeux anniversaire et la remercions de son aide pour cette importante étude.

Conformément à l'ordre de renvoi du lundi 24 avril 2023, le Comité reprend l'étude du projet de loi C-27, Loi édictant la Loi sur la protection de la vie privée des consommateurs, la Loi sur le Tribunal de la protection des renseignements personnels et des données et la Loi sur l'intelligence artificielle et les données et apportant des modifications corrélatives et connexes à d'autres lois.

J'aimerais souhaiter la bienvenue aux témoins et aussi leur présenter mes excuses pour le retard de cette réunion.

Nos témoins sont M. Sébastien Gambs, titulaire de la Chaire de recherche du Canada en analyse respectueuse de la vie privée et éthique des données massives, participant par vidéoconférence depuis l'Université du Québec à Montréal. Nous recevons également M. Philippe Letarte, directeur des relations gouvernementales et des affaires publiques à la société Flinks.

D'Option consommateurs, nous accueillons en personne les avocats Sara Eve Levac et Alexandre Plourde. Finalement, nous avons M. Sehl Mellouli, vice-recteur adjoint aux services à l'enseignement et à la formation tout au long de la vie, à l'Université Laval, qui se joint à nous par vidéoconférence.

Nous vous souhaitons la bienvenue à tous.

Sur ce, je ne prendrai pas plus de temps. Commençons sans plus tarder par les allocutions d'ouverture.

Monsieur Gambs, vous avez la parole pour cinq minutes.

M. Sébastien Gambs (titulaire de la Chaire de recherche du Canada en analyse respectueuse de la vie privée et éthique des données massives, Université du Québec à Montréal, à titre personnel): Bonjour et merci de m'avoir invité et offert la possibilité de m'adresser à vous.

Je vais faire mon intervention en français, mais je pourrai répondre aux questions en anglais ou en français par la suite. Au cours de ces cinq minutes, je vais tenter de me concentrer sur les notions de vie privée, d'explicabilité et d'équité en intelligence artificielle.

D'abord, il y a un élément important qu'on ne semble pas assez aborder dans le projet de loi. Quand on entraîne un modèle d'apprentissage, essentiellement, celui-ci va résumer les données personnelles à partir desquelles il a été entraîné. Il faudrait donc faire une évaluation des facteurs relatifs à la vie privée qui tient compte des attaques de l'état de l'art. Dans ma communauté de recherche, par exemple, on essaie de démontrer qu'on peut, à partir d'un modèle d'apprentissage ou d'une « boîte noire », comme un réseau de neurones, reconstruire des données d'entraînement.

Par ailleurs, un défi qu'on aura dans l'avenir et qu'on a actuellement, c'est que la plupart des modèles d'apprentissage que les gens développent sont améliorés à partir de modèles préentraînés qui ont eux-mêmes été entraînés à partir de données personnelles dont on ne connaît pas forcément l'origine. Je dirais donc qu'il va y avoir des défis importants à cet égard, en particulier dans le cas des systèmes d'intelligence artificielle à incidence élevée.

On voit aussi qu'il va y avoir des difficultés en ce qui concerne les créateurs de modèles et ceux qui les déploient. Par exemple, dans le projet de loi, à l'article 39 de la Loi sur l'intelligence artificielle et les données, on dit que les gens sont responsables de l'utilisation d'un modèle d'apprentissage, mais quand on parle de modèles de fondation, qui servent de base à des outils comme ChatGPT, ce sont des modèles qui peuvent servir à beaucoup de choses. Il est donc difficile pour le créateur d'un modèle de prévoir tous les usages bénéfiques ou mauvais qui pourraient en être faits. Il faudra donc réussir, en pratique, à faire la différence entre la personne qui a créé le modèle et l'usage qui est fait de celui-ci dans un cas particulier.

En ce qui concerne l'explicabilité, qui est le deuxième sujet important, au-delà de fournir une explication à une personne sur le pourquoi d'une prédiction, il faut aussi lui expliquer clairement quelles sont les données qui ont été collectées, le résultat final et son incidence sur les personnes. Il est particulièrement nécessaire d'être transparent à ces égards et de fournir une explication compréhensible dans le cas des systèmes d'intelligence artificielle à incidence élevée, afin que la personne ait des recours. Sans explication de qualité, essentiellement, on ne peut pas remettre en cause la décision de l'algorithme, puisqu'on ne la comprend pas. Dans le cas des systèmes à incidence élevée qui touchent des personnes, on devrait aussi avoir la possibilité d'avoir recours à un humain, quelque part dans le processus, qui a une solution permettant de réviser la décision. C'est une notion qui manque dans le projet de loi.

Alors, globalement, il faudrait faire une analyse d'impact qui tient compte non seulement des facteurs liés à la vie privée, mais aussi de ces questions éthiques. Je n'ai pas parlé de l'équité, mais c'est aussi un point important. Au-delà de la loi, un autre défi qu'on va avoir sera de se doter de normes en fonction des domaines d'application, afin de définir le bon indicateur d'équité à intégrer dans les systèmes d'intelligence artificielle et la bonne forme d'explication à offrir. Elle ne sera pas la même dans le domaine médical et dans le domaine bancaire, par exemple. Il faudra définir les mécanismes de protection à mettre en place dans chaque contexte.

J'aimerais terminer mon intervention en soulevant le risque associé au blanchiment éthique, une question sur laquelle j'ai travaillé. Essentiellement, cela prend des normes concrètes qui définissent l'indicateur d'équité qu'on doit utiliser dans un contexte particulier, car il y a beaucoup de définitions différentes de l'équité. Il y a déjà eu des débats entre des compagnies qui faisaient des systèmes d'intelligence artificielle et des chercheurs sur le fait qu'un système était discriminant. La compagnie disait qu'on n'avait pas utilisé le bon indicateur. Alors, sans normes précises mises en place par les parties prenantes, des entreprises pourraient tricher en disant que leur modèle ne discrimine pas, alors qu'elles ont choisi un indicateur d'équité qui les avantage. Il est aussi très facile de créer des explications qui semblent réalistes, mais qui ne reflètent pas du tout ce que fait la « boîte noire ».

Je dirais donc que la question du blanchiment éthique risque de se manifester quand la loi sera mise en application. Il faut réfléchir à des façons d'éviter cela et adopter des normes concrètes, qui ne seront pas forcément dans la loi, mais qui seront définies par la suite, pour éviter le flou juridique entourant les indicateurs d'équité et les formes d'explication liées aux questions de vie privée.

Enfin, s'il me reste 30 secondes, j'aimerais aborder un dernier élément en ce qui concerne la vie privée. La différence entre la définition d'une donnée anonymisée et celle d'une donnée dépersonnalisée est toujours difficile pour moi, car, en tant que chercheur en vie privée, je sais qu'il n'existe aucune méthode parfaite d'anonymisation des données.

Le projet de loi fait état de données anonymisées, un processus irréversible, et de renseignements dépersonnalisés, un processus qui, un jour ou l'autre, pourrait être inversé. En fait, je pense qu'il n'y a pas vraiment de méthode parfaite. Alors, même quand on nous dit qu'une donnée est anonymisée, en général, il y a toujours des risques de pouvoir identifier la personne à nouveau en croisant d'autres données ou d'autres systèmes. La différence de définition entre ces deux termes pourrait donc être clarifiée ou, en tout cas, devrait être clarifiée par des explications supplémentaires.

J'espère ne pas avoir trop débordé mon temps de parole.

● (1600)

Le président: Ça va. Je suis assez libéral avec le temps, mais je vous remercie de vous en soucier. Nous étions proches de la limite.

Monsieur Letarte, de Flinks, je vous cède maintenant la parole pour cinq minutes.

M. Philippe Letarte (directeur des relations gouvernementales et des affaires publiques, Flinks): Merci, monsieur le président.

Chers membres du Comité, je vous remercie de m'accueillir aujourd'hui.

Je m'appelle Philippe Letarte et je suis responsable des relations gouvernementales et des affaires publiques chez Flinks Technology inc.

Flinks est une entreprise technologique canadienne fondée à Montréal, dont la mission est de permettre aux consommateurs de contrôler leurs finances et de créer un environnement bancaire axé sur le client. Cet environnement bancaire, également appelé système bancaire ouvert, est basé sur la capacité du consommateur à contrôler et à diriger l'utilisation de ses données financières et personnelles, et ce, afin de recevoir les meilleurs services financiers et produits disponibles pour lui.

Afin de faciliter la période de discussion et d'éviter toute confusion possible relativement aux termes techniques, je vais continuer le reste de mon allocution en anglais.

[*Traduction*]

À Flinks, nous sommes heureux de voir que la notion de contrôle, ou de « consentement » dans le contexte de la législation sur la protection des renseignements personnels, est apparente partout dans la Loi sur la protection de la vie privée des consommateurs, ou LPVPC, qui, une fois en vigueur, va manifestement constituer la pierre angulaire de toutes les activités des organisations qui traitent des renseignements personnels. C'est une refonte grandement nécessaire de la loi qui a précédé la LPVPC. On va établir ainsi une approche qui protège davantage les consommateurs dans les activités de traitement, tout en rapprochant le régime de protection des renseignements personnels du Canada de ce qu'on voit dans les autres pays de l'OCDE. À Flinks, nous sommes heureux de voir que le consentement constituera dorénavant la base de toutes les activités de traitement de renseignements personnels.

Comme je l'ai déjà mentionné, l'une des raisons d'être de Flinks est de permettre aux consommateurs de contrôler leurs renseignements personnels et financiers, et de plus précisément dicter la façon dont ces renseignements sont utilisés et par qui. Fondamentalement, cela nécessite la participation de nombreuses personnes dans l'écosystème dans lequel Flinks mène actuellement ses activités.

Nous demeurons toutefois préoccupés par la formulation suivante proposée à l'article 72 de la LPVPC: « si ces deux organisations sont assujetties à un cadre de mobilité des données. » Cette formulation soulève des questions sur la façon dont une organisation participe à ce cadre, sur la possibilité qu'il y ait de multiples cadres pour différents types d'organisations, sur les limites en place lorsqu'une organisation donnée ne participe pas au cadre et sur les exigences qui devront être satisfaites pour continuer de se conformer au cadre.

Ce passage est également incompatible avec le libellé proposé dans l'énoncé économique de l'automne de la semaine dernière et dans l'énoncé de politique sur les services bancaires pour les gens, qui dit que le gouvernement fédéral imposera la participation des entités financières fédérales.

C'est dorénavant un fait incontestable que les pays avec des régimes bancaires ouverts efficaces ont non seulement forcé la participation au cadre d'une grande majorité de leurs institutions financières et des tierces parties, mais aussi, grâce à des règlements rigoureux et clairs, donné confiance aux consommateurs grâce à des protections adéquates.

Le libellé actuel risque de rendre inadéquats la LPVPC et les futurs règlements sur les services bancaires pour les gens, à défaut de préciser à quel cadre les entités et les ensembles de données seront assujettis, ce qui laissera les consommateurs perplexes et les privera des avantages de services financiers axés sur les gens. Nous recommandons donc de modifier le libellé de l'article 72 proposé afin de rendre obligatoire le cadre de portabilité des données pour les organisations du secteur financier — il n'est pas question de savoir si cela se fera, mais plutôt quand — et afin d'éviter des échappatoires ou des lacunes potentielles dans les différents règlements qui portent sur les droits de portabilité des données.

Nous sommes également préoccupés par le concept de l'exception relative au consentement en cas d'« intérêt légitime » qui est prévue aux paragraphes proposés 18(3) et 18(4) de la LPVPC. L'ajout de cette exception semble ouvrir la porte aux abus sans précisions supplémentaires, puisqu'aucune définition d'« intérêt légitime » ou d'« effet négatif » n'est fournie. Cela crée la possibilité d'un scénario dans lequel les organisations peuvent évaluer elles-mêmes le poids d'un intérêt légitime et d'un effet négatif, sans information supplémentaire sur laquelle s'appuyer à cette fin. C'est problématique, car une organisation pourrait, par exemple, chercher à utiliser l'exception concernant l'« intérêt légitime » comme moyen de contourner les limites mises en place par la LPVPC relativement au consentement ou aux utilisations secondaires des renseignements personnels. Ce type d'interprétation ou d'application d'un intérêt légitime par un participant dans un milieu bancaire ouvert éroderait complètement la confiance dans le système bancaire ouvert au Canada.

Veuillez donc nous permettre de respectueusement recommander l'éclaircissement de cette disposition à l'aide de définitions plus claires ou de critères d'évaluation pour ce qui constitue un « intérêt légitime » et un « effet négatif ». Dans le même ordre d'idées, nous demandons respectueusement au Comité de préciser également les types de scénarios ou de critères pour déterminer ce qui est « manifestement dans l'intérêt » d'un individu, comme on l'indique dans le paragraphe 29(1) proposé de la LPVPC.

En conclusion, j'aimerais répéter qu'il est urgent pour les Canadiens de pouvoir profiter d'un véritable système bancaire axé sur les consommateurs. Depuis l'avènement de l'économie numérique, peu de politiques publiques se sont révélées aussi profitables qu'un système bancaire ouvert. Cela favorise la concurrence et l'innovation dans un secteur très concentré et archaïque. Cela permet aussi aux consommateurs de prendre des décisions financières plus éclairées tout en ayant le contrôle de leurs propres données. C'est aussi un moyen d'accroître l'inclusion financière des plus vulnérables et de réduire les frais d'exploitation des petites entreprises tout en stimulant l'entrepreneuriat et les investissements étrangers, et j'en passe.

● (1605)

Les mesures proposées dans l'énoncé économique de l'automne, auxquelles s'ajoutent les dispositions et les protections établies dans la LPVPC, représentent une occasion unique d'offrir aux Canadiens une liberté financière et des protections adéquates de leurs renseignements personnels tout en comblant l'écart en matière de concurrence avec les partenaires commerciaux et d'autres économies modernes.

Je serai heureux de répondre de mon mieux aux questions que les membres du Comité pourraient avoir.

[*Français*]

Je le ferai aussi bien en français qu'en anglais.

Le président: Merci beaucoup, monsieur Letarte.

Je pense que M. Vis aimerait vous poser une question au sujet d'un article que vous avez mentionné.

[*Traduction*]

M. Brad Vis (Mission—Matsqui—Fraser Canyon, PCC): Monsieur Letarte, à la fin de votre déclaration, avez-vous mentionné l'article 21 ou le 29?

M. Philippe Letarte: Ce serait le paragraphe 29(1) proposé à l'article 2.

M. Brad Vis: C'est le paragraphe 29(1) proposé. Merci.

[*Français*]

Le président: Merci beaucoup.

Je donne maintenant la parole aux représentants d'Option consommateurs. Maître Levac ou maître Plourde, vous avez la parole.

Me Alexandre Plourde (avocat et analyste, Option consommateurs): Bonjour, monsieur le président et mesdames et messieurs les membres du Comité.

Nous vous remercions de nous offrir l'occasion de vous présenter nos observations.

Je m'appelle Alexandre Plourde. Je suis avocat chez Option consommateurs. Je suis accompagné de ma collègue Sara Eve Levac, qui est également avocate chez Option consommateurs.

Option consommateurs est une association à but non lucratif qui a pour mission d'aider les consommateurs à défendre leurs droits. En tant qu'association de consommateurs, nous sommes régulièrement en contact avec des citoyens qui éprouvent des difficultés en matière de protection de la vie privée. Au cours des dernières années, nous sommes fréquemment intervenus sur des questions touchant la vie privée, notamment en publiant des rapports de recherche et en participant à des consultations sur des projets de loi. Nous avons également entrepris des actions collectives d'envergure qui se fondent notamment sur la loi fédérale sur la protection des renseignements personnels.

Comme vous pourrez le lire dans le mémoire que nous avons soumis au Comité, le projet de loi C-27 comporte, selon nous, plusieurs lacunes, notamment quant aux exceptions au consentement, à l'absence du droit à l'oubli, aux limitations du droit à la portabilité et à l'encadrement des données des citoyens après leur décès.

Puisque le temps nous est compté, nous allons aborder deux aspects du projet de loi C-27 qui nous préoccupent plus particulièrement.

Premièrement, je vais parler du manque d'effet dissuasif du projet de loi C-27 et des entraves que celui-ci pourrait poser aux recours civils engagés par les consommateurs. Deuxièmement, je vais parler des lacunes en matière de protection de la vie privée des enfants.

Notre première préoccupation concerne le manque d'effet dissuasif du projet de loi C-27. Selon nous, le projet de loi comporte des lacunes qui pourraient entraver son application. D'abord, bien que le projet de loi comporte des sanctions administratives pécuniaires dont le montant est élevé, seuls certains manquements à la loi pourront mener à l'imposition de telles sanctions.

Ensuite, le Commissariat à la protection de la vie privée du Canada ne disposera pas du pouvoir d'imposer des sanctions directement; il ne pourra qu'en recommander l'imposition au nouveau tribunal de la protection des renseignements personnels et des données. Cette étape supplémentaire présage, à tout le moins, d'importants délais sur le plan de l'administration des sanctions imposées aux entreprises contrevenantes.

Par ailleurs, l'effet dissuasif d'une loi repose également sur la capacité des citoyens de l'invoquer devant les tribunaux civils. Or nous estimons que le nouveau droit privé d'action prévu à l'article 107 du projet de loi pose de sérieuses menaces à la capacité des consommateurs de s'adresser aux tribunaux pour faire valoir leurs droits. Le problème vient du fait que le nouveau droit privé d'action ne permet de poursuivre une entreprise que si des conditions préalables ont été remplies, en exigeant notamment que la situation ait d'abord été traitée par le Commissariat.

À notre avis, il est tout à fait envisageable que les grandes entreprises ciblées par des actions collectives invoqueront ces conditions d'ouverture très strictes dans le but de mettre en échec les procédures judiciaires engagées contre elles. Il s'ensuivra alors d'interminables débats devant les tribunaux, afin de déterminer la portée du droit privé d'action fédéral face à la compétence constitutionnelle des provinces en matière de droit civil.

En conséquence, nous invitons le gouvernement à clarifier que l'article 107 s'ajoute aux autres recours civils prévus en droit provincial, de façon à s'assurer qu'il ne fait pas obstruction aux poursuites civiles intentées en vertu du droit du Québec.

Je laisse maintenant la parole à ma collègue maître Levac.

Me Sara Eve Levac (avocate, Option consommateurs): Notre deuxième préoccupation concerne les lacunes en matière de protection de la vie privée des enfants. Ces lacunes subsistent malgré les amendements annoncés au début des consultations.

Bien que le projet de loi C-27 reconnaisse le caractère sensible des renseignements personnels des mineurs, nous estimons qu'il ne va pas suffisamment loin pour véritablement protéger la vie privée des enfants. Nous proposons de renforcer la protection accordée par ce projet de loi en y intégrant les meilleures pratiques reconnues en droit international.

D'abord, la loi doit offrir des protections plus solides aux enfants dans l'univers numérique, en les protégeant de l'exploitation commerciale de leurs renseignements personnels. Les applications Web que les enfants utilisent peuvent recueillir d'innombrables données sur eux. Ces données peuvent ensuite être utilisées pour faire du profilage ou pour cibler les enfants à des fins commerciales. Or rien dans le projet de loi C-27 n'interdit ces pratiques.

Ensuite, la loi devrait prévoir que les décisions concernant les renseignements personnels d'un enfant doivent être prises dans son intérêt supérieur. La notion de l'intérêt supérieur de l'enfant permet d'avoir une vision plus globale de la protection de la vie privée que la seule reconnaissance de la nature sensible de ses renseignements personnels. Elle permet notamment d'évaluer si l'utilisation de ses renseignements personnels par une entreprise favorise son développement global et si ses droits sont exercés à son bénéfice.

À titre d'exemple, il pourrait ne pas être dans l'intérêt de l'enfant de donner accès à ses renseignements personnels à ses parents ou tuteurs lorsque l'enfant subit de la maltraitance de leur part. Une analyse basée uniquement sur la nature sensible des renseignements personnels ne limiterait pas un tel accès.

C'est avec plaisir que nous allons répondre à vos questions.

● (1610)

Le président: Merci beaucoup.

Nous allons maintenant céder la parole à M. Mellouli, qui se joint à nous par vidéoconférence.

M. Sehl Mellouli (vice-recteur adjoint, Services à l'enseignement et à la formation tout au long de la vie, Université Laval): Merci beaucoup de l'invitation et de cette occasion de m'exprimer sur le projet de loi relatif à l'intelligence artificielle et son utilisation avec les données.

Je ne vais pas reprendre certains éléments que M. Gambs a soulevés tout à l'heure. Cependant, j'aimerais bien reprendre certains éléments du projet de loi qui, à mon avis, ne sont pas tout à fait clairs ou qui devraient être clarifiés, surtout lorsqu'on parle de résultats biaisés. C'est un des éléments qui m'a interpellé: qu'est-ce qu'un résultat biaisé et comment en est-on arrivé à un résultat biaisé?

L'intelligence artificielle ne donnera jamais un résultat vrai à cent pour cent. Elle se base toujours sur l'apprentissage, et c'est cet apprentissage qui fait qu'elle donne une recommandation ou une décision, ou qu'elle génère une nouvelle information, une nouvelle donnée.

Si une personne est visée par un résultat biaisé, est-ce que c'est la responsabilité de l'entreprise ou de l'organisation qui a créé ce biais? Est-ce un biais normal? Un système d'apprentissage automatique pourrait avoir un certain degré de succès, de 90 % ou de 97 %, par exemple. L'intelligence artificielle n'aura jamais une vérité à 100 %, aujourd'hui. Ce qui m'a interpellé, c'est vraiment la définition de ce qu'est un résultat biaisé.

Je veux attirer l'attention sur l'apprentissage et les données. On fait de l'apprentissage au moyen de données, mais l'entreprise a toutes les capacités pour fragmenter ces dernières entre différentes structures organisationnelles. On peut même transformer une donnée, une information. Le projet de loi soulève le fait qu'il faudrait avoir des informations sur la façon dont on gère des données et sur la manière de les anonymiser.

Il y a également des données anonymes ou dépersonnalisées, comme on l'avait soulevé. Or, comment peut-on nous assurer que l'entreprise n'a pas fragmenté ces données de manière à ce qu'elle puisse les retracer? La vérification ne permet pas de retrouver cette information. C'est un élément très important à considérer dans l'applicabilité. Je peux vous présenter tout un manuel qui démontre que j'ai bien anonymisé mes données et comment je les gère, mais on n'a aucune certitude, sur le plan de l'apprentissage, que ce sont ces données anonymes que j'ai utilisées. Même si on peut revenir en arrière pour connaître un peu les données qui ont été utilisées, comme l'avait mentionné M. Gambs, cela reste toujours une tâche difficile et assez complexe à réaliser.

Le dernier point que j'aimerais aborder, c'est quand on parle d'un système à incidence élevée, comme vous le définissez. On peut dire que c'est la perte de confidentialité, d'intégrité ou de disponibilité de données qui peut avoir des conséquences graves ou catastrophiques sur certaines personnes ou certaines entités. Si l'entreprise définit son système avec un taux de réussite de 97 %, cela signifie qu'il aura toujours un taux d'échec de 3 %.

Alors, le cas qu'on examine tombe-t-il dans ces 3 %? Comment est-on en mesure de vérifier qu'on est dans une de ces situations où on crée un préjudice ou un biais à une personne bien particulière, malgré le fait que l'apprentissage a été fait correctement?

Il y a donc plusieurs défis relativement aux données dont on se sert: comment s'assurer qu'elles sont anonymes, qu'elles ne sont pas fragmentées ou modifiées? L'entreprise aura toute la capacité de retracer ces données, mais un vérificateur voulant faire la même chose trouvera la tâche très compliquée et très complexe.

Même si on a très bien fait les choses, qu'est-ce qu'un biais et qu'est-ce qu'un résultat biaisé? Comment s'assurer que les résultats biaisés, qui ne fonctionnent pas et qui créent un préjudice à une personne, ne tombent pas dans les 3 % d'échec sur le plan de l'apprentissage?

Merci beaucoup. Je reste disponible pour répondre à vos questions, en anglais et en français.

● (1615)

Le président: Merci beaucoup, monsieur Mellouli.

Pour ouvrir la discussion, je vais passer la parole à M. Généreux pour six minutes.

M. Bernard Généreux (Montmagny—L'Islet—Kamouraska—Rivière-du-Loup, PCC): Merci, monsieur le président.

Je remercie tous les témoins d'être ici aujourd'hui.

Monsieur Mellouli, je vais commencer par vous, je pense que c'est moi qui vous ai invité par l'intermédiaire de votre présidente. Êtes-vous de l'Université de Montréal ou de l'Université Laval?

M. Sehl Mellouli: Je suis de l'Université Laval.

M. Bernard Généreux: Le hasard a voulu que je j'aille visiter l'Université Laval au mois de septembre. Je me suis alors rendu compte que cette université était bien placée pour faire de la recherche sur l'intelligence artificielle.

J'imagine que vous êtes vous-même chercheur. En tout cas, vous semblez bien connaître le sujet.

Dans les propos que vous venez de tenir, vous avez parlé de résultats biaisés, de responsabilisation de l'entreprise et de fragmentation des données. Quand vous parlez d'apprentissage, dans le langage de l'intelligence artificielle, quelle différence faites-vous entre l'apprentissage et l'anonymisation? Je veux être sûr de bien comprendre.

M. Sehl Mellouli: Je vais répondre à votre question avec plaisir. Je vais m'assurer que j'ai bien compris.

Parlons des données anonymes. Supposons que, pour l'apprentissage de la machine, je n'utilise pas le nom d'une personne, ni sa race ou son origine, ni son numéro d'assurance sociale...

M. Bernard Généreux: Excusez-moi de vous interrompre, mais pourriez-vous me donner la définition de l'apprentissage?

M. Sehl Mellouli: L'apprentissage, c'est quand nous fournissons un certain nombre de données à une machine. Cet apprentissage peut être supervisé ou non et je vais me limiter à ces deux types d'apprentissage.

Dans le cas d'un apprentissage supervisé, on fournit à la machine un ensemble de données qu'on va identifier. Par exemple, on lui dit que Sehl Mellouli est professeur. On peut ajouter qu'il appartient à une minorité ethnique ou qu'il a un excellent comportement, un comportement moyen ou un mauvais comportement, par exemple. Ainsi, on fait en sorte que le système apprenne à partir de ces données qu'on aura identifiées.

Par conséquent, le système pourra utiliser des données personnelles sur Sehl Mellouli pour faire de l'apprentissage en identifiant les données qui disent ce qu'il est comme personne, sans anonymiser ces dernières. À partir de ces données personnelles, le système pourra apprendre.

Si les données sont anonymes, c'est tant mieux. Si elles ne le sont pas, le système apprendra à partir de données qui ne sont pas anonymes et pourra profiler Sehl Mellouli en fonction d'un contexte qu'il choisira, comme son origine, son accent ou ce qu'il est comme personne.

M. Bernard Généreux: Cela explique la possibilité du pourcentage d'erreur de 3 %. Vous faites référence à ces 3 % de risque. Vous avez parlé de résultats potentiellement biaisés. Est-ce bien cela?

M. Sehl Mellouli: C'est cela.

Je dis toujours à mes étudiants que, si leur système leur donne des résultats qui sont bons à 100 %, il y a un problème. C'est un programme informatique qui apprend. Quand on apprend à partir de centaines de milliers de données, on n'a aucune certitude que toutes les données servant à l'apprentissage sont bonnes. Les systèmes ont toujours des degrés de réussite, qui servent à évaluer leur capacité.

Prenons l'exemple de ChatGPT. Aujourd'hui, il peut vous donner la bonne réponse à une question, mais, parfois, il peut aussi vous donner la mauvaise.

● (1620)

M. Bernard Généreux: En effet, nous avons déjà vu cela à plusieurs reprises.

Par conséquent, les degrés de réussite et d'erreur de 97 % et de 3 % sont-ils des pourcentages standard de l'industrie, ou représentent-ils un objectif que vous visez vous-même?

M. Sehl Mellouli: Cela dépend. Ce ne sont pas des critères de l'industrie et M. Gambs pourra me corriger si je me trompe.

Les taux de réussite permettent d'évaluer les systèmes. Si on est en train de construire un nouveau système, on compare parfois son taux de réussite à celui d'autres systèmes ou à d'autres algorithmes. On essaie de créer le meilleur système d'apprentissage possible. Parfois, on peut en trouver un qui donne un taux de réussite de 90 %, comparativement à d'autres pour lesquels il est de 80 %.

Certains chercheurs travaillent à améliorer les capacités de ces systèmes d'apprentissage afin de les augmenter ou d'accroître le taux de succès des prédictions quant aux résultats obtenus.

M. Bernard Généreux: L'autre élément dont vous avez parlé, ce sont les systèmes à incidence élevée, dont les résultats découlant du taux de réussite du système et de la collecte des données utilisées peuvent avoir de graves répercussions. Est-ce que vous voyez là un risque? En ce qui concerne la loi proposée ou la description de la loi, quels changements proposeriez-vous?

M. Sehl Mellouli: Je ne peux pas proposer ce qui pourrait être changé. Je dis qu'il faudrait vraiment comparer la capacité du système à bien se comporter et le risque qu'il commette des erreurs. Aujourd'hui, avec les systèmes d'intelligence artificielle disponibles, je pense qu'il y a un droit à l'erreur qui devrait être considéré, parce que les systèmes, même s'ils ont un très haut degré de fiabilité, ne sont pas fiables à 100 %.

C'est pour cette raison que j'ai évoqué la perte de confidentialité et d'intégrité ou de disponibilité des données qui peuvent avoir des répercussions graves sur certaines personnes. Sur le nombre total de personnes visées par le système, combien ont été affectées? Si 80 % des gens sont gravement affectés, nous avons vraiment un système à incidence élevée et il faut intervenir. Par contre, si, sur 100 000 personnes, à peine 1 % des gens sont affectés, ce pourcentage se situe peut-être dans le taux d'apprentissage, qui permet au système de commettre des erreurs dans 1 % des cas.

M. Bernard Généreux: Donc, même l'intelligence artificielle n'est pas parfaite.

M. Sehl Mellouli: Non.

M. Bernard Généreux: Merci beaucoup.

Le président: Merci beaucoup, monsieur Mellouli.

Madame Lapointe, la parole est à vous.

Mme Viviane Lapointe (Sudbury, Lib.): Merci, monsieur le président.

Monsieur Letarte, à votre avis, la législation prévoit-elle des mesures appropriées pour permettre aux entreprises de s'y conformer?

M. Philippe Letarte: Je crois que c'est déjà un bon début pour les entreprises, et c'est d'ailleurs pour ça que je suis ici.

Je sais que le partage des données bancaires n'est pas nécessairement le sujet principal du projet de loi C-27, mais je trouve que ce projet de loi établit la base du cadre législatif promis dans la mise à jour économique de l'automne. C'est ce qui se rapproche le plus, en ce moment, de ce qui permet le partage et la portabilité des données.

Je crois aussi qu'il faudrait établir des modalités plus poussées et les insérer dans une section de la réglementation découlant du projet de loi C-27, ou encore dans un futur projet de loi visant directement un système bancaire ouvert.

Mme Viviane Lapointe: Merci.

Nous comprenons que si la législation sur la protection de la vie privée et sur l'intelligence artificielle n'est pas harmonisée à l'échelle mondiale, l'efficacité des règles et des lois sera compromise. Que pensez-vous de la manière dont les différentes autorités peuvent travailler ensemble à la mise en œuvre des normes?

M. Philippe Letarte: Posez-vous la question pour l'intelligence artificielle?

Mme Viviane Lapointe: Je m'intéresse à la protection de la vie privée et à l'intelligence artificielle.

M. Philippe Letarte: En fait, il est important de comprendre que le système bancaire axé sur le consommateur est pas mal présent à l'échelle mondiale. Le Canada est l'un des derniers pays où il n'y a pas de droit à la portabilité des données. Plusieurs pays qui sont très proches de nous au sein du Commonwealth, comme la Grande-Bretagne et l'Australie, ainsi que toute l'Union européenne et certains pays d'Asie ont un tel système, et on voit déjà à quel point l'interopérabilité est facile entre ces pays.

Je pense qu'il est temps pour le Canada d'atteindre cette modernité et d'offrir aux Canadiens le droit à la portabilité. Pour tout ce qui est de l'interopérabilité, je dirais donc que ce n'est pas très complexe. Les règles se ressemblent quand même.

Pour ce qui est de l'intelligence artificielle, je m'abstiendrai de commenter, parce que je ne suis pas expert en ce domaine. C'est un sujet extrêmement complexe. Je pense que tout le monde essaie de comprendre, y compris le président d'OpenAI, qui s'est fait mettre dehors avant d'être réembauché. Je m'abstiendrai donc de commenter ce sujet dans le contexte d'une législation de portée générale.

● (1625)

Mme Viviane Lapointe: Certains témoins ont souligné que les fenêtres surgissantes demandant le consentement qui sont présentes sur plusieurs sites et applications sont sans intérêt parce que les gens ne lisent pas le texte et cliquent sur « oui » pour continuer. Je le fais souvent moi-même.

Que pensez-vous du consentement éclairé, du droit à la vie privée et des responsabilités des organisations? La responsabilité du consentement éclairé devrait-elle incomber à l'organisation?

M. Philippe Letarte: Absolument. C'est pour cette raison que nous sommes très contents qu'on ait déposé le projet de loi C-27. Notre entreprise fonctionne en ce moment dans un système qui se trouve un peu dans une zone grise et qui n'est pas très légiféré. Cela fait très longtemps que nous demandons au gouvernement fédéral d'intervenir au nom du consommateur.

Vous faites référence à des fenêtres surgissantes. De notre côté, c'est beaucoup plus précis que cela et beaucoup plus réglementé. Si vous avez une application en ligne pour faire votre comptabilité ou pour gérer votre retraite ou vos placements, vous allez avoir à donner un consentement. Nous voulons que ce consentement soit protégé de façon adéquate et qu'il soit renouvelé, également.

Bien que notre cas soit un peu différent de tout ce qui est fichiers témoins et fenêtres surgissantes, nous demandons l'ajout d'une réglementation qui donne au consommateur le pouvoir de consentir au partage de ses données et qui lui garantit une protection adéquate. Soyons honnêtes, il y a quand même deux sujets qui sont tabous dans la société, outre la religion: nos finances et nos données personnelles. Ici, nous combinons les deux.

En résumé, il est donc important d'avoir une protection adéquate et, pour nous, il est tout aussi important qu'il y ait un consentement à donner. Pour tous les systèmes et les compétences que j'ai mentionnés plus tôt, la responsabilité du consentement revient aux entreprises.

Nous sommes très contents de la teneur du projet de loi, parce qu'on créera un cadre législatif qui est sûr, et donc plus efficace pour le consommateur. Cela permettra également à notre entreprise de croître dans un environnement qui est sécuritaire et stable.

Mme Viviane Lapointe: Monsieur Plourde ou madame Levac, j'aimerais vous poser la même question.

Me Alexandre Plourde: Le consentement est effectivement l'une des méthodes de protection du consommateur. C'est la méthode qui a été choisie principalement dans ce projet de loi. On aurait pu choisir autre chose, on aurait pu ajouter d'autres normes de protection, mais nous avons encore ici un texte de loi qui tourne autour du consentement. Ce dernier peut être une méthode qui fonctionne pour protéger les consommateurs dans l'environnement numérique et leur permettre de contrôler leurs données, pourvu que ce consentement soit effectif et qu'il puisse être réellement utile au consommateur.

Le projet de loi C-27 pose problème quant aux exceptions liées au consentement. Ces exceptions nous paraissent trop larges. L'exception qui nous préoccupe le plus est celle prévue à l'article 18, en lien avec tout ce qui est fin légitime et utilisation pour des activités d'affaires. C'est une exception qui nous semble trop large. Nous comprenons mal comment elle s'arrime avec le consentement implicite qui existe déjà. Nous proposons donc de retirer l'article 18, qui donnerait trop de latitude aux entreprises pour utiliser les données des consommateurs sans leur consentement.

Ensuite, vous avez parlé au début de votre question des fenêtres surgissantes. J'ai l'impression que vous faites référence à la notion de fatigue du consentement, qui survient à force de se faire toujours demander son consentement. Les gens sont bombardés de demandes ou de requêtes de consentement, et nous sommes sensibles à cette préoccupation concernant la fatigue du consentement.

Nous pensons que les entreprises devraient faire preuve de créativité. Le projet de loi pourrait aussi offrir des solutions efficaces qui permettent au consommateur de refuser en bloc d'être pisté en ligne. Quand on va sur différents sites Internet, sur des applications mobiles, sur des plateformes d'entreprises technologiques, notre vie privée et nos données sont captées en permanence pour être utilisées à des fins commerciales et autres par les entreprises. La méthode actuelle est de nous faire consentir à la pièce auprès de chaque site Web où apparaissent des fenêtres surgissantes, auprès de chaque entreprise.

Dans notre mémoire, nous proposons comme solution de créer plutôt des mécanismes qui permettraient à un consommateur de refuser en bloc de transmettre ses données de navigation ou d'autres données personnelles à toutes les entreprises avec lesquelles il fait affaire. C'est ce que nous appelons le mécanisme « ne pas suivre », qui existe déjà dans les fureteurs Web, mais qui n'est pas reconnu par les entreprises. Nous proposons que les entreprises soient obligées de reconnaître ce type de signal ou ce type de paramètre qui, d'un seul coup, permet à quelqu'un de refuser en bloc de fournir ses données personnelles. À ce moment-là, il n'y aura plus cette fatigue de consentement qu'on déplore.

● (1630)

Mme Viviane Lapointe: Merci.

Le président: Merci, madame Lapointe.

Il est rare que je fasse cela mais, si vous me le permettez, j'aimerais poser une question au témoin.

Monsieur Plourde, ce que vous venez de mentionner est très intéressant, à mon avis. Il y a des fureteurs en ligne comme DuckDuckGo qui permettent de refuser en bloc de fournir ses données personnelles, d'après ce que je comprends. Avez-vous une proposition précise d'amendement à un article du projet de loi à cet effet?

Me Alexandre Plourde: C'est une très bonne question. Cela pourrait être formulé à l'article où l'on énonce le consentement. Je n'ai pas en tête l'article exact, mais il y en a un qui prévoit que le consentement doit être implicite. On pourrait y insérer la possibilité pour le consommateur d'émettre un refus général de partager ses données, qui pourrait cibler certains types de données, par exemple, les données de navigation d'une personne ou les données d'utilisation de ses appareils numériques.

Un consommateur pourrait signifier son refus au moyen d'une interface ou d'une technologie quelconque, et ce refus devra être respecté par les entreprises. Techniquement, ce ne serait peut-être pas si difficile que cela à intégrer, parce qu'il existe déjà des paramètres de ce genre dans les fureteurs Web. Il s'agirait simplement de contraindre les entreprises à respecter le souhait du consommateur.

Le président: Si d'aventure vous aviez une proposition à nous soumettre, sentez-vous libre de le faire. Il reste encore du temps à notre étude. Cela nous fera plaisir de la considérer.

Moi aussi, je suis assez préoccupé par cette fatigue du consentement. J'ai parfois l'impression qu'on donne au consentement beaucoup d'importance. Je comprends pourquoi, mais il ne faudrait pas que cela ait une valeur limitée, comme le mentionnait Mme Lapointe, compte tenu du fait que personne ne lit les conditions. Souvent, on clique sur « Accepter » simplement pour accélérer le processus.

Monsieur Letarte, j'aimerais une dernière clarification: pour un consommateur de produits financiers, que veut dire, concrètement, la portabilité des données?

M. Philippe Letarte: Techniquement, en ce moment, au Canada, personne n'est propriétaire de ses données financières. On fait affaire avec une banque, on a un compte en ligne, on a probablement un compte-chèques et une hypothèque. Tout cela crée des données, y compris des données de base comme son adresse. Présentement, si quelqu'un veut un autre produit financier offert par une autre banque, sa banque peut refuser de communiquer ses données financières parce qu'il n'en est pas propriétaire.

Je vais faire un bref rappel historique du droit à la portabilité de données. Il ne s'agit pas d'une invention du secteur privé ou des compagnies technologiques. En fait, cela résulte d'une proposition législative faite au Royaume-Uni par la Competition & Markets Authority à la suite de la crise financière de 2009. Elle trouvait que les banques n'avaient pas mis en avant le droit des consommateurs, et que c'était un secteur où régnait une concentration excessive.

Son rapport, intitulé « Making banks work harder for you », mentionnait que la solution était le droit à la portabilité. Autrement dit, il fallait redonner au consommateur le droit de prendre ses données financières et de faire affaire avec l'institution de son choix, ce qui lui permettrait entre autres de comparer les taux d'hypothèque, les différents placements ainsi que les différents pourcentages et taux d'intérêt en vigueur pour les comptes-chèques et autres.

Cette politique a fait boule de neige. Comme je l'ai dit, la plupart des pays de l'Organisation de coopération et de développement économiques et, je pense, les 70 plus grandes économies reconnaissent le droit à la portabilité des données. L'Australie a été un petit peu plus ambitieuse: elle utilise la portabilité des données dans d'autres secteurs, comme les télécommunications et l'énergie.

Est-ce que cela répond à votre question?

Le président: Oui, merci beaucoup.

Nous revenons à la programmation régulière.

Monsieur Lemire, vous avez la parole.

M. Sébastien Lemire (Abitibi—Témiscamingue, BQ): Merci, monsieur le président.

Monsieur Gambs, si vous me le permettez, je voudrais profiter de votre expertise.

Hier, Radio-Canada a révélé que des ministères et des agences gouvernementales utilisaient du matériel d'espionnage initialement associé au milieu du renseignement pour récupérer et analyser des données, y compris celles cryptées et protégées par des mots de passe. De plus, l'utilisation de ces outils de surveillance n'aurait pas fait l'objet d'une évaluation des risques pour la vie privée, malgré une directive fédérale exigeant cette démarche.

Dans le contexte, considérant l'inclusion du secteur public dans le projet de loi C-27, quelles sont vos préoccupations principales concernant l'utilisation de ce type d'outils de surveillance par des entités gouvernementales et, plus particulièrement, l'absence d'évaluation des risques pour la vie privée?

● (1635)

M. Sébastien Gambs: Je vais être bref. Les risques sont énormes. Déjà, la raison pour laquelle on utilise ces outils me semble discutable.

Pour l'instant, d'après les informations qui sont sorties, la raison pour laquelle ces outils ont été utilisés n'est pas très claire. Par ailleurs, je pense qu'un gouvernement devrait être irréprochable, puisque le projet de loi demande à des entreprises d'effectuer des analyses d'impact relatives à la vie privée et de démontrer que leurs pratiques sont exemplaires.

Je n'ai pas besoin de donner des détails, mais ces outils sont utilisés pour surveiller des activistes et des journalistes. Il y a des gens qui sont allés en prison ou qui sont morts à cause de ce type d'outils, qui sont aussi utilisés dans certains pays totalitaires ou des pays qui surveillent les opposants politiques. Je pense qu'il faut assurément mener une analyse et une enquête approfondies sur ces révélations.

M. Sébastien Lemire: Est-il nécessaire d'étendre les dispositions du projet de loi au secteur privé pour garantir une protection complète des données des Québécois ou des Canadiens? Parallèlement à cela, comment le projet de loi C-27 pourrait-il être adapté ou renforcé pour réglementer de manière adéquate l'utilisation de tels outils dans le secteur public?

M. Sébastien Gambs: Selon moi, on pourrait ajouter un article précisant que ces outils de surveillance ne servent assurément pas à une collecte de données pour laquelle on a obtenu le consentement des personnes visées. Cet article de loi devrait porter précisément sur l'encadrement de ces outils de surveillance et permettre de s'assurer que l'utilisation de ce genre d'outils est encadrée par d'importants garde-fous.

J'imagine qu'il pourrait y avoir des exceptions strictes en matière de sécurité nationale. Or, selon ce que j'ai compris des révélations, plusieurs ministères utilisent ces outils dans des contextes qui n'ont rien à voir avec la sécurité nationale. À mon avis, il est donc nécessaire d'ajouter un article de loi précis qui encadrerait les possibilités d'utilisation et imposerait des garde-fous, en plus d'un contrôle judiciaire important.

M. Sébastien Lemire: Étant donné l'émergence de la technologie quantique dans les années à venir et le fait qu'elle sera couverte par le projet de loi, je crois que des garanties ou des mécanismes de surveillance sont nécessaires. Quelles garanties ou quels mécanismes de surveillances pourraient protéger efficacement l'information et les données des Québécois et des Canadiens?

M. Sébastien Gambs: Le domaine quantique aura une incidence sur beaucoup d'aspects de la sécurité des communications, pas juste sur les outils de surveillance de données.

Je pense que les normes de sécurité qui sont élaborées par le National Institute of Standards and Technology aux États-Unis et qui vont s'appliquer à Internet affichent déjà une volonté d'offrir des outils de sécurité permettant de résister aux attaques quantiques.

Je ne sais pas s'il faudrait que le projet de loi C-27 fasse mention de la résistance postquantique. Outre les outils de surveillance de données, cela peut concerner les données personnelles ou la sécurité des données en général.

M. Sébastien Lemire: Maître Levac ou maître Plourde, le projet de loi C-27, qui remplacera la Loi sur la protection des renseignements personnels et les documents électroniques, accorde aux consommateurs un nouveau droit à des explications sur l'utilisation d'un système décisionnel automatisé pour effectuer des prédictions, émettre des recommandations ou prendre des décisions importantes les concernant, même lorsque les données utilisées ont été dépersonnalisées.

Cependant, à la différence de la loi 25 au Québec, le projet de loi C-27 ne prévoit aucune disposition permettant à quelqu'un de s'opposer à l'utilisation d'un système décisionnel automatisé ou de faire réviser une décision prise par un tel système. Selon vous, quelles seraient les répercussions potentielles pour les consommateurs de l'absence de telles dispositions dans le projet de loi C-27?

Me Sara Eve Levac: En ce moment, le projet de loi C-27 permet d'obtenir sur demande des explications au sujet de décisions automatisées. Pour notre part, nous proposons d'aller plus loin, un peu comme vous l'expliquiez avec l'exemple du Québec.

Premièrement, il peut être difficile pour un consommateur de savoir si une décision le concernant a été prise de façon automatisée. Par exemple, lorsque quelqu'un se fait refuser une demande de carte de crédit, on ne lui fournit pas d'explications qui lui permettent de savoir que la décision le concernant a peut-être été prise de façon automatisée. Par conséquent, nous recommanderions que le projet de loi C-27 prévoie l'obligation d'informer le consommateur qu'une décision le concernant a été prise de façon automatisée.

Par la suite, nous pourrions demander que le projet de loi C-27 prévoie que des explications soient fournies au sujet de cette décision. Une étape supplémentaire serait de prévoir également la possibilité de faire réviser par une personne une décision prise par un outil automatisé, un peu comme c'est possible au Québec, afin que cette personne puisse faire des observations.

On a rapporté dans les médias des cas de personnes qui se sont fait refuser du crédit parce que les informations qui avaient été prises en compte pour rendre la décision comportaient des erreurs. La possibilité que de telles décisions puissent être révisées pourrait donc éviter des situations où les consommateurs se feraient refuser des contrats ou des prêts parce que les décisions les concernant étaient basées sur de mauvaises informations.

● (1640)

M. Sébastien Lemire: Je comprends donc que vous êtes en faveur d'intégrer au projet de loi C-27 des dispositions similaires à celles de la loi 25 du Québec pour le renforcer.

À qui pourrait-on faire appel pour contester une décision automatisée?

Me Sara Eve Levac: Un peu comme c'est le cas pour la loi 25, au Québec, nous proposons que le consommateur ayant fait l'objet d'une décision prise par un système automatisé puisse s'adresser à l'entreprise qui a utilisé ce système afin de faire valoir son point de vue et de demander à faire réviser par un humain de cette entreprise la décision le concernant.

M. Sébastien Lemire: Merci.

Le président: Merci, monsieur Lemire.

Monsieur Masse, vous avez la parole.

[*Traduction*]

M. Brian Masse (Windsor-Ouest, NPD): Merci, monsieur le président.

Merci à nos invités d'être ici, et merci à ceux qui sont en ligne.

Je vais commencer par ceux qui sont en ligne pour ensuite m'adresser à ceux qui sont ici.

Nous avons deux modèles pour ce qui est du poste de commissaire à la protection de la vie privée: soit que nous lui donnons les pouvoirs nécessaires, soit que nous nous tournons vers un tribunal, ce qui diminuerait les capacités du commissaire. Je suis curieux. Il faut presque en choisir un à ce stade-ci, car le tribunal serait nouveau.

Je pourrais peut-être commencer par nos invités en ligne — je ne vois pas leur nom maintenant, monsieur le président, et vous pouvez peut-être donc choisir — et je vais ensuite passer aux témoins présents ici pour leur demander ce qu'ils feraient à notre place.

Nous allons commencer par M. Gambs, puis nous poursuivrons.

Si vous deviez faire un choix, quel modèle choisiriez-vous?

M. Sébastien Gambs: Je pense que je donnerais des pouvoirs au commissaire à la protection de la vie privée, plus particulièrement, car vous avez également besoin de renforcer l'expertise concernant l'explicabilité et aussi l'équité, et j'essaierais donc essentiellement de mobiliser l'expertise en matière de protection des renseignements personnels et d'ajouter à cela une expertise concernant d'autres questions d'éthique. Je pense que pouvoir analyser toutes ces sujets semble être la meilleure idée.

M. Brian Masse: Allez-y, monsieur Mellouli.

[*Français*]

M. Sehl Mellouli: Permettez-moi de vous répondre en français, dans le même sens que M. Gambs.

Il est important d'avoir la capacité de contrôler davantage l'utilisation de données personnelles dans les systèmes d'intelligence artificielle. À mon avis, au lieu de se pencher sur les systèmes d'apprentissage de l'intelligence artificielle, et il y en a plusieurs, le seul processus qu'il serait important d'examiner davantage, c'est la donnée sur laquelle nous allons apprendre. Il est là, le défi.

Comment aider le commissaire à s'assurer qu'on a utilisé la bonne donnée pour apprendre? C'est ma seule inquiétude. Je le dis et je le répète, parce que ces systèmes sont des « boîtes noires » et que ce n'est pas facile, quand il est question de plusieurs, voire de centaines de milliers de données d'apprentissage, de récupérer celles qui ont servi à l'apprentissage.

Quel mécanisme de contrôle peut-on apporter? À mon avis, je pense que cet aspect mérite plus de réflexion, mais je n'ai malheureusement vraiment pas de solution à proposer aujourd'hui.

[*Traduction*]

M. Brian Masse: Merci.

Nous allons passer aux témoins présents dans la salle.

[*Français*]

Me Alexandre Plourde: Si je comprends bien votre question, vous vous interrogez sur le modèle du tribunal de la protection des renseignements personnels et des données proposé dans le projet de loi. Est-ce exact?

[*Traduction*]

M. Brian Masse: Eh bien, oui. Le commissaire à la protection de la vie privée a-t-il un tribunal qui décidera des sanctions et du reste ou doit-on lui donner le pouvoir d'exercer ces fonctions? Si nous créons le tribunal, il pourra imposer des sanctions, corriger des comportements et ainsi de suite, plutôt que de donner ces pouvoirs au commissaire.

● (1645)

[*Français*]

Me Alexandre Plourde: En fait, c'est une des difficultés qu'Option consommateurs a soulevées dans son mémoire. Il y a quand même de bons aspects au projet de loi C-27, puisqu'on donne un pouvoir d'ordonnance au Commissariat à la protection de la vie privée du Canada et que le projet de loi prévoit des sanctions administratives pécuniaires pouvant atteindre 10 millions de dollars ou 3 % du chiffre d'affaires. C'est intéressant.

Par contre, ce système punitif a effectivement des lacunes. Le Commissariat aura seulement le pouvoir de recommander ces sanctions administratives pécuniaires, que seul le tribunal spécialisé pourra imposer par la suite. Ce processus nous semble trop long et superflu. En outre, ces sanctions administratives pécuniaires ne couvrent pas tous les manquements à la loi. Nous considérons pour notre part que n'importe quel manquement à la loi devrait pouvoir faire l'objet d'une sanction administrative pécuniaire, imposée directement par le Commissariat.

Nous ne voyons aucune raison de retarder l'imposition d'une telle sanction en transmettant le dossier à un tribunal. Si le Commissariat choisit d'imposer une sanction administrative pécuniaire, c'est parce qu'il a fait de nombreuses démarches concernant cette entreprise, qu'il l'a avertie plusieurs fois et qu'il s'agit d'une décision mûrement réfléchie. Par conséquent, je ne vois pas pourquoi on ralentirait le processus.

Au Québec, la Commission d'accès à l'information du Québec peut directement imposer des sanctions administratives pécuniaires. Récemment, un nouveau projet de loi au Québec permet à l'Office de la protection du consommateur d'imposer directement lui aussi des sanctions administratives pécuniaires. On ne voit pas pourquoi le fédéral ne pourrait pas faire la même chose qu'au Québec.

[*Traduction*]

M. Brian Masse: Merci.

Monsieur Letarte, voulez-vous intervenir?

M. Philippe Letarte: Nous n'avons pas d'opinion là-dessus.

Cela dit, dans l'énoncé économique de l'automne, il est écrit que pour renforcer les services bancaires pour les gens, il faut une sorte d'entité gouvernementale. Est-ce le Commissariat à la protection de la vie privée? Dans l'affirmative, il devrait avoir des ressources supplémentaires ou plus de personnel à cette fin, mais nous ne sommes pas pour ou contre la création d'un tribunal ou l'octroi de ces pouvoirs au commissaire.

M. Brian Masse: Merci, monsieur le président.

[*Français*]

Le président: Merci, monsieur Masse.

[*Traduction*]

Monsieur Williams, vous avez la parole.

M. Ryan Williams (Baie de Quinte, PCC): Merci, monsieur le président.

Merci à tous nos témoins.

Monsieur Letarte, je suis heureux de vous voir ici aujourd'hui. J'ai déposé un projet de loi il y a un mois au Parlement pour faire avancer le dossier des services bancaires axés sur les consommateurs — le système bancaire ouvert. À vrai dire, je vais parier environ 50 $ avec mon collègue d'Abitibi-Témiscamingue à propos de ce que nous allons voir en premier: l'étape de la troisième lecture pour le projet de loi C-27 ou un système bancaire ouvert. Je ne suis pas certain. Je pense que je pourrais gagner un peu d'argent à ses dépens.

Des voix: Ha, ha!

M. Ryan Williams: La prémisse dans ce cas-ci, c'est que ces mesures semblent bien progresser, parallèlement. Le projet de loi C-27 porte sur les données. Pour les personnes qui nous écoutent à la maison, l'idée des services bancaires axés sur les consommateurs consiste vraiment à obliger les banques à communiquer vos données personnelles à d'autres entités qui peuvent vous offrir ces services, ce qui permet... Au Royaume-Uni, où nous l'avons vu avec 4 000 entreprises, les gens économisent 12 milliards de livres sterling par année et les entreprises, 8 milliards. C'est vraiment formidable.

Ma première question pour vous alors que nous cherchons le moyen d'avoir des services bancaires axés sur les consommateurs est la suivante: ces services, c'est-à-dire le système bancaire ouvert, peuvent-il exister actuellement sans cette mesure législative?

M. Philippe Letarte: Je dirai dès le départ que oui, mais je pense que le projet de loi C-27 est une très bonne première étape pour avoir ces règlements. Il jette vraiment les bases sur lesquelles nous pouvons nous appuyer et il uniformise les règles du jeu à propos de la modernisation et de la protection des renseignements personnels au pays, ce qui est attendu depuis très longtemps.

Pour ce qui est de mes propres intérêts, j'espère que nous aurons un système bancaire ouvert plus tôt que tard. Je pense vraiment que c'est une sorte d'urgence en ce moment, pour plusieurs raisons.

Tout d'abord, nous savons que le coût de la vie pose problème au Canada. Nous savons aussi que nous devons donner plus de ressources aux Canadiens et que nous sommes moins concurrentiels à l'échelle internationale. Par conséquent, peu importe le moyen utilisé, ce qui compte, c'est que ce soit fait rapidement, mais le projet de loi C-27 est une bonne base sur laquelle nous pouvons nous appuyer.

M. Ryan Williams: Je vois. Je vais mettre l'accent sur la façon dont ce secteur peut prospérer grâce à cette mesure législative.

Vous aviez trois amendements, et je veux mettre l'accent là-dessus. J'aimerais que vous parliez un peu plus de ce qu'il faut exactement pour chaque amendement. Si vous avez une formulation que vous aimeriez voir dans un amendement, vous pouvez la transmettre à la greffière — c'est probablement la meilleure façon — pour que nous l'ayons.

Commençons par les intérêts légitimes.

Vous avez parlé des paragraphes 18(3) et 18(4) qui sont proposés. Parlez-en un peu plus, et si vous voulez parler des trois amendements, il est alors question de l'article 72 puis du paragraphe 29(1). Donnez-nous un peu plus de détails qui expliquent pourquoi ces amendements sont nécessaires pour avoir un système bancaire ouvert.

M. Philippe Letarte: Bien sûr.

Je vais commencer par l'article 18 proposé sur les intérêts légitimes. Merci beaucoup, monsieur Williams, d'avoir déposé ce projet de loi. Il interpelle vraiment les gens, et je pense qu'il fait vraiment valoir l'idée.

Comme vous le savez, le but d'un système bancaire ouvert est d'avoir le consentement des gens et de la transparence. Si nous voulons accorder des exceptions... Je ne suis pas contre l'article 18 à proprement parler; je pense juste qu'il devrait y avoir au moins certains critères ou une définition du mot « exception », car dans un système bancaire ouvert, il n'est pas question de l'utilisation de données secondaires. Dans ce cas, des entreprises pourraient dire qu'elles ont des intérêts d'affaires légitimes et miner ainsi la confiance des consommateurs, car lorsqu'on accepte la communication de nos données, on ne le fait pas nécessairement pour des utilisations secondaires.

À cette fin, je crois que nous devrions avoir des critères très clairs pour les exceptions et dire en quoi consiste un intérêt légitime, car, comme je l'ai dit, si les gens ne font pas confiance au système bancaire ouvert, il ne donnera pas de bons résultats.

Nous pouvons examiner aussi d'autres lois. En Europe, on indique explicitement en quoi consiste un intérêt légitime, et c'est la même chose en Australie. Il y a un libellé sur lequel on peut s'appuyer, mais je pense que c'est vraiment une question de confiance, et nous ne devrions pas laisser les entreprises décider du bien-fondé des utilisations secondaires.

Quant à l'article 72, il est proposé parce que, compte tenu de ce qui a été annoncé dans l'énoncé économique de l'automne, il est important — et vous l'avez dit — que le système bancaire soit assujetti à une réglementation financière. Personne ne devrait pouvoir échapper ou renoncer à ses responsabilités dans le cadre du régime. Les gens doivent participer. C'est un peu l'effet des réseaux en affaires. Nous devons faire très attention au libellé que nous choisissons pour éviter d'avoir un cadre concurrentiel et pour qu'aucun intervenant ne puisse échapper à ses responsabilités.

C'est la raison pour laquelle je reviens à la notion simple de tout à l'heure: il n'est pas question de savoir si cela se fera, mais plutôt quand cela se fera. Lorsqu'on adhère à un cadre en tant que participant, il faut suivre les mêmes règles que les autres. C'est un peu le concept. Comme je l'ai dit, chaque pays qui possède un système bancaire ouvert qui est efficace impose des règles rigoureuses aux banques.

Enfin, le dernier amendement dont vous vouliez que je parle portait, je crois, sur l'intérêt manifeste.

● (1650)

M. Ryan Williams: C'est l'article 29 proposé.

M. Philippe Letarte: C'est également intéressant, car comme pour l'article 18 proposé, nous ne sommes pas contre à proprement parler, mais nous devrions redéfinir le consommateur.

Par exemple, si mon entreprise offre une promotion qui donnera un meilleur taux d'intérêt à un consommateur, dois-je obtenir son consentement pour lui permettre de profiter de l'offre. C'est techniquement dans son intérêt, car le taux d'intérêt pourrait être moins élevé, mais en même temps, c'est avantageux pour mon entreprise. Nous devrions donc préciser l'exception dans les critères. Nous voyons aussi au Royaume-Uni des cas d'utilisation qui sont clairement définis.

Par exemple, il y a le cas des Canadiens les plus vulnérables. Si vous prenez soin de l'un de vos parents aînés, il n'est peut-être pas capable de donner son consentement pour la communication de ses données, mais vous pouvez peut-être travailler avec un organisme sans but lucratif qui vous indiquera clairement si cette personne est victime de fraude ou si elle a des dépenses inhabituelles. Si elle ne peut pas donner son consentement à cause d'une maladie mentale — l'Alzheimer ou autre —, cette exception devrait être clairement définie dans les critères.

Encore une fois, nous ne sommes pas contre à proprement parler, mais nous devrions être prudents à propos des sortes d'exceptions que nous accordons, car la portabilité des données repose sur le consentement.

[*Français*]

Le président: Merci beaucoup.

Monsieur Gaheer, vous avez la parole.

[*Traduction*]

M. Iqwinder Gaheer (Mississauga—Malton, Lib.): Merci, monsieur le président. Je remercie également les témoins de leur comparution devant le Comité.

Mes questions sont pour M. Letarte.

Je veux mettre l'accent sur l'article 9 proposé de la loi, qui, comme nous le savons, exige que chaque organisation assujettie à la loi élabore et tienne à jour « un programme de gestion de la protection des renseignements personnels qui comprend les politiques, les pratiques et les procédures » pour remplir ses obligations en vertu de la loi.

Votre organisation a-t-elle déjà un programme de gestion en place?

M. Philippe Letarte: Non. Nous ne sommes pas face aux clients. Je pense qu'il est important de le dire. Nous sommes essentiellement un agrégateur de données. Nous créons les réseaux au pays pour des applications comme Questrade ou Wealthsimple, pour les banques.

C'est une chose que chaque entreprise devrait avoir selon nous. C'est quelque chose que nous voyons, encore une fois, dans tous les autres pays qui ont un système bancaire ouvert. Il doit y avoir un recours évident ou une section évidente sur un site Web ou une application qui présente les recours et les programmes en place pour protéger le consommateur.

Lorsqu'un consommateur estime avoir été victime d'un acte criminel et qu'il veut être indemnisé, il peut consulter ces politiques en temps réel. C'est aussi une façon de désengorger le tribunal ou l'entité responsable en faisant en sorte que la personne vérifie d'abord avec l'entreprise.

En tant qu'entreprise de protection des renseignements personnels, nous offrons ce recours, mais il n'est pas aussi détaillé qu'il le devrait. Nous encourageons l'ajout de l'article 9. Nous croyons que chaque entreprise qui participe dans cet écosystème devrait avoir une sorte de recours en place.

● (1655)

M. Iqwinder Gaheer: Pensez-vous que cet article sera trop coûteux pour les organisations?

M. Philippe Letarte: Je ne pense pas. Je crois que c'est approprié.

M. Iqwinder Gaheer: Combien de temps pensez-vous qu'il faudra pour que les entreprises canadiennes respectent ce nouveau cadre réglementaire et pour qu'elles s'y adaptent?

M. Philippe Letarte: Cela dépend. Nous observons une croissance étonnante au Royaume-Uni. La progression sur 12 mois est de 80 %. C'est une politique publique très réussie.

Comme vous le savez, le système bancaire ouvert fait de plus en plus parler de lui. Les gens en parlent parce qu'ils le connaissent. De plus, une association dont nous sommes membres, Fintechs, a lancé une campagne à laquelle de nombreux Canadiens ont participé. Ils réclament des services bancaires ouverts et en ont besoin. Je pense que l'adoption par les Canadiens sera très rapide. C'est l'une des raisons pour lesquelles nous ne devons pas tarder dans ce domaine. Il y a manifestement un besoin au sein de la population.

Je crois vraiment que d'ici quatre ou cinq ans, l'adoption sera tout à fait généralisée.

M. Iqwinder Gaheer: Ma prochaine question est destinée à tous les témoins qui veulent y répondre.

Nous avons déjà entendu des témoignages là-dessus. En fait, un nouveau tribunal est constitué. C'est ce tribunal, et non plus le Commissaire à la protection de la vie privée, qui imposera directement les amendes.

J'aimerais savoir ce qu'en pensent les témoins.

[*Français*]

Me Alexandre Plourde: Notre point de vue sur le nouveau tribunal de la protection des renseignements personnels et des données est quand même mitigé. D'une part, il pourrait être intéressant d'avoir un tribunal spécialisé et possédant une expertise dans ce domaine pour rendre des décisions en matière de vie privée. Par contre, nous avons des réserves concernant le fait que ce tribunal aura beaucoup de pouvoirs pour ce qui est de revoir ou d'annuler les décisions du Commissariat. Comme ce dernier est un organisme auquel on peut faire confiance, à notre avis, on devrait peut-être éviter de renverser ses conclusions.

Il reste que, pour nous, le problème de fond n'est pas tant l'existence même de ce tribunal que le fait que le Commissariat ne pourra que recommander les sanctions administratives pécuniaires. Nous pensons que le Commissariat devrait avoir le pouvoir de les imposer directement.

[*Traduction*]

M. Iqwinder Gaheer: Ne pensez-vous pas qu'attribuer ce pouvoir uniquement au Commissaire à la protection de la vie privée serait trop?

[*Français*]

Me Alexandre Plourde: C'est le modèle qui a été adopté au Québec pour l'Office de la protection du consommateur. Un récent projet de loi qui traite de l'obsolescence programmée accorde à l'Office la possibilité d'imposer directement des sanctions administratives pécuniaires.

Je ne crois pas qu'une telle pratique donnerait trop de pouvoir au Commissariat. En raison de l'esprit et de la façon dont le projet de loi est conçu, celui-ci donne aux entreprises contrevenantes de multiples occasions de se conformer à la loi. Le rôle du Commissariat est notamment de fournir de l'information, mais aussi d'établir des accords de conformité et de discuter avec les entreprises contrevenantes pour les amener à se conformer à la loi. Ce n'est vraiment qu'en dernier recours que le Commissariat devrait imposer une sanction pécuniaire. Je ne crois donc pas que nous ayons à nous inquiéter à ce sujet.

[*Traduction*]

M. Iqwinder Gaheer: Je vous remercie.

[*Français*]

Le président: Je vous remercie.

Monsieur Lemire, je vous cède la parole.

M. Sébastien Lemire: Je vous remercie.

Maître Levac ou maître Plourde, j'ai une brève question pour vous. Il est question de modifier l'article 107 du projet de loi C-27 afin de lever toute restriction à l'exercice du droit des consommateurs d'intenter des recours civils. À votre avis, dans quelle mesure cet article restreint-il l'exercice du droit des consommateurs d'intenter un recours collectif?

Je pense qu'il s'agit d'un aspect assez unique, dont nous n'avons pas encore entendu parler à cette table.

Me Alexandre Plourde: Je vous remercie beaucoup de votre question. Vous avez dit qu'elle était brève, mais j'en aurais long à dire.

● (1700)

M. Sébastien Lemire: Ce sera alors au président d'intervenir.

Me Alexandre Plourde: Le problème que nous pose l'article 107 du projet de loi C-27, c'est qu'il menace le droit des Québécois d'intenter des recours civils, une question qui semble être passée sous le radar dans ce projet de loi, mais qui nous préoccupe beaucoup.

Selon la formulation actuelle de cet article, le droit privé d'action, c'est-à-dire le droit de poursuivre une entreprise devant un tribunal civil en invoquant la loi fédérale, ne peut être exercé qu'à des conditions très strictes: si le Commissariat à la protection de la vie privée du Canada a conclu qu'une entreprise a manqué à ses obligations, si un accord de conformité n'a pas permis de verser une indemnité au consommateur, ou si une amende a été imposée dans un des cas très précis prévus par le projet de loi.

Autrement, le consommateur ne peut pas poursuivre l'entreprise devant un tribunal civil, ne peut pas intenter une poursuite pour obtenir une indemnité et ne peut pas faire valoir ses droits devant le tribunal. Il pourrait se retrouver devant une situation où le Commissariat, par exemple, n'a pas accepté la plainte qu'il a déposée contre lui ou n'a pas rendu de conclusion, ne satisfaisant ainsi pas aux exigences prévues à l'article 107. Le consommateur se retrouverait alors privé de recours devant un tribunal et ne pourrait pas poursuivre l'entreprise au civil.

Option consommateurs est une organisation qui intente des recours collectifs, des recours civils devant les tribunaux. Dans de nombreuses situations, elle a intenté des recours collectifs contre des géants de la technologie. Par exemple, elle a intenté une poursuite contre Google. Or, ce recours collectif ne résulte pas d'une plainte traitée par le Commissariat. Si nous devions interpréter strictement l'article 107 du projet de loi, un tel recours collectif ne pourrait peut-être pas avoir lieu.

En conséquence, afin d'éviter des débats constitutionnels interminables devant les tribunaux, nous demandons que l'intention du législateur soit clarifiée, celle-ci n'étant pas, j'en suis sûr, de restreindre les recours des Québécois. Pour ce faire, nous demandons que soit ajouté à l'article 107 du projet de loi C-27 un alinéa indiquant que ce dernier n'exclut pas les recours provinciaux qui sont prévus dans le droit civil. Les recours provinciaux, les recours de droit civil, s'ajouteraient alors à ceux prévus par l'article 107. Cela règlerait beaucoup de problèmes et de débats judiciaires pour nous et assurerait aux consommateurs un très grand accès à la justice.

M. Sébastien Lemire: Mon temps est écoulé. Je vous remercie.

Le président: Je vous remercie.

Monsieur Masse, vous avez la parole.

[*Traduction*]

M. Brian Masse: Monsieur le président, je m'excuse d'avoir quitté la salle. Je mène de front plusieurs tâches. Il y a seulement un néo-démocrate au sein du Comité.

J'espère que la question n'a pas été posée, mais je pense qu'elle plaira à mes collègues. Nous allons encore faire un tour de table. Peut-être commencerons-nous cette fois-ci par ceux qui témoignent en personne.

Les partis politiques devraient-ils être visés ou non par la surveillance prévue au projet de loi? J'aimerais connaître votre opinion. Si vous ne savez pas, ce n'est pas grave non plus. C'est correct.

M. Philippe Letarte: Je m'abstiens.

M. Brian Masse: D'accord.

Des voix: Oh, oh!

M. Brian Masse: Simplement pour que nous ne puissions pas...

Des voix: Oh, oh!

[*Français*]

Me Alexandre Plourde: Comme nous sommes une association de consommateurs, nous ne traitons pas ce genre de question. Je veux cependant simplement mentionner qu'au Québec, les partis politiques sont visés par la loi.

Le président: Messieurs Gambs ou Mellouli, si vous voulez donner votre avis, vous avez la parole.

[*Traduction*]

M. Sébastien Gambs: Pour ma part, je pense qu'il faut aussi inclure les partis politiques. Toute personne qui doit recueillir des données personnelles devrait également être visée par la loi. En fait, je viens de France, où les partis politiques sont également soumis à la législation sur la protection de la vie privée. Je ne vois donc pas pourquoi ce serait différent ici. Il s'agit de données personnelles de nature sensible, de sorte que l'obligation devrait être la même pour les partis politiques.

M. Brian Masse: Vous ne devrez pas payer plus d'impôts malgré votre point de vue.

Ai-je assez de temps pour...

M. Sehl Mellouli: [*Inaudible*]

M. Brian Masse: Oh, je suis désolé.

[*Français*]

M. Sehl Mellouli: Je vais abonder dans le même sens que M. Gambs. Je crois que les partis politiques devraient être couverts.

[*Traduction*]

M. Brian Masse: C'est très bien. Je vous remercie.

Merci, monsieur le président.

[*Français*]

Le président: Merci, monsieur Massé.

Monsieur Vis, vous avez la parole pour cinq minutes.

M. Brad Vis: Merci, monsieur le président.

Madame Levac, le 3 octobre, le ministre Champagne a fait parvenir au Comité une lettre dans laquelle il indique que le gouvernement envisage la possibilité d'un amendement au préambule du projet de loi et à l'article 12 de la Loi sur la protection de la vie privée des consommateurs pour renforcer la protection des renseignements personnels des enfants.

Dans le mémoire que vous avez soumis au Comité, vous affirmez que les amendements proposés par le ministre Champagne ne sont pas suffisants pour protéger adéquatement la vie privée des enfants. Aujourd'hui, dans votre témoignage, vous avez mentionné que nous devrions apporter un amendement au projet de loi pour protéger l'intérêt supérieur de l'enfant.

Quelles sont les autres mesures que nous pouvons adopter pour améliorer ce projet de loi afin de protéger nos enfants?

Me Sara Eve Levac: Premièrement, l'amendement proposé à l'article 12 parle de la nature sensible des renseignements personnels qui sont recueillis, utilisés ou communiqués. Il y a d'autres étapes dans la vie d'un renseignement personnel où on devrait prendre en compte l'intérêt supérieur de l'enfant, par exemple lorsqu'il est question de l'accès à ce renseignement, de sa conservation ou de sa destruction.

Pour nous, l'intérêt supérieur de l'enfant est une vision plus globale qui permet de prendre en compte des considérations autres que la nature sensible d'un renseignement, en se posant des questions sur ce qui est favorable au respect de tous les droits de l'enfant et de son développement.

Outre les modifications qui intégreraient l'intérêt supérieur de l'enfant, nous proposons aussi une modification à la version française de l'alinéa 4a). Dans la version anglaise, il est manifeste que l'enfant a le droit d'exercer ses recours lui-même, mais en français, c'est moins clair.

● (1705)

M. Brad Vis: Merci.

Récemment, j'ai lu quelque chose sur l'entreprise VTech et les jouets pour enfants. Pourrions-nous apporter un amendement au projet de loi pour protéger les enfants en lien avec des jouets connectés à Internet, entre autres?

Me Sara Eve Levac: Une modification qui prendrait en compte l'intérêt supérieur de l'enfant nous forcerait à tenir compte de celui-ci dans toutes les étapes de la conception d'un nouveau jouet, de sa conception jusqu'à sa mise en marché, et dans toutes les décisions, par la suite, liées aux renseignements personnels d'un enfant.

Une autre façon de protéger les enfants en lien avec les jouets intelligents est le concept qu'on appelle la protection de la vie privée dès la conception, qui oblige à tenir compte des risques pour la vie privée dès la conception d'un nouveau service ou d'un bien et tout au long du processus.

M. Brad Vis: Merci beaucoup.

Dans le mémoire que vous avez soumis au Comité, vous affirmez que les mesures proposées à l'article 55 du projet de loi permettant aux consommateurs de demander le retrait de leurs renseignements personnels sont incomplètes. Vous déplorez le fait qu'on ne retrouve pas dans le projet de loi une forme de droit à l'oubli, comme il en existe en Europe et au Québec.

Quelles sont les lacunes de l'article 55, selon vous?

Me Alexandre Plourde: Je vous remercie sincèrement d'avoir posé cette question en français.

Il y a deux choses à dire sur l'article 55.

Tout d'abord, comme vous le mentionnez, il prévoit un droit de suppression, mais avec un bémol: si l'entreprise a inscrit dans sa politique qu'elle peut conserver les renseignements personnels, elle va les conserver. Cela donne une très grande porte de sortie aux entreprises. On devrait encadrer ce droit pour s'assurer de protéger les consommateurs.

Il est très important de pouvoir supprimer ses renseignements personnels. Au Québec, il y a eu la brèche de sécurité informatique chez Desjardins, une institution financière qui a conservé très longtemps les renseignements personnels de ses clients. La possibilité de supprimer ses renseignements personnels permet d'éviter des préjudices et le vol d'identité.

Par contre, le droit de suppression qui est prévu dans le projet de loi n'est pas un droit à l'oubli. Dans l'environnement numérique, il y a plein de renseignements nous concernant qui peuvent être propulsés dans la sphère publique, se retrouver sur les serveurs des entreprises et y demeurer éternellement. Internet n'oublie jamais. Même si ces renseignements ont été publiés légalement, cela peut causer des préjudices aux consommateurs qui ne sont pas concernés par le droit de retrait prévu dans le projet de loi.

Par exemple, imaginons que je suis quelqu'un qui a commis un crime mineur il y a plusieurs années ou plusieurs décennies. Si, chaque fois qu'on tape mon nom dans Google, on voit cela apparaître, cela peut nuire à mes perspectives d'emploi, à ma réputation et à la possibilité pour moi de refaire ma vie. C'est la même chose...

M. Brad Vis: Cela pourrait même être un enfant qui a fait quelque chose de stupide.

Me Alexandre Plourde: Oui, c'est un exemple plus sympathique encore. Lorsqu'un enfant commet une bévue ou que quelqu'un d'autre publie des photos ou des vidéos qui le concernent, tout cela reste en ligne indéfiniment et, quand on tape son nom dans Google, cela apparaît. Cela peut porter atteinte à sa réputation, l'amener à subir de l'intimidation, et même constituer du matériel pour commettre un vol d'identité.

Des solutions législatives ont été mises en place. L'Europe a adopté le droit à l'oubli, comme nous l'avons fait au Québec également. On l'appelle aussi le droit au déréférencement. Il permet à une personne de s'adresser à Google ou à n'importe quelle autre plateforme numérique pour lui demander de retirer certains renseignements personnels si elle subit un préjudice.

● (1710)

M. Brad Vis: Est-ce que la loi québécoise a déjà été utilisée? Avez-vous un exemple de cas?

Me Alexandre Plourde: C'est tout chaud, elle vient tout juste d'entrer en vigueur il y a un ou deux mois, alors je ne connais pas de cas d'application.

M. Brad Vis: D'accord.

Si jamais il y en a, je vous prie de nous en informer.

Me Alexandre Plourde: Cela me fera plaisir.

Le président: Merci, monsieur Vis. Cela me fait toujours plaisir de vous laisser plus de temps quand vous faites l'effort de vous exprimer en français. Je vous félicite pour vos efforts, d'ailleurs: ils sont remarqués, et remarquables.

Monsieur Sorbara, vous avez la parole.

[*Traduction*]

M. Francesco Sorbara (Vaughan—Woodbridge, Lib.): Je vous remercie, monsieur le président.

Monsieur Letarte, dans vos remarques liminaires, vous avez mentionné l'Australie à titre d'exemple ou de référence. J'espère que ce modèle ne limite pas toutes les législations qui sont créées.

Pouvez-vous nous expliquer comment l'Australie a conçu sa législation et ce qui vous plaît dans le modèle australien?

M. Philippe Letarte: Bien sûr, je peux tout à fait le faire.

L'Australie est allée au-delà du secteur financier et a créé un plein droit à l'égard des données des clients. J'ai dit que le mécanisme inclut les télécommunications, mais aussi l'énergie et d'autres secteurs. Au fond, il s'agit d'un modèle dirigé par le gouvernement, voire le Trésor australien, qui est un peu comme notre Trésor. Le mécanisme relève de trois entités distinctes, à savoir l'équivalent du Commissaire à la protection de la vie privée, l'équivalent de l'autorité de la concurrence et des marchés, et une autre entité chargée de l'évolution technique, c'est-à-dire de tout ce qui concerne les normes.

Il s'agit en fait d'un modèle piloté par le gouvernement, en collaboration avec l'industrie et certains groupes particuliers d'intervenants. Je pense qu'il est excellent, car il donne du pouvoir et assure une grande protection au consommateur.

M. Francesco Sorbara: Que pensez-vous des garde-fous que prévoit leur modèle, si je peux utiliser ce terme?

M. Philippe Letarte: Je pense que les garde-fous sont assez précis et complets. C'est un peu comme la carotte et le bâton. Si une personne participe à l'écosystème, elle peut lancer une entreprise dans un environnement sûr et sécuritaire. Toutefois, si elle ne met pas en place des interfaces de programmation d'applications, ou API, fiables, ou qu'elle ne respecte pas la législation en matière de protection de la vie privée, elle s'expose d'abord à des amendes importantes, mais peut aussi perdre toute crédibilité dès maintenant. La personne perd le privilège de prendre part au modèle.

Les consommateurs sont vraiment au cœur de ce modèle. Lorsqu'ils font affaire avec une entreprise, ils peuvent avoir la certitude que celle-ci a obtenu la validation adéquate et a mis en place des mesures de sécurité et de sûreté suffisantes.

M. Francesco Sorbara: Vous avez parlé de l'écosystème. Chaque fois que l'on met à jour des lois, des règles, des règlements et ainsi de suite après une période de 15 ou 20 ans, il faut que les règlements soient fondés sur des principes — j'aime bien ce terme — pour qu'ils puissent prendre de l'expansion et s'adapter à l'évolution de la technologie. Cela fonctionne dans les deux sens.

En ce qui concerne le modèle australien, puisqu'il est déjà en œuvre, comment se porte l'écosystème?

M. Philippe Letarte: Je dirais qu'il se porte plutôt bien, et c'est la même chose au Royaume-Uni. Il y a des formes d'accréditations, qui sont réalisées par de tierces parties. En gros, si on a un nouveau modèle, au lieu de suivre le lourd processus d'adhésion et d'accréditation, il est possible de passer par un agent. C'est également un modèle sûr et sécurisé.

Les choses progressent bien. Bien sûr, la technologie évolue rapidement. Comme vous l'avez mentionné, les décideurs ont veillé à ce que ce soit fondé sur des principes, mais ils ont des comités ou ses parties prenantes qui surveillent rigoureusement la façon de réaliser des échanges et de faire progresser la technologie.

Nous parlions de système bancaire ouvert, mais il s'agit de plus en plus d'un système financier ouvert comprenant l'assurance, les prêts hypothécaires et la gestion de patrimoine. L'évolution est favorable, car elle crée un environnement dans lequel les acteurs savent que les autres acteurs accrédités sont sûrs, et qu'ils peuvent faire des affaires avec eux.

M. Francesco Sorbara: Je suis un grand partisan du système bancaire ouvert, et je l'ai toujours été. J'ai travaillé à Wall Street et à Bay Street. J'essaie de me tenir au courant de tout ce qui se passe dans les services financiers. Dans le domaine du système bancaire ouvert, il y a différentes voies dans le monde au Royaume-Uni, dans l'Union européenne, en Australie et aux États-Unis. Nous avons vraiment besoin de mettre à jour de ces règles pour franchir la prochaine étape à ce chapitre.

M. Philippe Letarte: C'est tout à fait vrai.

M. Francesco Sorbara: J'ai toujours pensé que les données appartiennent au consommateur.

M. Philippe Letarte: Absolument.

M. Francesco Sorbara: Nous louons essentiellement ces données pour obtenir un service en retour de la part de l'entreprise ou de l'entité avec laquelle nous traitons.

● (1715)

M. Philippe Letarte: C'est une bonne façon de l'expliquer.

M. Francesco Sorbara: J'ai terminé, monsieur le président.

[*Français*]

Le président: Merci beaucoup, monsieur Sorbara.

[*Traduction*]

Je vous somme de vous asseoir, monsieur Perkins. La parole est à vous.

M. Rick Perkins (South Shore—St. Margarets, PCC): Je vous remercie, monsieur le président.

J'aimerais commencer par donner suite à deux questions, l'une posée par le président et l'autre par M. Gaheer, mon nouvel avocat.

Maître Plourde, je commencerai par la question intéressante sur le blocage du suivi, qui m'a frappé lorsque vous en parliez en réponse à la question du président.

S'agit-il d'un mécanisme similaire à celui que nous avons mis en œuvre il y a quelques années, à savoir la liste de numéros de téléphone exclus? Le gouvernement a décidé par voie législative que les personnes ne voulant pas être appelées par les télévendeurs, entre autres, peuvent s'inscrire à cette liste. Je crois qu'il s'agissait d'une période de cinq ans. Est-ce que ce type de mesure pourrait être prise dans le cadre de cette législation?

J'ai du mal à comprendre comment on pourrait s'y prendre, parce qu'il faut tout de même avoir quelqu'un... Si c'est fait au moyen de témoins de connexion, ce qui est très difficile en raison de la fatigue que vous avez mentionnée, il est très difficile d'affirmer qu'une personne va bel et bien sélectionner « Ne pas me suivre » parmi de nombreuses options.

[*Français*]

Me Alexandre Plourde: J'aime bien l'analogie que vous faites entre la liste de numéros de téléphone exclus et une liste permettant aux gens de refuser d'être pistés. Je vais la pousser un peu plus loin. Si je demande que mon numéro soit ajouté à la liste de numéros de téléphone exclus, toutes les entreprises devront respecter mon refus d'être appelé. Je n'aurai pas besoin d'appeler tous les télévendeurs, l'un après l'autre, pour leur dire que je refuse qu'ils m'appellent. C'est un peu le même principe que nous proposons, mais pour le numérique. Effectivement, l'analogie a du sens.

J'aimerais maintenant nous remettre un peu dans le contexte. Quand je navigue sur Internet, sur presque n'importe quelle application mobile ou sur les plateformes des entreprises technologiques, il y a une collecte omniprésente de mes données personnelles, qui sont réutilisées à des fins commerciales par les géants technologiques pour faire de la publicité ciblée, des analyses et autres. Le consentement des consommateurs à ces pratiques est souvent peu effectif. La plupart des sites Web qui font du pistage utilisent des fenêtres surgissantes pour demander aux consommateurs leur consentement à la collecte de données.

Nous proposons qu'il y ait un paramètre intégré dans le fureteur, par exemple, ou dans le téléphone, qui force les entreprises à respecter le refus d'une personne de faire l'objet d'une collecte continue de ses données personnelles. Il existe toutes sortes de mécanismes dans l'industrie qui permettent de faire cela en partie. Certains mécanismes permettent par exemple de refuser la publicité ciblée, mais cela ne nous permet pas de refuser la collecte continue de nos renseignements personnels.

Si je suis un consommateur et que je veux vraiment mettre fin à la collecte de mes renseignements personnels en ligne, une des seules façons de le faire est de me tourner vers l'autodéfense numérique, c'est-à-dire bloquer les fichiers témoins et télécharger des applications qui permettent de bloquer ces systèmes. Cependant, aucune obligation juridique ne contraint les entreprises à respecter mon refus que mes données soient recueillies. C'est ce que nous proposons d'intégrer à la loi depuis plusieurs années. Cela réglerait le problème en rendant le consentement des consommateurs effectif et simple. Ce serait très accessible pour les consommateurs.

[*Traduction*]

M. Rick Perkins: Je vous remercie.

Je reviendrai plus tard à la prochaine question que je voulais poser. C'est sur ce point que je souhaitais demander l'avis juridique de M. Gaheer. Il s'agissait de questions concernant le tribunal. J'y reviendrai si j'ai encore le temps.

Monsieur Letarte, je pense que vous avez mentionné des enjeux concernant le paragraphe proposé 29(1).

M. Philippe Letarte: C'est juste.

M. Rick Perkins: Lorsque j'examine ce paragraphe proposé — et je vous remercie de l'avoir soulevé —, je constate qu'il est sous la rubrique « Intérêt public ». Or, il est assez vaste, et je ne trouve nulle part dans le projet de loi une définition de l'« intérêt public ». J'en déduis que si on ne peut pas obtenir le consentement en temps opportun, on peut quand même faire ce qu'il faut si c'est dans l'intérêt public. C'est ainsi que j'interprète le paragraphe.

Je me demande si vous pourriez nous en dire un peu plus sur ce que vous pensez du paragraphe proposé 29(1).

● (1720)

M. Philippe Letarte: Oui, je peux certainement le faire.

Encore une fois, je trouve que c'est un peu trop large. En tant qu'exploitant d'une entreprise, je pense qu'il faut des critères plus clairs pour déterminer ce qui est dans l'intérêt public. Nous ne voulons pas en subir les contrecoups en essayant de créer un produit pour constater ensuite qu'il n'est pas dans l'intérêt public. C'est pourquoi je demanderais des critères et des exceptions afin de clarifier la teneur de l'intérêt public.

Encore une fois, j'ai donné un exemple à M. Williams tout à l'heure. Si je peux bénéficier d'un nouveau programme qui me fera automatiquement économiser de l'argent, mais que je dois m'engager avant la date limite, est-ce que c'est tout à fait dans mon intérêt? Probablement, puisque je vais réaliser des économies, mais est-ce aussi dans mon intérêt commercial? La réponse est oui.

C'est le genre de clarification que nous voulons avoir parce que, comme je l'ai mentionné, le système bancaire ouvert est fondé sur la confiance et sur la prise de contrôle de ses données, de façon à toujours savoir où elles se trouvent et où un consentement est nécessaire. Si, tout à coup, une personne est inscrite à un programme auquel elle n'a pas consenti ou reçoit des messages de marketing direct auxquels il n'a pas consenti, ce n'est pas ainsi que devrait fonctionner le système bancaire ouvert, ce qui effrite la confiance.

C'est pourquoi nous voulons qu'on clarifie ce qu'est l'intérêt public, et qu'on prévoie des exceptions et des situations pour montrer comment nous pouvons nous y retrouver. Je vous remercie de votre question.

M. Rick Perkins: En tant que spécialiste du marketing, je suis toujours à la recherche de ces failles pour utiliser les données de la manière que je souhaite dans l'intérêt de l'entreprise pour laquelle je travaille.

Des voix: Oh, oh!

M. Rick Perkins: S'il me reste du temps, monsieur le président, je vais poser ma dernière question à M^{e} Plourde, à la lumière de mes échanges.

Je pense que nous avons tous du mal à comprendre les témoignages que nous avons entendus au sujet du tribunal. Certains pensent que c'est une bonne chose. Or, certains juristes sont de l'avis contraire, pour différentes raisons. Ils estiment qu'une seule personne, le Commissaire à la protection de la vie privée, aurait trop de pouvoir, et que tous les commissaires ne sont pas égaux. Il y en a qui affirment que le tribunal ralentira la procédure, tandis que d'autres encore croient qu'il accélérera en fait les choses parce qu'il évite les dédales judiciaires en passant directement par le Commissaire à la protection de la vie privée. De plus, si une personne veut aller à la cour parce qu'elle n'aime pas le tribunal, c'est plus difficile, mais cela peut en fait accélérer ou ralentir le processus. Le Tribunal de la concurrence, par exemple, ne s'est pas avéré aussi rapide que les gens le pensaient.

Vous avez fait quelques commentaires, mais je pense que nous avons besoin d'un peu plus de conseils à ce sujet.

[*Français*]

Me Alexandre Plourde: Vous voulez comprendre l'effet du tribunal de la protection des renseignements personnels et des données sur les droits des consommateurs, je crois.

Comme je le disais tantôt, notre opinion est partagée quant à l'existence du tribunal de la protection des renseignements personnels et des données. Nous préférerions que ce soit le Commissariat à la protection de la vie privée du Canada qui ait le pouvoir d'imposer des sanctions administratives pécuniaires.

Par contre, pour nous, la question du tribunal de la protection des renseignements personnels et des données n'est pas le problème le plus important. Ce qui nous préoccupe vraiment, ce n'est pas ce tribunal, mais bien tous les autres tribunaux de droit commun devant lesquels un consommateur pourrait poursuivre une entreprise en invoquant la nouvelle loi fédérale sur la protection des renseignements personnels. Là, il y a un problème important, puisque le projet de loi actuel comporte une restriction de taille, qui pourrait nuire aux consommateurs lorsqu'ils veulent invoquer cette loi devant les tribunaux.

Le problème n'est pas le tribunal de la protection des renseignements personnels et des données. Il est plutôt à l'extérieur du processus pénal, incluant le Commissariat à la protection de la vie privée du Canada et le nouveau tribunal de la protection des données. À notre avis, le projet de loi C-27 fait que le processus civil est sévèrement entravé ou, à tout le moins, risque de l'être.

Je vais parler du Québec, parce que c'est le seul territoire que nous connaissons bien, évidemment. Le Québec a sa propre loi sur la protection des renseignements personnels, et celle-ci a plus de mordant que ce qui est sur la table aujourd'hui. Le Québec prévoit aussi des recours civils. Si une entreprise manque à ses obligations en vertu d'une loi fédérale, je peux m'adresser aux tribunaux civils, au Québec, pour faire valoir mes droits.

Selon nous, le projet de loi actuel comporte des risques. Nous ne pouvons pas prédire ce que les tribunaux vont dire quant à la portée de l'article 107, et nous craignons que cela mène à de longs débats judiciaires. Nous invitons donc les députés à s'assurer que ce projet de loi n'entrave pas les recours civils. Cette question nous préoccupe beaucoup et nous vous demandons d'agir pour protéger les droits des consommateurs au Québec, afin de s'assurer qu'ils peuvent intenter des recours en vertu de cette loi, le cas échéant.

Le président: Merci beaucoup.

Monsieur Van Bynen, vous avez maintenant la parole pour cinq minutes.

[*Traduction*]

M. Tony Van Bynen (Newmarket—Aurora, Lib.): Je vous remercie, monsieur le président.

Dans les témoignages précédents, et encore dans certains d'aujourd'hui, il était question de deux façons distinctes de gérer et rendre sûre l'utilisation de l'intelligence artificielle.

Pour l'instant, nous examinons la manière d'en réglementer différents volets, à savoir la protection de la vie privée, la compétitivité et l'utilisation de la technologie.

Il a déjà été question — je pense que c'est ce qui a été mentionné à la réunion précédente — d'avoir recours au modèle décentralisé à des fins de réglementation. Il consiste à demander au Commissaire à la protection de la vie privée d'examiner le recours à l'intelligence artificielle de son côté, et de demander au commissaire à la concurrence et à la technologie de faire de même.

Ma question s'adresse à M. Gambs.

Que pensez-vous de ces deux approches? Laquelle préférez-vous, ou laquelle recommanderiez-vous puisqu'elle est plus efficace?

● (1725)

M. Sébastien Gambs: Je pense qu'utiliser l'expertise du Commissaire à la protection de la vie privée sur les questions de vie privée et d'autres enjeux entourant l'intelligence artificielle est une bonne façon de tirer parti d'un mécanisme déjà en place. Je crois qu'une entité centralisée capable de vérifier si les entreprises respectent la protection de la vie privée, l'équité et l'explicabilité serait le moyen le plus efficace de procéder, plutôt que de diviser la tâche entre différentes entités qui devraient de toute façon se coordonner puisque cette question est complexe. Si vous êtes un ingénieur en apprentissage automatique et que vous devez intégrer la protection de la vie privée, l'équité et l'explicabilité à votre modèle d'IA, il y a une synergie entre ces éléments, et vous ne pouvez pas les traiter séparément. Je pense que la vérification serait également confiée à une entité possédant l'expertise nécessaire.

M. Tony Van Bynen: Je vous remercie.

Ma prochaine question s'adresse à M. Mellouli.

Vous faites sans cesse référence à la boîte noire. Tout d'abord, vous avez dit qu'il est extrêmement important d'authentifier les données et de s'assurer qu'elles sont exactes. D'une part, comment pouvons-nous nous en assurer? Devrions-nous réglementer une méthode d'authentification des données?

D'autre part, en ce qui concerne la boîte noire dans laquelle tout cela s'inscrit, la Loi sur l'intelligence artificielle et les données imposera aux responsables du système d'intelligence l'obligation d'y contribuer. Existe-t-il un moyen d'assurer une transparence algorithmique suffisante, et ce projet de loi y arrive-t-il? Y a-t-il suffisamment de pouvoir à ce chapitre dans ce que vous avez vu du projet de loi? Je m'inquiète de l'authenticité des données et de l'existence d'un moyen de réglementer ce volet.

Par ailleurs, il y a la transparence. Le projet de loi va-t-il assez loin pour répondre aux besoins de transparence de l'algorithme?

Est-ce que mon écran est figé? M'entendez-vous?

Le président: Nous vous entendons, monsieur Van Bynen. Il faut laisser un peu de temps pour l'interprétation.

[*Français*]

M. Sehl Mellouli: Je pense que le projet de loi, tel qu'il est présenté aujourd'hui, ne va pas assez loin pour encadrer la « boîte noire », car c'est vraiment de cela qu'il s'agit.

Vous demandez s'il faudrait réglementer l'utilisation des données. Je pense qu'il faut le faire. Comme vous l'avez mentionné à plusieurs reprises également, je pense que le commissaire à la protection de la vie privée peut jouer un très grand rôle pour sensibiliser les gens.

On peut jouer avec la donnée — on va le dire en toute honnêteté et franchise — comme on veut. Je peux vous donner n'importe quelle application. Vous cliquez sur le bouton pour accepter et on vous dit que votre demande a été bien transmise. Vous, comme consommateur, vous n'avez aucune idée si cela a été bien transmis ou non. À l'ère des mégadonnées, la gestion par les entreprises de centaines de millions de données est très complexe.

Est-on certain que le projet de loi permettra de tout contrôler? Je n'en suis pas sûr personnellement. Est-on en mesure de définir des mécanismes de formation et de sensibilisation relatifs aux définitions des données, aux choix des données et aux façons d'exploiter les données dans des systèmes d'intelligence artificielle? Je pense que oui.

Cela peut aller plus loin que la donnée elle-même. Cela peut même toucher les équipes qui font le choix des données. Ce choix peut avoir une incidence majeure en matière de discrimination. On a constaté cela dans des applications, pour lesquelles certaines catégories de personnes n'avaient pas été présentes au moment du choix des données. Il en est résulté des traitements positifs pour certains groupes, mais négatifs pour une tranche de la population. Il en existe certains exemples.

À mon avis, je pense qu'on peut améliorer le projet de loi pour mieux encadrer l'utilisation des données, favoriser une meilleure reddition de compte de la part des entreprises et donner un plus grand rôle et plus de pouvoirs au commissaire à la protection de la vie privée, notamment pour accroître sa capacité de sensibiliser et de former les gens sur l'utilisation de ces données.

● (1730)

[*Traduction*]

M. Tony Van Bynen: J'ai une petite question. Pensez-vous que les pénalités sont suffisantes?

J'ai lu qu'il y avait des sanctions pécuniaires. Y a-t-il une disposition qui devrait être envisagée pour exiger de la partie contrevenante qu'elle restitue les données qui ont été créées ou qu'elle cesse de les traiter? Pensez-vous qu'il s'agirait d'une autorité cruciale pour le Commissaire à la protection de la vie privée ou le tribunal?

S'il y a uniquement une sanction pécuniaire, elle devient tout simplement un coût d'exploitation. Comment pouvons-nous avoir un régime plus sévère de sanctions?

[*Français*]

M. Sehl Mellouli: On peut toujours mettre en place un régime de sanctions plus sévère, mais, comme je l'ai dit au début, ce ne sont pas des systèmes certains. Il faut tenir compte de l'imperfection de ces systèmes d'intelligence artificielle. Il se peut qu'une entreprise se conforme à tous les processus, mais qu'on trouve finalement des résultats qui ne sont pas concordants ou attendus. Également, quand une entreprise utilise des données d'intelligence artificielle et qu'il y en a des centaines de millions, on n'a pas la certitude que toutes sont propres ou conformes.

Si on impose des restrictions beaucoup plus sévères à l'utilisation des données, on risque également de mettre un frein au développement économique, à mon avis, parce que c'est un écosystème qui se développe à une vitesse vertigineuse et dans lequel nos entreprises doivent être concurrentielles. Pour ce faire, elles ont besoin d'utiliser les données. Si on leur impose beaucoup trop de contraintes quant au contrôle des données, cela pourrait retarder le développement des systèmes. Le développement d'un système intelligent ne se fait pas en une journée. Cela prend du temps.

C'est pour cela qu'il faut contrôler l'utilisation des données tout en reconnaissant que ce contrôle ne peut être exhaustif. C'est un contrôle d'appoint qui pourrait être exercé. C'est important, car la donnée est le coeur même de l'intelligence artificielle. Plus on va imposer de contraintes et d'obligations de reddition de comptes aux entreprises, plus cela aura une incidence négative sur l'économie. Je ne sais pas quelle serait l'ampleur de cet effet, mais la concurrence mondiale est énorme dans ce domaine.

Le président: Merci beaucoup, monsieur Mellouli.

Je pense que vous mettez le doigt précisément sur ce qui nous préoccupe, c'est-à-dire trouver un équilibre entre ces deux intérêts qui ne sont pas toujours amis.

Monsieur Lemire, vous avez la parole.

● (1735)

M. Sébastien Lemire: Merci, monsieur le président.

Monsieur Letarte, nous avons entendu que le projet de loi n'était pas clair au sujet de ce qui constitue un effet négatif, notamment en ce qui a trait à l'exception qui dispense une organisation ayant un intérêt légitime d'obtenir le consentement d'une personne pour la collecte, l'utilisation et la communication de ses données.

Selon votre expertise, comment le projet de loi devrait-il clarifier cette disposition sur les effets négatifs, et quelles sont les implications potentielles de cette ambiguïté pour la protection des renseignements personnels?

M. Philippe Letarte: En fait, il faut se demander pourquoi il y a un effet négatif. Une violation de la vie privée peut être bénéfique pour une entreprise, mais est-ce que c'est bon pour le consommateur? Il y a toujours une espèce de dilemme.

Par exemple, les habitudes de consommation d'une personne peuvent révéler des informations très personnelles. Cela peut nous indiquer si elle commence un régime, si elle a acheté une maison, si elle a réduit ses dépenses ou si elle a changé d'emploi, par exemple. Une compagnie pourrait mettre la main sur les données de cette personne pour créer un profil, puis remarquer qu'elle a changé ses habitudes de consommation et conclure qu'elle pourrait bénéficier de nouveaux rabais. Techniquement, c'est un avantage pécuniaire pour le consommateur, mais, personnellement, je ne crois pas que ce soit une bonne chose qu'une entreprise ait autant d'information sur une personne.

Il s'agit donc de définir ce qui est un effet positif ou négatif en se basant sur des cas de figure. Il faut toujours se préoccuper du consommateur en premier. Lorsqu'une entreprise recueille trop de données sur une personne, cela peut devenir très problématique pour elle.

M. Sébastien Lemire: Un de ces effets négatifs pourrait être de conclure par association que la personne souffre d'une dépression ou a des problèmes de santé mentale.

Puisque je sais que vous aimez rechercher les meilleures pratiques innovantes, existe-t-il des meilleures pratiques ou des modèles mis en place ailleurs qui pourraient être utilisés pour clarifier la disposition sur les effets négatifs liés à l'exception pour intérêt légitime?

M. Philippe Letarte: Oui. En Europe, le Règlement général sur la protection des données couvre tout le continent européen et est extrêmement précis au sujet de l'intérêt légitime. Il prévoit aussi différentes exemptions, et va même jusqu'à définir ce qu'est le marketing direct et les circonstances dans lesquelles il est interdit. Dans plusieurs projets de loi, on va jusqu'à déterminer si une publicité très ciblée et pertinente peut être considérée comme ayant un effet positif ou négatif. Encore une fois, l'Australie fait un peu l'inverse. Elle interdit le marketing direct, sauf dans certains cas, et elle clarifie ces exceptions.

Alors, en effet, il y a plusieurs bonnes pratiques, et l'avantage d'être en retard sur le reste du monde à cet égard est qu'on peut choisir l'approche qui nous convient le mieux.

M. Sébastien Lemire: Merci beaucoup.

Le président: Merci.

Je cède la parole à M. Masse.

[*Traduction*]

M. Brian Masse: Je vous remercie.

J'aimerais connaître votre avis sur les États-Unis et leur processus actuel. Si nous adoptons une méthode différente, comment cela pourrait-il avoir une incidence sur le commerce de placements, parce que nous avons beaucoup d'entreprises qui s'appuient les unes sur les autres?

Je vous remercie.

M. Philippe Letarte: La bonne nouvelle, c'est que le Consumer Financial Protection Bureau, ou CFPB, a publié sa première série de règles il y a quelques semaines, et examine de près ce qu'il veut faire. Bien sûr, le CFPB ne se préoccupe pas de tout et adopte plutôt une approche de laisser-faire sur certaines choses. Mais pour la première fois, il dit clairement vouloir créer un droit universel à la protection des données, qui sera imposé aux institutions financières. Une fois que ce sera fait et que nous serons sur la même longueur d'onde — je sais que les gens du ministère des Finances du Canada parlent aussi à leurs homologues du CFPB —, je ne pense pas qu'il sera si difficile de faire du commerce transfrontalier, puisque la grande équipe et le principe de base sont très similaires.

M. Brian Masse: C'est vrai. Ainsi, le consommateur a un plus grand pouvoir discrétionnaire et peut choisir le niveau d'exposition qu'il souhaite.

M. Philippe Letarte: Absolument, et les clients peuvent choisir le moment de l'exposition. Par exemple, si une personne veut essayer le même produit de deux sociétés différentes et qu'elle préfère l'une d'entre elles, elle peut laisser tomber l'autre immédiatement. Par conséquent, les données du client ne seront plus utilisées par cette entreprise.

Il s'agit en fait de redonner le pouvoir au consommateur et de réduire le délai avec lequel il peut révoquer son consentement.

M. Brian Masse: Je vous remercie.

Merci, monsieur le président.

[*Français*]

Le président: Merci beaucoup, monsieur Masse.

Ceci conclut cette 100e réunion du Comité permanent de l'industrie et de la technologie de la Chambre des communes.

Je remercie le groupe de témoins et j'en profite pour souligner le fait que d'avoir des rencontres qui se tiennent autant en français à Ottawa relève plus de l'exception que de la règle. À titre personnel, c'est un plaisir que cela ait été le cas pour cette 100e réunion.

Sur ce, je vous remercie. Je tiens également à remercier M. Mellouli et M. Gambs, qui se sont joints à nous en mode virtuel. Je salue particulièrement M. Mellouli, qui est de l'Université Laval et donc dans ma circonscription. Je remercie aussi les interprètes, les analystes et la greffière.

Nous allons suspendre brièvement la réunion avant de poursuivre à huis clos pour les affaires du Comité.

La rencontre est suspendue.

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