CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

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

ETHI • NUMÉRO 099 • 1re SESSION • 42e LÉGISLATURE

TÉMOIGNAGES

Le mardi 17 avril 2018

Président

M. Bob Zimmer

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

Le mardi 17 avril 2018

● (0845)

[*Traduction*]

Le président (M. Bob Zimmer (Prince George—Peace River—Northern Rockies, PCC)): Bon retour à tous.

La séance est ouverte. Le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique tient aujourd'hui sa 99e réunion. Conformément au paragraphe 108(2) du Règlement, nous examinons l'atteinte à la sécurité des renseignements personnels associée à Cambridge Analytica et Facebook.

Nous avons aujourd'hui des témoins en personne et par vidéoconférence.

En personne, nous avons Daniel Therrien, commissaire à la protection de la vie privée du Canada, et Barbara Bucknell, directrice des politiques et de la recherche.

Par vidéoconférence, nous avons Chris Vickery, directeur de la recherche sur les risques cybernétiques, à UpGuard.

Bienvenue à tous.

Monsieur Therrien, je vous cède la parole.

M. Daniel Therrien (commissaire à la protection de la vie privée du Canada, Commissariat à la protection de la vie privée du Canada): Bonjour.

[*Français*]

J'aimerais remercier les membres du Comité de m'avoir invité à discuter aujourd'hui de l'incidence des plateformes en ligne sur la protection de la vie privée et des solutions législatives qui pourraient répondre aux préoccupations des citoyens concernant l'utilisation de leurs renseignements personnels.

Comme vous le savez, il y a quelques semaines, j'ai reçu une plainte à ce sujet et j'ai annoncé que le Commissariat avait lancé une enquête officielle sur la façon dont les activités de Facebook et d'AggregateIQ ont pu porter atteinte à la vie privée des Canadiens.

Compte tenu de mes obligations juridiques en matière de confidentialité lors d'une enquête, je ne peux discuter des détails de cette enquête avec vous aujourd'hui. Je ne peux certainement pas préjuger de nos conclusions.

Je peux toutefois vous offrir mes observations sur le contexte plus général qui, je l'espère, pourraient vous aider lors de vos délibérations.

[*Traduction*]

Les Canadiens veulent profiter des nombreux bienfaits de l'économie numérique, mais ils s'attendent à juste titre à ce qu'ils puissent le faire tout en sachant que leurs droits et leurs renseignements personnels seront protégés par des lois efficaces. Ils veulent avoir la confiance que les règles, les lois et le gouvernement les protégeront contre d'éventuels préjudices.

Dans la récente affaire Facebook, le PDG de l'entreprise, Mark Zuckerberg, a admis qu'il y avait eu un « grave bris de confiance ». Comme l'a reconnu le PDG d'un autre géant de la haute technologie, Tim Cook d'Apple, la situation est tellement alarmante qu'il est maintenant temps d'adopter des lois à la mesure du problème afin de réglementer l'économie numérique. Le temps de l'autorégulation est terminé.

Bien sûr, au Canada, nous avons des lois relatives à la protection de la vie privée. Mais celles-ci sont très permissives et accordent aux entreprises une grande latitude en ce qui concerne l'utilisation des renseignements personnels dans leur propre intérêt. En vertu de la Loi sur la protection des renseignements personnels et les documents électroniques, la LPRPDE, les organisations doivent respecter le principe de responsabilité, mais les Canadiens ne peuvent se fier exclusivement aux entreprises pour gérer leurs renseignements de façon responsable. La transparence et la responsabilité sont nécessaires, mais elles ne sont pas suffisantes.

Pour être clair, il ne suffit pas de demander aux entreprises d'être à la hauteur de leurs responsabilités. Les Canadiens ont besoin de lois plus strictes en matière de protection des renseignements personnels qui les protégeront lorsque les organisations échoueront à le faire. C'était l'une des principales conclusions de mon rapport annuel au Parlement l'année dernière. J'ai également soulevé ce point au cours de votre étude récente de la LPRPDE, la loi fédérale sur la protection des renseignements personnels dans le secteur privé.

Compte tenu de l'opacité des modèles d'affaires et de la complexité des flux de données, la loi devrait permettre au commissariat, à titre de tiers indépendant, de se rendre dans une organisation et de vérifier si cette dernière respecte les principes de protection de la vie privée, et ce, sans devoir au préalable soupçonner qu'il y a eu violation de la loi.

Le moment est aussi venu de conférer au commissariat le pouvoir d'émettre des ordonnances et d'imposer des sanctions pécuniaires contre ceux qui refusent de se conformer à la loi.

Une législation renforcée n'a pas à être un obstacle à l'innovation. Nous savons que nos renseignements personnels sont au coeur de la révolution numérique, y compris les avancées en intelligence artificielle. Ces avancées sont essentielles au développement social et économique du pays. Nous avons besoin d'un cadre législatif qui exige un consentement éclairé comme règle générale, tout en reconnaissant que le consentement ne sera pas toujours possible dans le monde des mégadonnées et de l'intelligence artificielle, où les renseignements personnels sont utilisés à des fins qui ne sont pas toujours connues lors de leur cueillette initiale.

C'est pourquoi nous avons recommandé que le Parlement examine la possibilité de proposer de nouvelles exceptions au consentement. Nous pensons qu'il est préférable d'adopter de telles exceptions, assorties de conditions qui protégeraient réellement la vie privée, plutôt que de s'en remettre à une interprétation si élastique du consentement qu'il en perd son sens. Nous préférons des exceptions restreintes et particulières — mais nous reconnaissons qu'une option pourrait être une exception d'intérêt légitime comme il en existe en Europe.

J'ai constaté avec grand plaisir que votre comité a récemment publié un rapport réclamant des changements en profondeur à la loi fédérale sur la protection des renseignements personnels dans le secteur privé, qui comprenait certaines recommandations que j'avais formulées, ainsi que plusieurs autres suggestions qui renforceraient de façon significative les droits des Canadiens en matière de protection de la vie privée. Votre rapport montre que vous comprenez bien les conséquences du caractère désuet des lois fédérales actuelles, et vous avez activement réclamé que le gouvernement apporte des changements en profondeur.

● (0850)

Plusieurs autres intervenants, en particulier au cours des dernières semaines, en arrivent au même constat, y compris certains chefs de file de l'industrie technologique.

Je suis d'avis qu'il est maintenant temps d'agir.

[*Français*]

Il est également temps d'agir dans le domaine des mesures de protection de la vie privée et des partis politiques.

Comme vous le savez, aucune loi fédérale sur la protection de la vie privée ne s'applique aux partis politiques. La Colombie-Britannique est la seule province qui possède une législation en la matière.

La situation est différente dans de nombreux autres pays. Le Royaume-Uni, la plupart des pays membres de l'Union européenne et la Nouvelle-Zélande, entre autres, ont des lois qui régissent les organisations politiques à cet égard.

En fait, dans de nombreux États membres de l'Union européenne, les renseignements relatifs aux opinions politiques sont considérés comme étant de nature très délicate et, à ce titre, ces renseignements sont considérés comme nécessitant des mesures de protection supplémentaires.

Dans l'environnement numérique, il existe maintenant de nombreux acteurs qui jouent un rôle dans ce domaine, dont les courtiers en données, les entreprises d'analyse de données, les réseaux sociaux, les fournisseurs de contenu, les spécialistes du marketing numérique et les entreprises de télécommunications.

Par conséquent, pendant que je mène une enquête sur des organisations commerciales comme Facebook et AggregateIQ, je ne suis pas en mesure d'enquêter sur la façon dont les organisations politiques utilisent les renseignements personnels que des entreprises leur transmettent.

Il s'agit, selon moi, d'une lacune importante.

Il faudrait qu'une entité indépendante détenant les pouvoirs nécessaires puisse examiner les pratiques des partis politiques et déterminer si les droits en matière de respect de la vie privée sont véritablement respectés par tous les principaux intervenants.

Cette lacune doit être comblée au moyen d'une mesure législative qui reste à déterminer, soit une loi existante sur la protection des renseignements personnels, soit la Loi électorale du Canada ou encore une autre loi.

En conclusion, je voudrais de nouveau souligner l'urgence de la situation ainsi que les enjeux auxquels il faut faire face.

L'intégrité de nos processus démocratiques et la confiance à l'égard de l'économie numérique sont exposées à des risques importants.

Il s'agit de questions pressantes sur lesquelles les législateurs doivent se pencher, et je vous félicite de le faire.

Je vous remercie à nouveau de l'invitation, et c'est avec plaisir que je répondrai à vos questions.

Merci.

[*Traduction*]

Le président: Merci, monsieur Therrien.

Nous passons maintenant à Chris Vickery, qui se trouve sous le soleil de la Californie aujourd'hui.

Monsieur Vickery.

M. Chris Vickery (directeur de la recherche sur les risques cybernétiques, UpGuard, à titre personnel): Bonjour.

C'est un plaisir de comparaître devant vous aujourd'hui. Je vous remercie de m'en donner l'occasion. Je pense que le sujet à l'étude en est un d'une grande importance. Facebook est certainement un des principaux éléments en cause, mais je vous encourage tous vivement à garder un oeil sur les efforts très ciblés de ceux dont Facebook sert de pilier à leurs activités, mais pas uniquement Facebook; ceux dont l'objectif ultime est, à mon avis, de nuire à l'institution même de la démocratie.

Au cas où vous n'auriez jamais entendu parler de moi, je me trouve en quelque sorte dans une situation idéale pour parler de ce sujet. Mon travail consiste principalement à traquer les fuites de données. Je me suis autoproclamé « chasseur de fuites de données ». Au cours des dernières années, je me suis taillé une réputation de grand expert sur la prévalence et les causes des fuites de données, de même que sur les modèles d'intervention communs des entités touchées. Je vous prie de noter toutefois que les fuites de données que je localise et sécurise ne sont pas le fait d'actions malveillantes ou d'exploitation des ordinateurs. Il s'agit tout simplement de données qui, pour une raison ou une autre, se promènent à l'air libre, et dont personne ne s'est rendu compte jusqu'à ce que j'intervienne. Et vous seriez surpris du nombre de fois où cela se produit. Il y a une épidémie d'erreurs de configuration sur Internet.

J'ai sécurisé des fuites de données en provenance, par exemple, de Verizon, Viacom, Microsoft, Hewlett-Packard, le département de la Défense des États-Unis, l'institut national électoral au Mexique, l'INE, des listes noires du terrorisme international, de même que le site Web de Trump lors de la campagne présidentielle en 2016. Il y avait là des fuites d'information également.

Au total, mes efforts ont permis de protéger près de deux milliards de dossiers contenant des renseignements personnels, alors je connais bien le sujet. Je serai heureux de répondre à vos questions.

Plus précisément, j'aimerais mentionner que deux fuites de données que j'ai découvertes en décembre 2015 concernaient l'enregistrement des électeurs partout aux États-Unis, dans les 50 États, plus le district de Columbia. La deuxième fois, en décembre, les données étaient plus détaillées. Il y avait des renseignements personnels sur les gens, leur personnalité, leurs comportements, et on mentionnait s'ils possédaient une arme, s'ils suivaient les préceptes de la Bible.

Six mois plus tard, en 2016, je suis tombé sur une autre base de données nationale d'électeurs aux États-Unis, encore plus détaillée que la précédente, qui précisait si une personne suivait les courses NASCAR, si elle était contre l'avortement et si elle était susceptible de posséder une arme.

Puis je suis tombé sur un autre ensemble de dossiers nationaux. Je les ai téléchargés après les avoir trouvés en juin 2017. Il s'agissait alors de la troisième série de données électorales des États-Unis au complet sur laquelle je tombais. Elle contenait 198 millions de dossiers, ce qui constituait la plus importante fuite de données sur les électeurs aux États-Unis connue de toute l'histoire. J'aimerais souligner qu'au moment de leur découverte, aucune de ces bases de données n'était protégée par un simple nom d'utilisateur ou mot de passe. Les données étaient à l'air libre. En sachant où chercher, n'importe qui dans le monde pouvait les trouver.

Le cas d'AggregateIQ qui m'amène ici aujourd'hui a commencé le 20 mars de la présente année — c'est donc tout récent. Je ne connaissais pas AggregateIQ avant le 20 mars. Je me promenais sur un site Web ouvert au public appelé GitHub où les développeurs collaborent et publient un code source ouvert.

● (0855)

J'ai vu un renvoi à @aggregateiq.com au sujet d'un code de SCL Group qui était à l'air libre et accessible au public. J'ai suivi les miettes de pain, découvert qui était AggregateIQ et remarqué que l'entreprise avait un sous-domaine appelé GitLab. Quand j'ai regardé gitlab.aggregateiq.com, je me suis rendu compte qu'on pouvait s'inscrire et, qu'en fait, l'entreprise invitait toute la planète à s'ouvrir un compte sur son portail de collaboration.

Je me suis donc ouvert un compte, je suis entré sur le site, et j'ai eu accès à tous les outils, utilitaires, authentifiants, messages, problèmes et notes des employés, et les demandes de fusion me sont apparues. Je me suis vite rendu compte de l'importance de cela et que cela intéresserait au plus haut point les organismes de réglementation, les gouvernements et les gens de plusieurs pays, alors j'ai commencé le téléchargement. Normalement, je m'efforce de protéger les gens qui peuvent être touchés par ce genre de choses, mais je dois dire que, dans ce cas, l'intérêt évident de la population de connaître la vérité au sujet des activités de Cambridge Analytica, AggregateIQ et SCL Group a été un facteur décisif. Je ne veux pas que vous pensiez que je me contente de remettre aux intéressés leur linge sale quand je découvre ce genre de choses. La situation est différente dans ce cas.

Je répète que n'importe qui dans le monde possédant une connexion Internet aurait pu trouver la même chose, en s'ouvrant un compte comme je l'ai fait, et en téléchargeant exactement la même information, peu importe le pays où il se trouve, et le type de loyauté qu'il éprouve. Les données étaient à l'air libre, sans aucune protection. Un internaute malveillant aurait pu faire un pas de plus, car il y avait, et y a, des mots de passe de bases de données, des noms d'utilisateur, des authentifiants, des clés et des méthodes d'authenfication documentées dans ces dossiers dont je n'ai pas tiré parti. Je les ai téléchargés, mais je ne suis pas passé à l'étape suivante, soit utiliser les mots de passe pour avoir accès aux bases de données.

Si quelqu'un d'autre les avait trouvés et qu'il était convaincu de pouvoir en tirer un avantage, la fuite de données aurait pu et pourrait être beaucoup plus grave que ce qui a été mentionné. L'infiltration aurait pu être totale. Chaque donnée ayant passé par les mains d'AggregateIQ pourrait être entre les mains de quiconque aurait pu constater la même brèche.

Il y a quelques questions auxquelles je n'ai pas trouvé totalement de réponse et que votre enquête devrait, je crois, tenter d'éclaircir. Même si j'examine encore une partie des données, je n'ai pas encore compris exactement les liens d'AggregateIQ avec SCL Group et Cambridge Analytica. Les murs qui séparent ces entités sont très poreux. Il est clair que les trois, et d'autres groupes, ont eu accès aux permissions d'accès et aux données, alors je vous en prie, allez au fond des choses.

La deuxième question est de savoir dans quelle mesure, si c'est le cas, AggregateIQ ou ses employés ont utilisé des renseignements privés ou politiques à accès limité à des fins commerciales et lucratives. J'ai trouvé des preuves de la présence de réseaux de publicité en formation sous le même domaine, dont un qui s'appelle notamment Ad*Reach — à noter qu'il y en a quelques-uns qui portent ce nom sur Internet, alors assurez-vous d'avoir le bon avant de vous lancer dans un interrogatoire —, de même que aq-reach. Un des employés qui travaillait à AIQ travaillait aussi pour une entreprise de publicité appelée easyAd Group AG, basée en Suisse et ayant des filiales aux États-Unis et en Russie. J'adorerais savoir quel genre de travail on faisait et si les données qui transitaient par AIQ étaient utilisées dans ces campagnes de publicité ou ces montages sur lesquels travaillait l'employé à ce moment.

● (0900)

Le président: Vos 10 minutes sont écoulées, alors si vous pouviez conclure, ce serait parfait.

M. Chris Vickery: Oui. J'ai un dernier point.

Il y a aussi une cryptomonnaie associée à cela. Un commentaire très exactement dans la section commentaires de GitLab était marqué d'un drapeau, et j'ai vu plus tard qu'il s'agissait d'un drapeau confidentiel. Le commentaire portait sur le jeton Midas. J'ai regardé de quoi il s'agissait. Le jeton Midas était un projet sur lequel ils travaillaient, et il était en lien avec un site Web qui vendait de la cryptomonnaie à un montant minimal de 10 000 $.

Le site Web a été fermé depuis que l'affaire a été rendue publique, et si vous voulez mon avis, il y a anguille sous roche. Si vous pouviez découvrir pourquoi quelqu'un tentait de concevoir une cryptomonnaie sur AggregateIQ GitLab, pour vente au public, et pourquoi on voulait le faire à l'abri des regards, je pense que cela vaudrait la peine d'enquêter.

Merci. Je serai heureux de répondre à vos questions.

● (0905)

Le président: Merci, monsieur Vickery.

J'aimerais simplement signaler aux membres du Comité qu'il est environ trois heures plus tôt en Californie, alors il est debout à 5 heures du matin.

Merci encore d'avoir comparu.

Nathaniel Erskine-Smith sera le premier intervenant.

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

Il y a beaucoup d'éléments dans ce que nous avons entendu. Ma première question en est une de clarification.

À partir de tout ce que vous avez examiné — et bien sûr, vous n'avez pas tout examiné compte tenu du volume d'information auquel vous avez eu accès —, vous pensez que les renseignements qui ont été recueillis au cours de différentes campagnes à des fins précisément politiques et publiques ont été utilisés à des fins commerciales et lucratives.

M. Chris Vickery: C'est très probable que ce soit le cas. J'ai les outils. Je n'ai pas les ingrédients avec lesquels on les amalgame, car il aurait fallu pour ce faire que je fasse un pas de plus pour accéder aux bases de données. À mon avis, il n'y a pas de raison d'avoir ces outils organisés de cette façon, et la documentation comme elle est, si ce n'est pas pour amalgamer les données politiques pour s'en servir à des fins commerciales.

M. Nathaniel Erskine-Smith: D'accord.

Pour ceux d'entre nous qui connaissent moins bien le domaine, pourriez-vous nous donner un exemple? Vous avez parlé des propriétaires d'arme à feu. Vous avez parlé de ceux qui vivent selon les préceptes de la Bible et de quelques autres exemples. Quel est le renseignement le plus personnel que vous ayez trouvé?

M. Chris Vickery: Le renseignement le plus personnel dans les données sur les électeurs ou en général?

M. Nathaniel Erskine-Smith: Quand vous parlez d'utiliser différentes bases de données pour arriver à dresser le profil d'une personne, à quel point ce profil est-il détaillé?

M. Chris Vickery: Le message le plus détaillé que vous avez envoyé à un être cher dans une application de chat peut facilement être lu, archivé et rattaché à votre nom.

M. Nathaniel Erskine-Smith: Vous avez vu des exemples de ce genre?

M. Chris Vickery: Oui, mais laissez-moi apporter quelques précisions. Il y a un incident distinct lié à Facebook dont on n'a absolument pas encore parlé — je travaille avec un journaliste en ce moment pour le rendre public — qui ne concerne pas Cambridge Analytica, à ce que je sache, mais on parle de 48 millions de personnes dans ce cas. Il concerne des messages. On ne sait pas encore le degré de caractère privé des messages qui ont été envoyés, mais on y trouve des renseignements très personnels.

M. Nathaniel Erskine-Smith: Vous avez mentionné que différentes bases de données sont amalgamées, si j'ai bien compris, de certaines façons pour créer ces profils. Pouvez-vous nous parler de l'importance de ces bases de données? Certaines sont sans doute les bases de données sur les électeurs dont vous avez parlé. Pouvez-vous nous donner d'autres exemples?

M. Chris Vickery: Oui. Dans sa documentation, Aggregate IQ décrit son système en détail. Au départ, elles sont amalgamées par l'entrepôt de données du Data Trust du RNC, soit le Republican National Committee ici aux États-Unis. J'avais trouvé la base de données du Data Trust avant qu'elle fasse partie des résultats de recherche en juin 2017. Elle est assez étendue. Elle contient des données fusionnées avec i360, qui est une entreprise spécialisée dans les renseignements politiques financée par les frères Koch. Data Trust a supprimé un article de blogue dans lequel il faisait valoir que ses données avaient été fusionnées avec celles d'i360.

Il y a aussi L2 Political. Cette entreprise a fourni des données à cette énorme machine. Cambridge Analytica l'a récemment admis sur son site Web.

Il est évident que Facebook entre en ligne de compte. La documentation d'AggregateIQ explique ensuite que les bases de données commerciales sont visées. Je sais qu'Experian en est une qui a versé des données au dossier du Deep Root Analytics du RNC que j'ai trouvé en 2017. Si je le sais, c'est qu'il y avait des identifications d'Experian pour chaque identification d'électeur et que les habitudes de consommation de chaque personne y étaient associées.

AggregateIQ affirme aussi que les candidats peuvent apporter leurs propres sources d'information concernant les bénévoles, les partisans et les donateurs. Ils réunissent toutes ces données dans une « base de données de la vérité » principale, comme ils l'appellent. Les registres électoraux de l'État corroborent ensuite le contenu des dossiers du RNC.

Alors, il n'y a vraiment aucune limite à ce qu'ils peuvent y ajouter.

● (0910)

M. Nathaniel Erskine-Smith: Vous avez mentionné qu'il y a des murs poreux entre certaines de ces entités, comme AIQ et Cambridge Analytica. Lorsque vous accédez aux renseignements d'AIQ, pouvez-vous nous donner un exemple pour nous montrer à quoi ressemble cette relation poreuse? Donnez-nous les principaux exemples dans lesquels vous voyez les acteurs de diverses entreprises accéder aux mêmes renseignements.

M. Chris Vickery: Un exemple qui est très à propos, car il illustre tant la découverte initiale que la nature de cette relation, est celui d'un employé du nom d'Ali Yassine. J'essaie habituellement ne pas nommer de personnes, mais j'estime que c'est important que vous le sachiez pour vous pencher sur la question. Il était développeur complet pour le compte du SCL Group. Sur sa page GitHub publique, il avait un code d'AggregateIQ. Je le sais parce que je l'ai trouvé dans la base de codes d'AggregateIQ, et il était inscrit que ce code avait été écrit par un employé d'AggregateIQ du nom de Koji. Alors SCL et AggregateIQ, qui n'ont supposément aucun lien entre eux, travaillent tous les deux avec la même base de codes. Ensuite, plus loin dans la base de codes, il y a un champ « client » où il était écrit « Cambridge Analytica ». Je ne vois pas pourquoi le SCL Group dirait que Cambridge Analytica est un de ses clients puisqu'il est, au fond, propriétaire de Cambridge Analytica. Le SCL Group est son organisation mère. La seule explication raisonnable pour moi est que ce serait AggregateIQ qui aurait indiqué que Cambridge Analytica était son client, avant de transmettre le code au SCL Group, code qui n'aurait pas été modifié immédiatement. Il y a là une petite situation triangulaire.

Je peux aussi vous dire que les registres de GitLab montrent très clairement que, dans le cas du projet Ripon, qui a été principalement élaboré pour la campagne de Ted Cruz en 2016, les toutes premières données ont été téléchargées du domaine scl.ripon.us, elles ont été placées dans le GitLab, et elles se sont ensuite développées et ont évolué à partir de là. Scl.ripon.us est un domaine sous le nom d'Alexander Nix. C'est lui qui est enregistré dans les dossiers WHOIS. C'est un autre exemple de code qui passe de l'un à l'autre.

En outre, dans ses déclarations publiques, Cambridge Analytica a présenté des exemples de données qu'elle a utilisées. Récemment, je suppose qu'elle s'est sentie obligée d'être transparente quant à l'origine des données. Elle a avoué qu'elle avait les données du Data Trust du RNC. Les identifications du RNC se trouvent partout dans les champs, les catégories, les scripts cibles et les analyseurs qui se trouvent dans le dépôt central d'AggregateIQ ainsi que dans sa documentation. Donc, si les données [*Difficultés techniques*] directement de l'un à l'autre, il est clair qu'ils traitent le même type de données.

Le président: Merci, monsieur Erskine-Smith. Nous aurons une autre série de questions puisque nous avons deux heures.

La parole est maintenant à M. Kent pour sept minutes.

L'hon. Peter Kent (Thornhill, PCC): Merci, monsieur le président.

Merci, monsieur Therrien et monsieur Vickery d'être avec nous aujourd'hui.

Monsieur Therrien, je sais que vous ne pouvez pas parler en détail de votre enquête officielle sur Facebook et AIQ dans le contexte canadien, mais je me demande si vous pourriez nous dire quand vous vous attendez de terminer l'enquête et de présenter un rapport.

● (0915)

M. Daniel Therrien: C'est difficile à dire. Bien des facteurs entrent en jeu. La loi nous donne un an pour mener à bien notre enquête. Nous essaierons évidemment de terminer avant cela.

Lorsque vous prenez les allégations qui ont été soulevées, vous voyez une série d'interactions relativement complexes entre un certain nombre d'acteurs. Il nous faudra les clarifier, ce qui pourrait prendre un peu de temps. Nous travaillons aussi en concertation avec d'autres commissaires ou responsables de la protection des données. Bien entendu, nous le faisons avec la province de la Colombie-Britannique, avec laquelle nous menons conjointement cette enquête, mais nous sommes aussi en contact avec d'autres personnes, notamment au Royaume-Uni, mais pas seulement là-bas. Il y a, ensuite, un peu de coordination à assurer.

Ce que je dis, c'est que c'est un processus en quelque sorte complexe, ce qui pourrait le rallonger, mais nous avons pour objectif de le terminer au plus tard dans un an, et nous essaierons de le faire avant cela.

L'hon. Peter Kent: Merci.

Vos remarques d'aujourd'hui dans lesquelles vous demandez encore qu'on modifie la Loi sur la protection des renseignements personnels pour qu'elle vise l'utilisation que font les partis politiques des renseignements personnels a considérablement plus de portée compte tenu de l'information qui se trouve devant nous et le public concernant les tentatives — dans certains cas, peut-être couronnées de succès — d'entrave au processus démocratique dans le contexte des dernières élections aux États-Unis et du vote du Brexit au Royaume-Uni. Il est clair que nous avons des questions à poser à M. Wylie concernant la période pendant laquelle il a travaillé pour le Parti libéral du Canada sous la direction de deux chefs entre 2007 et 2009, son congédiement pour ce qu'un des chefs a décrit comme étant des aspects indiscrets du travail qu'il faisait ou qu'il proposait qu'on utilise, et ensuite sa nouvelle embauche par le groupe de recherche libéral après les élections de 2015 — en 2016 — et le paiement de 100 000 $. Ce sont des questions que nous garderons pour un autre jour.

Cependant, vous demandez que les partis politiques soient visés par la loi et qu'ils soient réglementés par la Loi sur la protection des renseignements personnels ou la Loi électorale du Canada. Selon vous, laquelle devrait avoir priorité?

M. Daniel Therrien: Je dirais probablement les deux, en fait. Dans la situation actuelle, la plupart des partis politiques fédéraux ont des politiques en matière de protection des renseignements personnels — des codes de déontologie internes, pour ainsi dire, qui régissent leur relation avec les personnes avec lesquelles ils interagissent et au sujet desquelles ils recueillent des renseignements. C'est un début.

Premièrement, si j'en juge par ce que nous avons vu, je pense que la teneur de ces politiques pourrait être rehaussée. Un élément commun qui manque aux politiques en matière de protection des renseignements personnels est le droit des électeurs d'avoir accès aux renseignements personnels qui leur appartiennent et que détiennent les partis politiques fédéraux. C'est une énorme lacune. Il y a, ensuite, la question de la teneur. Cependant, il s'agit de codes volontaires, et aucune personne indépendante des partis ne vérifie si les partis honorent réellement la promesse qu'ils font dans ces politiques. Cela m'amène à la raison très importante pour laquelle les partis politiques devraient être gouvernés par une loi: pour veiller à ce que les règles de droit substantielles, quelles qu'elles soient et qui seront — espérons-le — meilleures que celles qui existent, soient vérifiées par un tiers indépendant.

Ce tiers indépendant devrait-il être le commissaire à la protection de la vie privée, le directeur général des élections ou une tierce personne? On peut en discuter, mais je pense que cela nous amène à penser — du moins c'est mon cas — qu'il y a au moins deux types de questions qui entrent en jeu ici. Il y a la question de la protection des renseignements personnels et celle de savoir si les partis traitent ceux des personnes comme il se doit, ce qui est un cas de protection des renseignements personnels qui ferait peut-être de moi la meilleure personne pour enquêter sur la question. Ensuite, les allégations qui ont été soulevées au cours des dernières semaines font ressortir une combinaison d'utilisation et de protection des renseignements personnels d'une part et des activités politiques d'autre part, ce qui est plus du ressort du directeur général des élections. Idéalement, je dirais que les deux institutions seraient en mesure de vérifier ce qui se passe pour pouvoir mettre leurs expertises respectives en commun.

● (0920)

L'hon. Peter Kent: Je présume que vous avez écouté le témoignage de M. Zuckerberg à Washington la semaine dernière.

M. Daniel Therrien: Nous avons lu à ce sujet.

L'hon. Peter Kent: Je me demande si vous pourriez me donner vos impressions sur ce qu'il a dit. A-t-il apaisé ou intensifié une quelconque de vos préoccupations avec ses réponses?

M. Daniel Therrien: Pas particulièrement. Les médias en ont beaucoup parlé. Nous enquêtons sur Facebook, alors ce que je dis se rapporte à ce qu'en ont dit les médias et à des faits qui diffèrent de ceux sur lesquels je mène une enquête. Cependant, je pense qu'il convient de dire que le public sait que Facebook a fait bien des promesses à ses utilisateurs au fil des ans pour rectifier ceci ou cela, pour les mettre en contrôle de leurs renseignements personnels. Cela a été fait année après année pendant un certain nombre d'années, et Facebook n'est pas la seule entreprise à agir ainsi.

L'hon. Peter Kent: Non, non, j'en suis conscient.

M. Daniel Therrien: Cela m'amène à la question de la responsabilité. Il est nécessaire que les entreprises en fassent preuve, mais ce n'est pas suffisant. Il faut une personne indépendante qui vérifie si elles sont vraiment responsables.

L'hon. Peter Kent: Merci.

Permettez-moi de vous poser une question brève, monsieur Vickery. J'en aurai certainement d'autres au cours des deux prochaines heures. Facebook maintient, peut-être pour des raisons de responsabilité légale, qu'il ne s'agissait pas en fait d'une atteinte à la sécurité des renseignements, mais simplement d'un usage abusif des conditions de service. Nous sommes au courant de l'atteinte à la sécurité dans le cas du scandale d'Equifax, par exemple, mais estimeriez-vous qu'il s'agit d'un autre type de violation?

M. Chris Vickery: On m'a posé la question, et ma réponse serait que oui, je le ferais. Cependant, je dois expliquer que, dans le cadre de mon travail, je fais la distinction entre une atteinte malveillante et une atteinte non malveillante. Dans ce cas, je ne placerais pas nécessairement cela dans la catégorie des atteintes malveillantes, mais il s'agissait d'une violation de la façon attendue de gérer ces données puisqu'elles ont été recueillies sous couvert de recherche universitaire et non pour être utilisées à des fins commerciales ou autres — et elles l'ont clairement été. On a franchi cette limite. Facebook a demandé que les renseignements soient supprimés, etc. Nous connaissons tous l'histoire.

Je parlerais d'une atteinte à la sécurité des données, mais seulement [*Difficultés techniques*] la différence entre une attaque et un autre type d'atteinte à la sécurité des données.

Le président: Merci, monsieur Kent.

La parole est maintenant à M. Angus pour sept minutes.

M. Charlie Angus (Timmins—Baie James, NPD): Merci, messieurs. Vos récits ont été très très instructifs.

J'aimerais commencer par vous, monsieur Therrien. En 2008, la Clinique d'intérêt public et de politique d'Internet du Canada, la CIPPIC, a déposé sa plainte auprès de votre prédécesseur concernant Facebook. À l'époque, on a dégagé les applications de tierce partie comme représentant une menace pour la vie privée.

Dans le monde de 2008 — monde dans lequel je me trouvais bel et bien — on avait vraiment le sentiment qu'Internet était déréglementé — vous savez, on laissait faire les choses — et que Facebook était un endroit amusant où rencontrer des anciens copains de l'école secondaire. Dix ans plus tard, il est devenu la principale source de nouvelles — des fausses comme des vraies — et le principal joueur dans bien des élections à l'échelle internationale.

Compte tenu du fait que le contrôleur européen de la protection des données affirme que le contrôle dominant de Facebook se traduit par un extrémisme politique et un isolement croissants ainsi qu'une diversité de points de vue politiques, je veux vous poser une question, à la lumière de l'examen de 2008, sur les applications de tierce partie. Est-ce que les choses auraient été différentes si le commissaire à la vie privée avait haussé le ton? Disposiez-vous des outils nécessaires à l'époque pour composer avec ces atteintes à la vie privée? Et maintenant, eu égard à ce que nous voyons avec Cambridge Analytica, avons-nous besoin d'outils beaucoup plus efficaces pour traiter ces questions?

M. Daniel Therrien: Je devrais commencer par dire que l'une des choses que nous allons faire pour le moment sera d'examiner si le Facebook de 2018 continue de respecter les conditions auxquelles il a souscrit en 2008 et 2009. En 2008-2009, mon bureau — qui, bien sûr, était dirigé par un autre commissaire — était convaincu que Facebook avait fait certaines choses pour se conformer aux recommandations formulées par le CPVP. Vous avez raison de souligner qu'il y a une certaine similitude entre les questions de l'enquête effectuée à l'époque, la situation actuelle et la formulation concernant l'utilisation de renseignements par des applications de tiers. Tout cela pour dire que nous allons réexaminer cette question.

La situation aurait-elle été différente si nous avions eu des pouvoirs accrus? À l'époque et encore maintenant, tout ce que le CPVP peut faire, ce sont des recommandations. Il ne peut pas ordonner quoi que ce soit. Il aurait assurément été utile d'être en mesure d'imposer une certaine conduite. Est-ce que cela aurait empêché ces choses de se produire? Peut-être pas.

Je crois que la combinaison d'un certain nombre de mesures et de règles de consentement plus claires — de toute évidence, les règles en matière de consentement sont extrêmement nébuleuses, ce dont j'ai parlé dans mon rapport et dont vous avez parlé dans le vôtre — fait partie de la solution. Une autre partie importante de la solution, c'est le fait que l'organisme chargé de la réglementation, le CPVP, doit être autorisé à inspecter les activités des sociétés de façon proactive — et pas seulement lorsqu'il y a une plainte — afin d'assurer que ces sociétés assument vraiment leurs responsabilités. Le fait d'avoir à attendre que des plaintes soient déposées signifie que le problème doit avoir été repéré par quelqu'un. Étant donné l'opacité du système, c'est quelque chose qui ne se produira pas souvent. C'est pour cela que je dis qu'une partie de la solution serait aussi d'être en mesure d'inspecter sans motifs et de procéder ainsi à certaines vérifications. Le pouvoir de rendre des ordonnances et d'imposer des amendes aurait aussi fait une différence. Cela aurait-il permis de tout éviter? Non.

● (0925)

M. Charlie Angus: Non. Je présume que mon inquiétude vient de ce que nous avons vu, de ces allégations en provenance du Myanmar, ainsi que des allégations et des questions soulevées en Islande au sujet de l'appli Facebook qui repérait les gens qui devaient aller aux urnes le jour de l'élection, une appli qui a eu une incidence énorme sur le système électoral. Une élection provinciale est en cours en Ontario. Mon fil de nouvelles Facebook est rempli de pubs qui, je peux le voir, ne proviennent d'aucun parti politique. Et pourtant, il y a bien quelqu'un qui les a mises là.

Que le cadre de la protection de la vie privée soit suffisant ou non, Facebook semble se voir comme étant au-dessus des États. Nous faudrait-il un cadre juridique plus vaste et plus robuste qui engagerait, peut-être, la commission électorale, et qui prévoirait des normes médiatiques particulières pour remédier à la prolifération des fausses nouvelles? En ce qui concerne la protection de la vie privée, la crainte vient du fait que l'on soit en mesure de cibler des personnes pour ensuite les abreuver de fausses nouvelles. C'est l'allégation qui a été formulée dans le cadre du Brexit et au Nigeria. On reproche à ces personnes d'être en mesure d'influencer sérieusement les électeurs par l'intermédiaire de leur réseau d'amis.

Vous n'avez pas les pouvoirs voulus pour endiguer ce phénomène. Comment une nation peut-elle mobiliser ces monopoles gigantesques et les forcer à se montrer responsables?

M. Daniel Therrien: Vous avez raison de le dire: il y a beaucoup d'aspects dont il faut tenir compte — ce que j'appellerais des domaines de réglementation. Que cela se fasse par l'intermédiaire d'une seule loi ou de plusieurs lois, je laisse cela à votre discrétion, mais je suis certes d'accord avec vous pour dire que les géants technos actuels jouent sur un certain nombre de tableaux qui sont assujettis à de nombreuses lois. Vous avez parlé de protection de la vie privée et du processus électoral, et je crois que cela touche aussi à la question des monopoles. Ces sociétés existent-elles pour offrir un service public? Au contraire, sont-elles des entités qui recueillent des renseignements dans le but de donner un service tout en dégageant un certain profit? C'est là une autre question.

Toutes ces questions sont pertinentes. Elles sont toutes pertinentes, et il faut répondre à chacune d'elles. Du point de vue de la mécanique, je ne sais pas exactement comment procéder, mais je crois qu'il est important que nous nous penchions sur chacune d'elles. Les organismes de réglementation devraient être en mesure de se parler entre eux, car ces questions recoupent bien des domaines.

M. Charlie Angus: Diriez-vous que c'est quelque chose que notre comité devrait examiner pour veiller à ce que nous ayons une loi qui défend l'intégrité démocratique et les droits des citoyens face aux monopoles numériques? À votre avis, est-ce un sujet que notre comité devrait examiner et au sujet duquel nous devrions faire des recommandations?

● (0930)

M. Daniel Therrien: Oui, bien sûr.

M. Charlie Angus: Merci.

Le président: Merci, monsieur Angus.

Les sept prochaines minutes sont pour M. Saini.

M. Raj Saini (Kitchener-Centre, Lib.): Monsieur Therrien, monsieur Vickery, bonjour. Merci beaucoup d'être là, surtout vous, monsieur Vickery. Je ne suis pas vraiment une personne matinale, alors je ne perds pas de vue qu'il n'est que 6 h 30 chez vous, en Californie.

Monsieur Therrien, j'aimerais commencer par vous. Différents rapports ont été publiés sur le nombre de profils Facebook qui ont été touchés. M. Wylie a avancé le chiffre de 50 millions. Facebook a parlé de 87 millions. Pouvez-vous nous dire combien de comptes Facebook ont été touchés par cette fuite au Canada?

M. Daniel Therrien: Pour le moment, nous nous basons sur les données fournies par Facebook. Facebook a expliqué les différents chiffres qui circulent par le fait qu'il ne sait pas lui-même le nombre exact de comptes qui ont été touchés. Je crois que le chiffre de 87 millions renvoie au nombre de personnes qui utilisent l'application, le questionnaire, qui est à l'origine de cela, selon les allégations.

M. Raj Saini: Alors, ce questionnaire dont vous parlez...

Pardon.

M. Daniel Therrien: Puis, ils font des projections pour calculer combien d'amis ont pu être touchés à leur tour. En fait, il s'agit d'une réaction en chaîne, alors même Facebook ne sait pas exactement combien de personnes ont été touchées.

M. Raj Saini: Selon les rapports, la société qui a mené ce sondage a eu accès aux données — ou les a téléchargées — des 270 000 personnes qui ont répondu, et il semble que l'on a calculé une moyenne de 322 ou 332 amis par personne pour arriver à ce chiffre de 87 millions. Quoi qu'il en soit, vous vous fiez à Facebook, mais vous n'êtes pas certains à 100 % du nombre de profils de Canadiens qui ont été touchés.

M. Daniel Therrien: Pas pour l'instant. Bien entendu, au cours de notre enquête, nous allons essayer de déterminer ce chiffre avec plus de précision.

M. Raj Saini: Facebook a dit qu'il allait envoyer des avis aux Canadiens touchés par cette fuite. Savez-vous si tous les Canadiens ont reçu cet avis, oui ou non?

M. Daniel Therrien: Je ne le sais pas. C'est commencé, mais je ne sais pas si c'est terminé. Quoi qu'il en soit, c'est commencé.

M. Raj Saini: D'accord.

Vous avez également déclaré dans les médias que vous comptiez participer à l'enquête en Colombie-Britannique et collaborer avec le bureau du commissaire à la protection de la vie privée qui est là-bas. Nous savons qu'au cours des dernières semaines, le commissariat à l'information du Royaume-Uni, à Londres, en Angleterre, a fait une descente dans les bureaux de Cambridge Analytica. Nous savons que cette intervention se traduira par la rétention ou la découverte de grandes quantités de renseignements. Auriez-vous la possibilité de travailler avec le commissariat à l'information du Royaume-Uni et d'accéder à l'information qui a été découverte, ce qui faciliterait votre propre enquête au Canada?

M. Daniel Therrien: Nous disposons de pouvoirs robustes qui nous permettent, dans le cadre d'enquêtes, d'échanger des renseignements avec d'autres organismes de protection de données, tant au Canada qu'à l'étranger. Or, comme nous le savons tous, ce qui nous manque à la fin de l'enquête, c'est le pouvoir de rendre des ordonnances et d'imposer des amendes, au besoin. Cependant, les pouvoirs que nous avons pour obliger la production d'éléments de preuve et pour échanger des renseignements avec d'autres organismes de protection de la vie privée sont adéquats.

M. Raj Saini: Monsieur Zimmer, me reste-t-il encore du temps? D'accord.

M. Daniel Therrien: Cependant, en ce qui concerne la question qu'a soulevée M. Angus à propos des nombreux domaines de réglementation en cause, dont celui de la concurrence, disons qu'il y a des lacunes. Par exemple, je peux échanger de l'information avec le commissariat à la protection de la vie privée du Royaume-Uni, mais pas le Bureau canadien de la concurrence.

M. Raj Saini: D'accord. C'est un bon point.

Monsieur Vickery, j'ai beaucoup de questions à vous poser, mais je n'ai malheureusement pas beaucoup de temps. Je vais donc commencer par vous en poser une.

Des rumeurs circulent sur le fait que Cambridge Analytica conserverait AggregateIQ afin de contourner certaines lois britanniques. Pouvez-vous nous dire ce que vous pensez de cela et, peut-être, formuler des observations plus générales au sujet du travail qui se fait en sous-traitance dans le but de contourner les lois de certains pays, notamment lorsqu'il s'agit de campagnes qui se déroulent à l'étranger? Le Kenya pourrait aussi être cité en exemple.

M. Chris Vickery: Ce que je peux dire à ce sujet, c'est qu'il n'y avait aucune facture, aucun reçu ni quoi que ce soit de semblable dans le dépôt GitLab que j'ai téléchargé. Il n'y avait pas de reçus ou de papiers potentiellement incriminants où l'on aurait écrit « nous avons payé tel montant à telle personne ». Je peux cependant vous faire part de ce que j'ai retenu de mes lectures et de tout ce que j'ai examiné et cru. Un bon exemple de l'argent qui a circulé entre Cambridge Analytica et AggregateIQ est la mise au point de la plateforme Ripon qui est survenue au début de la campagne présidentielle de Ted Cruz, en 2016. L'équipe de Ted Cruz croyait que l'argent qu'elle payait pour ce produit — sa mise au point, le service connexe, etc. — allait à Cambridge Analytica, alors que c'est AggregateIQ qui travaillait là-dessus. C'est AggregateIQ qui faisait tout le travail, mais les chèques, eux, étaient adressés à Cambridge Analytica.

Cela vous donne-t-il une idée de la façon dont l'argent cheminait?

● (0935)

M. Raj Saini: Vous avez parlé de cryptomonnaie. Croyez-vous que la cryptomonnaie peut être utilisée pour dissimuler les transactions financières entre les entités qui se servent de ces renseignements?

M. Chris Vickery: C'est une possibilité. Je tiens à souligner que je n'ai aucune raison de croire qu'il y a eu blanchiment d'argent, mais j'estime qu'il serait utile d'examiner cela de plus près.

M. Raj Saini: D'accord.

Je sais qu'UpGuard a produit un rapport où il décortique les activités d'AggregateIQ. J'ai essayé de le lire, mais malheureusement, je ne comprends pas le code. Pouvez-vous nous en faire un résumé?

M. Chris Vickery: De quel rapport parlez-vous? Nous en avons produit quatre jusqu'ici.

M. Raj Saini: Je crois que c'est la quatrième partie.

M. Chris Vickery: C'est le plus récent. C'est celui qui porte sur la politique canadienne et d'autres sujets connexes. Ce rapport a confirmé les noms présents. Ce n'est pas parce que le nom d'un candidat apparaît dans un projet sur lequel AggregateIQ travaillait que ce candidat faisait nécessairement quelque chose de répréhensible, ou que quoi que ce soit d'illégal a eu lieu. Ils ont peut-être été mêlés à AggregateIQ sans qu'il y ait la moindre malveillante. Quelqu'un aura peut-être proposé leur nom ou quelque chose du genre. Néanmoins, nous avons effectivement repéré des projets qui contenaient des noms, dont ceux de Todd Stone, Andy Wells et Doug Clovechok. Les verts de la Colombie-Britannique y avaient quelques dossiers. Je crois qu'une bonne partie de ces informations ont déjà été mises au jour par les médias canadiens. Si nos rapports ne sont pas parvenus à brosser un portrait suffisamment clair, il y a probablement plusieurs articles où l'on explique les différents degrés d'engagement des personnes visées.

Le président: Merci, monsieur Saini.

Passons maintenant à M. Gourde, pour cinq minutes.

[*Français*]

M. Jacques Gourde (Lévis—Lotbinière, PCC): Merci, monsieur le président.

Ma question s'adresse à vous, monsieur Therrien.

Il y a environ deux semaines, je vous ai entendu dire, dans une entrevue que vous avez accordée à un média national francophone, qu'il y avait une zone grise liée à l'information recueillie par les partis politiques. J'aimerais bien obtenir des clarifications à ce sujet.

Tous les politiciens et tous les partis politiques reçoivent la liste électorale, où figurent le nom et le prénom du citoyen, son adresse complète, un numéro permanent d'électeur et l'emplacement du bureau de vote. Tout le monde y a accès, non seulement les partis politiques, mais aussi les candidats qui se présentent dans une circonscription, qu'ils soient des candidats indépendants ou non. Toutefois, au grand désarroi de tous ces politiciens, aucun numéro de téléphone ne figure sur cette liste.

À l'époque où nous étions tous plus jeunes, il était relativement facile de trouver un numéro de téléphone à l'aide du bottin téléphonique, car 80 % des gens qui étaient abonnés à un réseau téléphonique fixe y étaient inscrits. Lorsque nous voulions appeler quelqu'un, nous n'avions qu'à chercher son nom dans ce bottin. Par la suite, nous pouvions ajouter son numéro de téléphone à la liste électorale.

Monsieur Therrien, les numéros de téléphone des Canadiens sont-ils maintenant considérés comme étant une information relative à la vie privée? Ne devraient-ils pas être accessibles aux partis politiques, ou s'agit-il d'un cas relevant d'une zone grise? Il y a les réseaux téléphoniques fixes et il y a aussi les réseaux de téléphones cellulaires. Or, les numéros de téléphone cellulaire sont de plus en plus difficiles à trouver. Le numéro de téléphone du réseau fixe est public, mais celui du téléphone cellulaire ne l'est pas.

M. Daniel Therrien: Que les partis politiques veuillent communiquer avec les électeurs, il n'y a évidemment rien de mal là-dedans. Cependant, pour répondre à votre question précise visant à savoir si les partis devraient avoir accès aux numéros de téléphone ou à d'autres renseignements personnels, je dirai que la notion de consentement devrait entrer en jeu, compte tenu des principes relatifs à la vie privée. Si le numéro de téléphone d'un individu n'est pas public et que cet individu ne veut le divulguer à personne, y compris à un parti politique, il devrait être possible pour lui de garder ce numéro confidentiel.

● (0940)

M. Jacques Gourde: Il y a donc une distinction à faire entre les numéros de téléphone du réseau fixe, que l'on peut retrouver dans n'importe quel bottin téléphonique, et ceux du réseau cellulaire.

Pouvons-nous présumer que l'inscription des numéros de téléphone dans le bottin téléphonique signifie qu'elle a été autorisée au préalable?

M. Daniel Therrien: C'est un renseignement public.

M. Jacques Gourde: Le numéro de téléphone cellulaire n'est donc pas considéré comme étant un renseignement public?

M. Daniel Therrien: Certains sont publics et d'autres ne le sont pas; cela dépend de la décision d'un individu de donner ou non son consentement.

M. Jacques Gourde: Pour obtenir le consentement d'une personne, il faut lui téléphoner. Si nous n'avons pas un numéro de téléphone pour joindre la personne, que pouvons-nous faire? Il faudrait aller la voir?

M. Daniel Therrien: Euh! Oui.

M. Jacques Gourde: Vous comprendrez que cela représente un grand défi: il faudrait joindre 85 000 électeurs en 40 jours de campagne électorale, sans compter le fait que des personnes ne sont pas sur place toute l'année. Cela fait à peu près 2 500 portes par jour auxquelles frapper, ce qui est humainement impossible, même avec une équipe de 15 personnes. Il faut bien prendre le temps de parler aux gens!

Le problème de base qui se pose pour les personnes désireuses de s'engager en politique est celui de ne pas pouvoir accéder à un minimum d'information sur les électeurs. On utilise donc des moyens technologiques afin d'obtenir une idée de leur allégeance. On ne se le cache pas: si on veut avoir leur numéro de téléphone, c'est pour les appeler, même si on peut toujours aller les voir. Au bout du compte, l'information que les politiciens veulent obtenir est celle de savoir s'ils peuvent compter sur leur soutien. Si la personne dit clairement qu'elle soutient un certain candidat, celui-ci va conserver l'information, et il va par la suite s'assurer que cette personne ira voter le jour du scrutin. Les listes des partis politiques s'allongent au fil des années, et l'on peut toujours les utiliser si, bien sûr, l'information consignée est à jour. Il y a malgré tout une marge d'erreur.

Si des Canadiens décident de faire de la politique et qu'ils n'ont pas accès à un minimum d'information, pouvons-nous leur reprocher d'utiliser des moyens qui leur feront gagner du temps et connaître au plus tôt les tendances de vote?

M. Daniel Therrien: En fait, je vous dirais de vous attaquer au problème d'accès à un minimum d'information. Vous dites que la liste électorale ne vous permet pas d'obtenir le minimum d'information nécessaire, si je comprends bien, pour être capable à tout le moins de communiquer avec une personne et de vérifier si elle va vous appuyer ou pas. Revoir ce qui constitue un minimum d'information me semble la solution plutôt que de trouver d'autres moyens de communiquer avec un individu.

Au bout du compte, il y a d'une part la notion du consentement, mais je conçois parfaitement que le désir des partis de vouloir communiquer avec les électeurs soit extrêmement légitime et qu'il peut leur être nécessaire d'obtenir un minimum de renseignements pour ce faire.

M. Jacques Gourde: Je reviens à la zone grise. Ne serait-ce pas plus équitable de permettre, sur le plan législatif, que ces numéros soient distribués à l'ensemble des partis politiques et à tous ceux qui se présentent dans les circonscriptions? On pourrait peut-être retirer les numéros de téléphone de la zone grise et rendre l'information accessible à tout le monde.

Une personne qui se présente comme candidat indépendant, par exemple, et qui n'a jamais fait de recherche, peut utiliser la liste des noms, prénoms et adresses, mais elle n'aura jamais le temps de trouver les numéros de téléphone. Elle est donc vraiment désavantagée par rapport à tous ceux qui représentent des partis politiques depuis 25, 30 ou 40 ans.

Ne croyez-vous pas que ce serait plus juste de donner au moins la même information de base à tout le monde pour que tous soient sur un même pied d'égalité au début d'une campagne électorale?

M. Daniel Therrien: Il semble que ce soit le cas. Je ne suis pas un expert en la matière, mais je comprends que tous les partis possèdent certains renseignements qui proviennent de la liste électorale.

Vous dites que ces renseignements ne vous donnent pas le minimum d'information nécessaire pour que vous puissiez communiquer avec les électeurs. Alors, c'est une question qui se pose et qui peut être étudiée. Vous pourriez examiner cette question.

Par ailleurs, quand j'ai parlé d'une zone grise, c'était dans le sens où, n'ayant pas compétence pour vérifier comment les partis utilisent les renseignements, je ne sais pas ce qui se passe. Les partis se dotent de politiques de protection de la vie privée afin d'assurer un minimum de règles dans leurs relations avec les électeurs. Cependant, ni moi ni aucune autre personne indépendante ne peut vérifier ce qui se passe. Alors, c'est ce que je voulais dire par « zone grise », une zone où il n'y a pas d'arbitre indépendant qui peut s'assurer que les règles qui sont mises en place sont respectées.

[*Traduction*]

Le président: Merci, monsieur Gourde.

Le prochain sur la liste est M. Baylis, pour cinq minutes.

M. Frank Baylis (Pierrefonds—Dollard, Lib.): Monsieur Therrien, monsieur Vickery, merci d'être là.

Lorsqu'il est question de données, il semble que nous ayons une question fondamentale à nous poser en tant que société, à savoir ce que nous allons autoriser et ne pas autoriser. Il incombe au gouvernement d'établir les règles et de ne pas permettre à chaque entreprise de décider comment et quand les données doivent être utilisées.

Pour que je puisse bien comprendre de quoi il retourne, ma question s'adresse à vous deux. Mais d'abord, permettez-moi de vous rappeler que la mise en marché ciblée a toujours existé. Je viens tout juste de faire une recherche sur Michael Dell de Dell Computers. Avant de devenir un magnat de l'informatique, Michael Dell vendait des journaux. Il parcourait les bases de données sur les personnes nouvellement mariées ou qui venaient de déménager. Il a connu un succès retentissant alors qu'il n'était encore qu'un adolescent. Aujourd'hui, je pourrais me procurer ces données dans Facebook, par exemple. Si je voulais vendre des journaux comme cela se faisait autrefois, je chercherais à savoir qui vient de déménager et qui vient de se marier. La mise en marché ciblée est quelque chose que nous avons déjà permis.

Maintenant, en ce qui concerne la vente de données — encore une fois, cela n'a rien à voir avec Facebook —, disons que je fais des dons à des organismes caritatifs, et je sais que certains d'entre eux communiquent mes coordonnées à d'autres organismes caritatifs, car c'est une bonne façon de taper une deuxième fois sur le même clou. Il arrive qu'ils demandent la permission de faire ces échanges, mais ce n'est pas toujours le cas. Ce partage de données à des fins commerciales et ce ciblage ont été permis. Ces deux choses ont été permises dans le passé. Facebook rend le processus beaucoup plus efficace. Si j'étais un parti politique, disons le Parti vert, je dirais que toute personne qui affiche plein de choses sur des questions environnementales serait une bonne personne à cibler aux fins de dons ou de conversion.

J'aimerais vous poser cette question fondamentale. Sachant que ces pratiques ont déjà cours, que devrions-nous permettre et que devrions-nous nous abstenir de permettre? En tant que gouvernement, comment devrions-nous baliser ce comportement?

Commençons par vous, monsieur Therrien. Ensuite, ce sera au tour de M. Vickery.

● (0945)

M. Daniel Therrien: Je ne crois pas qu'il y ait de réponse courte à cette question, mais s'il y en avait une, je dirais que nous avons fait tout ce que nous avons pu pour arriver avec une réponse raisonnable dans le cadre de l'étude que nous avons réalisée pour le rapport sur le consentement. S'ajoute à cela les recommandations et les mesures que nous misons de l'avant à cet effet. Je crois que votre comité a bonifié substantiellement ces dispositions dans le rapport qu'il a présenté en février. Alors, c'est une partie de la réponse, réponse qui comporte une série d'éléments.

M. Frank Baylis: Sur le plan philosophique, devrions-nous permettre... Par exemple, je vous demande si nous devrions dire: « Regardez, je vous donne ces données, mais vous ne pouvez les utiliser qu'à telle fin. Je fais un don. Je suis dans votre base de données, mais je ne vous permets pas de les communiquer à d'autres. » Je pourrais aussi vous permettre de le faire.

Sur le plan philosophique, ce que je donne m'appartient-il ou pas?

M. Daniel Therrien: À cet égard, je crois que la réponse est que les renseignements personnels sont une chose sur laquelle les gens devraient être en mesure d'exercer un contrôle. Vous présentez cela sous l'angle de la propriété, et c'est un aspect qui est parfois évoqué. Je préfèrerais parler d'un droit de la personne; la protection de la vie privée est un droit de la personne. Vous devriez être en mesure de contrôler votre vie privée et, par conséquent, l'information que vous permettez que l'on communique à autrui et à quelle fin. Le partage doit se faire parce que vous en avez décidé ainsi et parce que vous pensez que cela va vous apporter quelque chose, ce qui est bien différent du fait de donner son consentement à des fins extrêmement vastes en des termes qui prêtent flanc aux interprétations de chacun selon ses desseins.

M. Frank Baylis: Alors, d'un point de vue philosophique, vous ramèneriez cela à la formulation du consentement. Je vous cède ces données, mais je les assortis de paramètres indiquant ce que vous pouvez en faire et ce que vous devez vous abstenir d'en faire.

M. Daniel Therrien: Oui, une formulation appuyée par des règles de droit — c'est là le rôle qui incombe au gouvernement — en vue de garantir le respect de ce concept philosophique.

M. Frank Baylis: Oui, nous définirons les détails techniques. Une fois que nous aurons déterminé ce que nous souhaitons faire, nous pourrons creuser la question et établir, par exemple, votre droit d'enquêter, votre droit d'imposer des amendes, etc.

Je m'entends avec vous pour dire qu'il faut appliquer ces règles même aux partis politiques. Toutefois, ce sera un détail, une fois que nous aurons décidé ce que nous souhaitons faire.

Monsieur Vickery, qu'en pensez-vous? Vous évoluez constamment dans cet univers.

M. Chris Vickery: Je pense que les gens qui peuvent bénéficier de la diffusion des données seront fortement incités à les diffuser. En cédant un peu de terrain, non seulement nous nous retrouverons sur une pente glissante, mais il est couru d'avance que cette diffusion survienne dans une grande mesure. Et, ce n'est qu'une question de temps avant que les partis politiques, les développeurs de listes commerciales et les groupes de surveillance des consommateurs s'entendent entre eux et s'offrent mutuellement d'importantes sommes d'argent pour échanger leurs données.

Ce que je pourrais suggérer à titre d'éventuel compromis, ce serait de décider d'accorder à tous un droit de propriété sur leurs propres données. S'il s'agit de donner à un organisme de bienfaisance le droit ou la permission de communiquer vos données à un autre organisme de bienfaisance du même genre, je ne crois pas qu'il soit déraisonnable de s'attendre à ce que le premier organisme de bienfaisance vous envoie un courriel pour vous indiquer ce qu'il planifie de faire et pour vous demander si vous êtes d'accord — « Cliquez ici pour partager vos données » — ou à ce qu'il vous envoie au moins un avis pour vous informer de la transmission de vos données. Alors, rien ne serait fait en cachette ou clandestinement; tout serait connu; le consentement aurait été donné, et il y aurait une trace écrite.

● (0950)

M. Frank Baylis: Merci.

Le président: Le prochain intervenant est M. Kent, qui dispose de cinq minutes.

L'hon. Peter Kent: Merci, monsieur le président.

Je vous remercie, monsieur le commissaire, d'avoir remarqué le rapport unanime et les recommandations que le Comité a adressés au gouvernement en février. Nous espérons que le gouvernement les a consultés, comme vous l'avez fait.

L'une des recommandations de ce rapport, une recommandation que vous avez faite de diverses manières indirectes, c'est de travailler avec les organismes de réglementation de la protection de la vie privée de l'Union européenne. Dans quelques semaines seulement, le RGPD de l'Union européenne, le Règlement général sur la protection des données, entrera en vigueur. Il protège pratiquement tous les éléments de données des citoyens de l'ensemble de l'Europe, de leurs renseignements de base — leur numéro d'assurance sociale, dans le contexte canadien — à l'ensemble de leurs activités sur les réseaux sociaux, en passant par tous leurs renseignements personnels, les ordinateurs qu'ils possèdent, leurs numéros de téléphone, etc.

Est-ce que le scandale de Facebook, le scandale de Cambridge Analytica, les agissements d'AIQ, tous les sujets dont nous discutons aujourd'hui, et le fait que l'intelligence artificielle, qui a apporté de grands bienfaits à la société, à l'humanité, bien qu'en même temps, des gens se soient hâtés de développer de nouveaux programmes sans songer à prendre des précautions et à mettre en oeuvre des mesures de protection..? Est-il temps pour le Canada d'envisager de mettre au point quelque chose comme le RGPD pour protéger la vie privée de ses citoyens contre toutes les atteintes, allant des plus minimes aux plus compliquées, que ce soit des algorithmes, des stéréotypes ou de l'exploitation?

M. Daniel Therrien: Il est grand temps que le Canada légifère à cet égard. J'ai fait valoir cet argument maintes fois. Le RGPD, c'est-à-dire le règlement européen, est certainement une bonne norme à laquelle nous comparer, mais je crois qu'il importe que chaque pays conçoive ses propres lois. Certaines règles pourraient différer pour des raisons culturelles ou constitutionnelles, mais le modèle européen est excellent. J'ai formulé plusieurs recommandations en m'inspirant de ce modèle.

Le point principal est qu'il est grand temps — plus que temps — de légiférer à cet égard.

L'hon. Peter Kent: Merci.

Monsieur Vickery, vous avez effleuré ce sujet à plusieurs reprises en répondant précédemment à des questions, mais y a-t-il un moyen technique d'empêcher la multiplication ou l'accroissement des données personnelles des utilisateurs de médias sociaux, par l'entremise de leurs amis, et leurs listes téléphoniques et leurs comptes Facebook, si ces utilisateurs décident de ne pas autoriser le partage de leurs données? Ou la question se résume-t-elle à avoir bon espoir que les sociétés de médias sociaux auxquelles les utilisateurs accordent leur confiance respecteront les engagements qu'elles prennent ou non en ce moment ou que la réglementation les obligera à prendre dans les années à venir?

M. Chris Vickery: J'ai à la fois une réponse positive et une réponse négative à vous donner à ce sujet.

Je vais commencer par la réponse négative. Il n'y a aucune façon de garantir que toute donnée ou toute série de caractères que vous saisissez ou qui peut se rapporter à vous ne sera pas transmise plus tard à une autre entreprise. Les données se multiplient. J'observe constamment ce phénomène. Il n'y a simplement aucune façon d'empêcher cela, car elles sont trop prolifiques.

Toutefois, j'ai une idée à vous suggérer pour tâcher de contenir la quantité de données qui se multiplient sur Internet à n'importe quelle fin. Cette suggestion consiste à adopter des lois ayant du mordant. Ces sociétés ne géreront pas d'énormes bases de données si elles savent qu'elles représentent une énorme responsabilité et qu'elles pourraient menacer leurs résultats financiers. Ce n'est que lorsque les organismes de réglementation seront en mesure d'imposer des amendes qui peuvent nuire aux profits de ces sociétés et à la valeur de leurs actions qu'elles respecteront les termes de la réglementation.

● (0955)

L'hon. Peter Kent: Il faudrait donc quelque chose dans la même veine que, par exemple, le RGPD qui prévoit des pénalités et des amendes atteignant jusqu'à 20 millions d'euros, ou l'équivalent de 4 % des revenus de l'entreprise en question? Certaines de ces entreprises génèrent plusieurs milliards de dollars de revenus.

M. Chris Vickery: Je ne peux pas parler précisément des chiffres et des calculs qui conviennent, mais je crois que ces nombres sont dans la même veine que ce à quoi je faisais allusion et que, oui, la réglementation doit avoir du mordant pour vraiment attirer l'attention des cadres supérieurs. Le RGPD a grandement polarisé l'attention des cadres supérieurs.

L'hon. Peter Kent: Merci.

Le président: Merci, monsieur Kent.

La prochaine intervenante est Mme Fortier.

[*Français*]

Mme Mona Fortier (Ottawa—Vanier, Lib.): Merci beaucoup.

Messieurs, je vous remercie d'être ici aujourd'hui.

Monsieur Therrien, vous êtes devenu un habitué. C'est comme si vous étiez un chouchou à *Tout le monde en parle* et que vous aviez votre carte. Je vais commencer par vous, parce que je veux vraiment comprendre l'exercice que nous faisons présentement et, surtout, celui que vous faites de votre côté.

Comme vous le savez, le Comité a décidé à l'unanimité d'étudier également la violation apparente des données Facebook par Cambridge Analytica, mais sans compromettre votre propre enquête.

Je suis curieuse de savoir de quelle façon vous caractérisez la violation de la vie privée dans ce cas-ci. Si j'ai bien compris les commentaires que vous avez formulés récemment, vous estimez que les règlements en vigueur ont laissé une trop grande latitude à Facebook en matière de collecte de données personnelles et que cela a créé des conditions suffisantes pour que Cambridge Analytica utilise ces renseignements de manière illégale ou contraire à l'éthique.

Pourriez-vous caractériser la violation de la vie privée que vous étudiez présentement?

M. Daniel Therrien: À cause de l'enquête qui est en cours et de nos obligations juridiques, dont la plus importante consiste à ne pas tirer de conclusions avant d'avoir terminé cette enquête, j'apporterais une nuance à vos propos.

Les conclusions que vous m'attribuez seraient davantage fonction de ce que nous observons de façon générale, en tant que représentants d'une agence de réglementation, quant au comportement de l'ensemble des compagnies et aux lois qui s'appliquent à ces dernières. Nous constatons tous les jours que les politiques de protection de la vie privée sont très permissives en ce qu'elles permettent une utilisation très large des renseignements, ce qui n'est pas toujours compatible avec un consentement éclairé.

Peut-on dire que Facebook a violé la vie privée en s'appuyant sur les faits allégués? Nous allons certainement nous pencher sur la question. Notre enquête est en cours et nous ne pouvons pas encore tirer de conclusions. Par contre, je peux vous dire quelles questions nous allons examiner, sans pour autant parler des conclusions à venir au sujet de cette affaire.

De façon générale, nous nous demanderons si les deux compagnies au sujet desquelles nous enquêtons, soit Facebook et AggregateIQ, ont violé la loi fédérale relative à la protection de la vie privée et, dans le cas de la Colombie-Britannique, la loi provinciale.

Plus précisément, nous allons nous pencher sur la question de savoir si les politiques relatives à la protection de la vie privée adoptées par Facebook étaient effectivement trop permissives et si elles ont joué un rôle dans l'utilisation ultérieure des renseignements par des firmes d'analyse de données, entre autres, pour donner des conseils qui ont pu être utiles ou non à des formations politiques.

Nous allons aussi tenter de déterminer, comme je l'ai dit plus tôt, si les recommandations qu'a faites le Commissariat avant que j'arrive en poste en 2009 sont toujours applicables en 2018.

Finalement, nous allons regarder le rôle joué par AggregateIQ dans tout cela et comment cette compagnie a recueilli les renseignements. Cela a-t-il été fait en conformité avec les lois? Nous considérerons surtout le type d'analyse de données qui a été fait. Le produit final qui a été communiqué aux formations politiques était-il conforme aux lois sur la protection de la vie privée?

Toutes ces questions sont pertinentes, et nous les examinerons. Je ne peux évidemment pas tirer de conclusions à l'heure actuelle.

● (1000)

Mme Mona Fortier: Je comprends, merci beaucoup.

Vous menez votre enquête de votre côté, mais notre comité accueillera pour sa part les représentants de Facebook plus tard cette semaine. Selon vous, y a-t-il des questions particulières que nous devrions leur poser? Avez-vous des suggestions à faire au Comité?

M. Daniel Therrien: Oui.

Sur le plan factuel, comment est-ce que Facebook s'assure qu'une tierce partie, soit les personnes qui effectuent la recherche, obtient les renseignements personnels de ses utilisateurs de façon conforme au consentement donné par ces derniers et aux exigences en matière de respect de la vie privée?

De plus, comment est-ce que Facebook protège les données de ses utilisateurs contre quiconque voudrait les utiliser à des fins indues ou non autorisées? Je pense ici à des pirates malintentionnés, ce que l'on appelle des *bad hackers* en anglais.

Enfin, la semaine dernière, M. Zuckerberg a déclaré que le temps était venu pour Facebook d'avoir une réglementation appropriée. Alors, que signifie cela pour Facebook, compte tenu notamment de nos recommandations — au Commissariat à la protection de la vie privée du Canada —, des recommandations du présent comité et des règlements européens?

Mme Mona Fortier: Merci beaucoup, monsieur Therrien.

[*Traduction*]

Le président: Merci, madame Fortier.

Le prochain intervenant est M. Angus, qui dispose de trois minutes.

M. Charlie Angus: Merci.

Monsieur Vickery, nous avons commencé par composer avec une atteinte à la protection de 85 millions de comptes Facebook qui pourrait avoir chamboulé la plus importante élection européenne de la génération actuelle. Puis vous prenez la parole ce matin, et vous mentionnez en passant que les renseignements de 48 millions de personnes supplémentaires, y compris des données très personnelles, pourraient avoir été violés.

Je sais que c'est probablement un événement sur lequel vous enquêtez encore, mais était-ce une atteinte à Facebook?

M. Chris Vickery: Non, à ce que je sache en ce moment, c'est un événement complètement distinct.

Une partie de mon travail vise à mettre en évidence la prévalence de ce type d'atteintes à la protection des renseignements personnels. Ces atteintes se produisent beaucoup plus fréquemment que les gens en ont conscience. Ce sont des problèmes que je rencontre constamment. Il est très difficile de me surprendre ces temps-ci. Les gens ne semblent avoir aucune idée de la fréquence de ces énormes atteintes à la protection des renseignements personnels.

M. Charlie Angus: Au cours de la prochaine série de questions, je donnerai suite à mes interrogations en mettant encore plus l'accent sur la question de l'attaque contre la base de données et sur le rôle qu'AIQ a joué dans celle-ci. Toutefois, vous avez indiqué que la base de données était ouverte, qu'il suffisait d'y accéder. J'imagine que si vous cherchez ce genre de fuites, d'autres personnes doivent faire de même. Je veux dire, il y a des armées de trolls russes, des cybermenaces et des bandes criminelles. Cette base de données pouvait-elle être exploitée par d'autres personnes? Vous avez mentionné le danger que présentaient d'autres acteurs. Auriez-vous l'obligeance de nous fournir plus de renseignements sur le danger que pourrait faire peser sur nous l'accès à ces données par d'autres acteurs?

M. Chris Vickery: Oui. Tous les renseignements personnels auxquels j'ai pu porter atteinte — et que, par la suite, j'ai veillé à faire sécuriser avant d'en parler dans des rapports publics — étaient entièrement ouverts à toute personne ayant accès à Internet. Il n'y avait aucun code d'utilisateur ou mot de passe à saisir, ni d'autres mesures de protection à contourner.

Pour en arriver à la question que vous m'avez posée, je crois, la réponse est oui. Si j'ai trouvé tout cela par moi-même — je travaille avec une équipe ces temps-ci mais, relativement parlant, j'ai trouvé tout cela seul —, il serait extrêmement étonnant que des nations adverses ne consacrent pas d'énormes ressources à faire la même chose à des fins malveillantes.

M. Charlie Angus: Nous allons aborder ce sujet au cours de ma prochaine série de questions, mais le problème ne se résume pas au fait que les utilisateurs de Facebook ont été privés des données provenant de l'application qu'ils ont utilisée à partir de Facebook. Le problème est également lié au fait que des agents politiques comme AIQ ou Cambridge Analytica ont la capacité d'utiliser Facebook — c'est-à-dire la plateforme — pour déformer les nouvelles ou influencer les électeurs.

Pourriez-vous parler de la façon dont Facebook est utilisé non seulement pour accéder à des renseignements, mais aussi pour introduire de l'information?

● (1005)

M. Chris Vickery: Oui. Pour commencer à répondre à cette question, je tiens à indiquer clairement que j'ai constaté que l'utilisation et l'exploitation potentielle d'applications offertes sur Facebook étaient un problème très répandu, en passant en revue la zone grise des usages qu'on peut en faire. J'ai découvert au cours du week-end que l'une des applications de Facebook liées à AggregateIQ — son nom figure sur l'application à titre de racleur — a été classée dans la catégorie « Jeux » des applications de Facebook. Je crois que personne n'a encore mentionné cette application. Il y a probablement un grand nombre…

M. Charlie Angus: Cette application peut-elle encore être utilisée?

M. Chris Vickery: Ces applications ont été suspendues de la plateforme Facebook. Par conséquent, je crois qu'elle n'est plus en service, mais l'identificateur de l'application figure toujours dans le code que j'ai trouvé.

Voilà la réponse à la première partie de votre question. Pouvez-vous me rappeler la teneur de sa deuxième partie?

Le président: Quatre minutes se sont écoulées maintenant

M. Charlie Angus: Quatre minutes?

Le président: Oui, croyez-le ou non.

M. Charlie Angus: Vraiment ? Je pense que vous trichez, monsieur le président.

Des voix: Oh, oh!

Le président: Le temps passe simplement vite.

M. Chris Vickery: Je suis désolé. J'essaierai d'être plus bref.

Le président: Cela ne pose pas de problème, car vous apportez un précieux témoignage.

Nous allons amorcer une toute nouvelle série de questions. À la fin des interventions, j'essaierai de réserver 10 minutes pour aborder la question des travaux du Comité. Je vais donc tenter cette fois d'être légèrement plus strict avec vous à propos du respect des temps de parole.

Nous allons commencer par Mme Vandenbeld, qui dispose de sept minutes.

Mme Anita Vandenbeld (Ottawa-Ouest—Nepean, Lib.): Merci.

J'aimerais vous remercier tous les deux d'être parmi nous. Vous nous avez communiqué beaucoup d'information aujourd'hui. Ce que nous souhaitons vraiment, c'est trouver des solutions, des mesures que nous pouvons prendre en tant que législateurs, parce que je crois qu'une grande partie de ces problèmes sont très alarmants pour nos électeurs et pour les Canadiens, en général.

Je veux m'assurer que je comprends exactement la nature du problème. Monsieur Vickery, vous avez mentionné que les données se multipliaient. Donc, en fait, vous ne pouvez éviter cela, mais vous pouvez limiter ce phénomène. Vous avez également déclaré que ces fuites se produisaient constamment. À mon avis, il s'agit là d'une très mauvaise combinaison de circonstances. D'une part, il y a la question de l'utilisation légitime des données. Disons qu'en faisant du porte-à-porte, les membres d'un parti politique rencontrent quelqu'un qui déclare: « j'aime beaucoup votre plateforme relative à la garde d'enfants. Pour cette raison, je vais voter pour votre parti ». Ces membres prennent note de ce fait afin que, la prochaine fois que le parti prend des mesures liées à la garde d'enfants, ils puissent le faire savoir à cette personne. Même si cette personne donne son consentement en déclarant, « oui, veuillez me tenir au courant des développements de cette nature », vous disposez maintenant de cette information qui sera ajoutée à la base de données par la suite. Ce qui me préoccupe, ce n'est pas tellement le fait que le candidat puisse visiter de nouveau la personne et lui dire, « voyez la merveilleuse politique que nous avons établie », mais plutôt le fait que ce renseignement puisse être communiqué accidentellement ou malicieusement à, disons, l'entreprise Toys"R"Us, laquelle pourrait dire, « Ah!, puisque cette personne est préoccupée par la garde d'enfants, vendons-lui des jouets ».

Est-ce le scénario que nous examinons? Est-ce la nature du problème, ou, au contraire, craignons-nous que l'entreprise Toys"-R"Us parvienne, d'une façon ou d'une autre, à avoir accès à ces données politiques... ou examinez-vous les produits que l'entreprise Toys"R"Us vend aux enfants, ou le fait qu'elle tire des conclusions lorsque quelqu'un montre qu'il a des enfants sur Facebook? Le problème est-il donc lié à l'utilisation des données à des fins contradictoires?

M. Chris Vickery: Cela se produit dans les deux directions. Les données politiques finissent par servir aux entreprises commerciales ou aux entreprises de marketing, et les données sur le comportement des consommateurs que recueille Toys"R"Us ou une entreprise, quelle qu'elle soit, finissent par servir à des fins électorales.

Je ne crois pas que le recours au porte-à-porte pour recueillir des données soit réellement problématique. Il est impossible d'accroître le nombre de visites de façon exponentielle, car les gens sont limités par le temps et l'espace.

Je ne sais pas à quoi ressemble la législation canadienne sur les armes à feu mais, aux États-Unis, nous partons du principe qu'il est acceptable d'être propriétaire de certaines armes à feu. Par contre, nous n'autorisons pas les civils à posséder des mitraillettes. Le même genre de principe s'applique ici. Vous pouvez tolérer que des gens frappent aux portes pour recueillir un par un les numéros de téléphone des résidents ou n'importe lequel de leurs renseignements mais, lorsque la situation s'apparente davantage à l'effet d'une mitraillette, en ce sens que vous envoyez, entre autres, des milliers de questionnaires, de courriels et d'annonces sur Facebook, et que vous collectez des renseignements privés — ou, du moins, des renseignements personnels — de façon massive auprès de plusieurs milliers de fois plus de personnes que vous pourriez le faire normalement, cette pratique devient dangereuse.

Mme Anita Vandenbeld: Ce qui me préoccupe, c'est ce dont vous parliez. Je crois que vous avez indiqué que des fuites se produisaient constamment. Même si vous souhaitiez limiter la campagne afin qu'elle demeure locale et circonscrite… ne serait-ce que les renseignements que vous conservez ou dont une entreprise commerciale garde la trace, les achats des gens dans leur magasin, ou des données à des fins publicitaires… lorsqu'une fuite survient accidentellement...

Nous ne parlons pas d'une mesure législative stipulant que vous devez envoyer des avis lorsque vous partagez des renseignements avec telle ou telle organisation, parce que bon nombre de ces organisations n'auront même pas conscience de partager cette information, qui se trouve à un endroit où quelqu'un d'autre peut y avoir accès. En réalité, il me semble que le problème se situe au niveau global, au niveau où d'autres organisations sont en quête de renseignements, qu'elles combinent, puis vendent. En réalité, c'est sur ce niveau que nous devons nous concentrer, sur la vente de quantités massives de renseignements qui proviennent peut-être de plusieurs sources différentes.

● (1010)

M. Chris Vickery: Dans une certaine mesure, c'est vrai, mais je crois qu'il vaudrait également la peine de se pencher sur la source des données. Bon nombre de fuites se produisent parce que les entreprises ignorent volontairement leur situation en matière de sécurité. Elles n'exercent aucune surveillance. Elles savent que leurs activités sont rentables et ne cherchent donc pas à déceler les problèmes. Toutefois, ces problèmes existent, et d'autres personnes en tirent parti, mais ces entreprises ne tiennent pas à le savoir. Rien ne les incite à repérer une atteinte à la protection de leurs données parce que, le cas échéant, il leur incombera de résoudre le problème.

Nous devons les inciter à rechercher les problèmes et punir les organisations qui ne sont pas disposées à intensifier leurs efforts.

Mme Anita Vandenbeld: En nous appuyant simplement sur ce que vous avez dit à propos de la cryptomonnaie, nous constatons que nous avons affaire à un tout autre niveau qui comprend peut-être des organisations clandestines, des États-nations ou des criminels qui pourraient tenter d'exercer ces activités à d'autres endroits où nous ne sommes pas en mesure de légiférer, des endroits où ils sont peut-être en train de collecter ces données ou de les utiliser à des fins très répréhensibles. Il nous est pratiquement impossible d'adopter des lois pour prévenir cela.

Y a-t-il des moyens de le faire ou, comme vous l'avez dit, faut-il vraiment se préoccuper des lieux où les données sont recueillies et stockées, et s'assurer que les organisations sont incitées à mettre en oeuvre des mesures de sécurité à ce niveau?

M. Chris Vickery: La bonne nouvelle, c'est que ces données ne peuvent servir à des fins malicieuses que si elles sont exactes et continuellement mises à jour, tout comme c'est le cas pour une utilisation légitime. Si nous arrivons à couper l'accès au flux de données à jour, les données qui sont en possession des fraudeurs finiront, avec le temps, par être largement inutilisables.

Mme Anita Vandenbeld: Dans ce cas, est-ce qu'une partie de la solution serait de faire en sorte que les entreprises prennent la protection des renseignements personnels plus au sérieux? J'aimerais aussi savoir ce que vous entendez par « exception d'intérêt légitime ». C'est l'autre point que j'aimerais clarifier avec vous.

M. Daniel Therrien: Je suis d'accord avec M. Vickery; la solution réside dans la somme des mesures appliquées. Compte tenu de votre mandat, il serait peut-être indiqué d'explorer les utilisations légitimes de ces données, afin de communiquer en toute légitimité avec les électeurs. Les préoccupations à cet égard vont dans les deux sens, c'est-à-dire les données recueillies à des fins politiques qui sont utilisées à des fins commerciales, et vice versa. Il faut se pencher là-dessus, mais j'ajouterais un léger bémol: bien que cela mérite notre attention, tout échange d'information n'est pas nécessairement inapproprié. Sachant que les partis politiques doivent communiquer avec les électeurs, qu'ils doivent les connaître pour leur servir des arguments convaincants, est-ce nécessairement une mauvaise chose d'évaluer les habitudes d'achat d'une famille, qu'on parle de jouets ou autres?

Je ne suis pas un expert en matière d'élections, et je ne m'avancerais pas sur ce qui va à l'encontre ou non de l'intégrité du processus, mais je regarde le tout d'un point de vue théorique. Les partis doivent pouvoir communiquer intelligemment avec les électeurs, et pour cela, ils doivent savoir à qui ils s'adressent. Donc, l'analyse des données peut être correcte en partie, mais cela ne justifie absolument pas tout. Et les allégations concernant Facebook et Cambridge Analytica sous-entendent certainement une utilisation inappropriée des données à des fins politiques. Je veux seulement préciser que certaines utilisations peuvent être légitimes.

Pour ce qui est des intérêts légitimes, ce n'est pas ce qu'on a avec Facebook et Cambridge Analytica. Si les lois sur la protection des renseignements personnels devaient être resserrées, il faudrait s'assurer qu'elles ne viendraient pas gêner l'innovation qui s'appuie sur une utilisation légitime et responsable. J'ai répondu à M. Baylis tout à l'heure que la valeur à défendre avant tout est celle du consentement, soit la capacité de chacun de contrôler ses renseignements personnels. Dans le monde moderne, toutefois, ces renseignements peuvent être utilisés à différentes fins, et il n'est pas toujours possible d'informer leur détenteur de toutes les utilisations qu'on en fera. Les données sont utilisées à bon escient dans le cadre de certaines initiatives d'intelligence artificielle, par exemple.

Le défi consiste entre autres à établir des règles strictes qui font généralement en sorte que le consentement est respecté. Mais dans le monde des mégadonnées et de l'intelligence artificielle, il est possible qu'on doive prévoir une exception à la règle du consentement. En Europe, cette exception d'intérêts commerciaux légitimes permet de justifier le traitement légal des données en l'absence d'un consentement. Je crois qu'une loi bien équilibrée favoriserait le consentement, d'une part. D'autre part, nous devons nous interroger sur ce qu'il est acceptable d'obtenir au Canada sans nécessairement avoir le consentement de la personne — cela peut être dans le secteur de la santé —, pourvu que ce soit dans une optique commerciale ou sociale appropriée, et dans l'avantage véritable de la société.

● (1015)

Le président: Merci, monsieur Therrien.

Pour sept minutes, la parole est maintenant à M. Gourde.

[*Français*]

M. Jacques Gourde: Merci, monsieur le président.

Ma question s'adresse à M. Vickery.

Lors de la dernière élection présidentielle américaine, relativement serrée, la candidate qui avait remporté le vote populaire a perdu, alors que le candidat qui aurait dû, selon certains, arriver deuxième dans les suffrages a réussi à gagner en récoltant une majorité des votes du collège électoral, peut-être grâce à une publicité plus ciblée.

La semaine passée, le fondateur de Facebook a expliqué que la raison d'être de sa compagnie, son modèle d'affaires, était de vendre de la publicité. Et Facebook le fait très bien, étant notamment capable de cibler des régions, voire des rues ou des édifices: si quelqu'un habite dans tel édifice, il va recevoir telle publicité.

À titre d'exemple, je suis propriétaire d'un véhicule Mazda et, comme par hasard, Facebook m'envoie tous les jours une publicité de Mazda sur mon fil Facebook. On voit donc que Facebook cible les publicités de façon extrêmement efficace. Il est probable que les partis politiques américains ont recours à Facebook pour diffuser de la publicité dans certains secteurs, dans certains États ou dans certaines parties d'États où les électeurs sont susceptibles de leur être plus favorables et donc de voter pour eux.

Pensez-vous que les partis politiques américains, tant les Démocrates que les Républicains, ont effectué un certain profilage électoral ou recouru aux services de compagnies ayant analysé la meilleure façon de cibler les publicités ou d'influencer les Américains dans certains États? Serait-il possible d'en conclure que la personne ou le parti qui a été le plus efficace dans sa campagne publicitaire sur Facebook a remporté l'élection américaine?

[*Traduction*]

M. Chris Vickery: Je précise d'emblée que je ne suis aucunement affilié ni à l'un ni à l'autre des partis, mais je peux vous affirmer que tous les cas de violation des données sur les électeurs que j'ai recensées récemment aux États-Unis — en ce qui concerne le milieu politique et tous les systèmes d'influence que j'ai examinés — étaient attribuables à une intervention du Parti républicain. Je n'ai jamais découvert de système d'ultraciblage et d'influence sélective qui aurait été employé par le Parti démocrate. Il en existe peut-être un, mais comme je n'ai rien vu de tel, je ne peux pas dire que c'est ce qui se passe du côté des démocrates. Une chose est sûre, le Parti républicain a effectivement eu recours à des techniques d'ultraciblage, à des compilations de bases de données disparates et hypervariées, et de sources parfois assez inattendues. Il a colligé le tout à son grand avantage et de façon très efficace, afin de dénicher des personnes d'influence et d'autres influençables et de leur envoyer des messages ciblés dans un objectif très précis.

● (1020)

[*Français*]

M. Jacques Gourde: Merci.

Monsieur Therrien, il semble que l'entreprise Cambridge Analytica ait eu accès aux données de 650 000 utilisateurs canadiens de Facebook. Si ces utilisateurs canadiens avaient été des électeurs indécis, auraient-ils pu être influencés et, compte tenu de notre système électoral canadien, cela aurait-il pu déterminer l'issue d'une élection relativement serrée?

M. Daniel Therrien: Je pense qu'il s'agit d'environ 620 000 utilisateurs. Je ne suis pas un expert en matière électorale, mais ce nombre est de toute évidence important. Je pense donc que la réponse à votre question est oui.

M. Jacques Gourde: Dans votre enquête, serez-vous capable de déterminer si ces 620 000 utilisateurs étaient éparpillés partout au Canada ou si certaines circonscriptions étaient visées? C'est parce que 620 000 personnes ciblées dans 90 circonscriptions ont beaucoup plus d'influence que si elles sont réparties dans 338 circonscriptions. Nous pourrions peut-être découvrir quelque chose que personne n'avait encore vu.

M. Daniel Therrien: C'est une question que je vais certainement prendre en note.

Notre point de départ est davantage la question de la finalité. Notre enquête va se concentrer sur l'usage de renseignements d'utilisateurs de Facebook — un réseau qui sert essentiellement à communiquer avec des amis — à des fins d'analyse en appui à des buts politiques.

Vous nous suggérez de pousser notre travail à un niveau de détail qui ne serait probablement pas nécessaire pour nos objectifs, mais qui pourrait être utile. Nous allons en tenir compte, mais je pense que cette question serait plus du ressort de M. Perrault, à Élections Canada.

M. Jacques Gourde: Si Facebook offrait à un parti politique de diffuser de la publicité sur Facebook et que, une semaine avant l'élection, elle lui fournissait une liste de 620 000 Canadiens ayant regardé cette publicité au sujet de son chef, cela ne voudrait pas dire que le vote de ces Canadiens serait acquis ou que ceux-ci auraient l'intention de voter. En revanche, si comme par hasard, une deuxième publicité du parti était diffusée, laquelle inciterait les personnes à voter en fonction des valeurs du parti, par exemple, et que cela apparaissait trois, quatre ou cinq fois par jour sur leur page Facebook au cours de la semaine précédant l'élection, cela pourrait-il avoir une incidence, surtout si ces personnes avaient déjà dit avoir regardé la publicité auparavant? Ce serait plus que du profilage. Cela deviendrait tendancieux.

M. Daniel Therrien: Cela peut certainement avoir une conséquence sur le plan électoral. Je vous encourage donc à considérer ces questions. Quand vous me décrivez cette situation, je pense surtout au fait que l'usager de Facebook a fourni des données à cette entreprise essentiellement pour communiquer avec certaines personnes, mais certainement pas pour recevoir la veille de l'élection de la publicité l'encourageant à voter pour telle ou telle raison.

En ce qui concerne les principes entourant la vie privée, dans le scénario que vous nous décrivez, le consentement semble avoir été interprété de façon excessive. Pour ce qui est de savoir si cela aurait des conséquences sur le plan électoral, je répondrais que ce serait probablement le cas, même si ces questions ne sont pas de mon domaine.

[*Traduction*]

Le président: Votre temps est écoulé, monsieur Gourde. Le temps file.

Notre prochain intervenant, pour sept minutes, est M. Angus.

M. Charlie Angus: Monsieur Vickery, tentons de jouer à « suivre les données ». Il y a SCL, il y a GSR, et il y a Cambridge Analytica. GSR produit une application Facebook à des fins de recherche scientifique, amasse quelque 86 millions de profils, et vend toutes ces données pour des miettes — peut-être pour le prix de deux canettes de Coke — à Cambridge Analytica. Facebook l'apprend et lui demande de supprimer l'information, et l'entreprise accepte. Et soudainement, AggregateIQ, une entreprise de Victoria dont personne n'a entendu parler, et qui n'a même pas de site Web, obtient 40 % du budget du camp du oui pour diriger la campagne menant au Brexit.

Êtes-vous en mesure de nous dire si l'information tirée de Facebook, qui devait être supprimée, est celle qui se retrouve dans la base de données d'AggregateIQ?

● (1025)

M. Chris Vickery: J'aimerais éclaircir certains malentendus qui pourraient persister. Les données obtenues par les applications Facebook, de même les renseignements tirés des sondages menés sur Mechanical Turk d'Amazon — GSR a eu recours à bien des moyens pour recueillir des données et les associer plus tard à des profils Facebook —, ne sont pas nécessairement utiles après avoir servi à la modélisation, à l'analyse et à l'élaboration des outils comportementaux. Quand vous avez compris les interactions et que vous savez comment faire réagir les gens à l'aide de certains messages, les données brutes de Facebook peuvent bien être supprimées. Elles ne servent plus à rien. Il suffit par la suite d'appliquer ce même cadre à des données axées sur les élections pour obtenir les résultats voulus, car le modèle a déjà fait ses preuves avec les données des médias sociaux.

Alors non, je n'ai pas vu des données clairement tirées de Facebook dans cette base. Cela ne veut pas dire qu'elles n'y ont jamais été, mais...

M. Charlie Angus: Vous avez dit que les données avaient aussi pu provenir d'Amazon?

M. Chris Vickery: Il faut savoir que le système Mechanical Turk d'Amazon est une plateforme qui sert à rémunérer des gens pour remplir des sondages. C'est un des moyens employés par GSR pour obtenir ce type de données. Les données ont été associées aux profils Facebook, mais c'est le système Mechanical Turk d'Amazon qui a été utilisé pour y arriver.

M. Charlie Angus: D'accord. Alors, quel est le lien entre les deux? Cambridge Analytica et AggregateIQ affirment être deux entités totalement distinctes. Je répète qu'AggregateIQ a obtenu 40 % du budget de la campagne du camp du oui. Christopher Wylie dit que cette entreprise a essentiellement servi d'outil de propagande et de blanchiment d'argent pour Cambridge Analytica. Quelle base de données permet de connecter les deux?

M. Chris Vickery: Une des premières connexions entre Cambridge Analytica et AggregateIQ est que les deux ont obtenu le logiciel original pour la plateforme Ripon d'un serveur au nom d'Alexander Nix, le PDG sortant du groupe SCL de Cambridge Analytica. C'est ce qu'indique le code, de même que les commentaires des employés. Il y a donc là un lien direct entre les deux.

Une des applications conçues par AggregateIQ est une plateforme téléphonique de messages d'approche communautaire, visant à influencer les électeurs. Elle logeait sous le nom de domaine « dclisten.com », aussi enregistré au nom d'Alexander Nix. Ce n'est pas les exemples qui manquent de ressources et de biens passant d'un groupe à l'autre.

M. Charlie Angus: Lorsque AggregateIQ a obtenu 40 % du budget de la campagne du oui du Brexit, le seul site Web recensé pour l'entreprise était celui d'Alexander Nix, qui travaille pour SCL et qui siège au conseil d'administration de Cambridge. N'était-ce pas le site Web de SCL-AggregateIQ?

M. Chris Vickery: Le seul site Web actif de l'entreprise à ce moment-là? Je ne connais pas l'historique de ce site Web. Je ne pourrais pas vous dire.

M. Charlie Angus: D'accord.

Les rumeurs veulent qu'AggregateIQ soit impliqué dans nombre de processus électoraux, et les allégations de Christopher Wylie sont très troublantes, à l'effet qu'il règne une culture d'illégalité. Il a entre autres fait allusion à la collecte illégale de données brutes sur les utilisateurs de fournisseurs d'accès Internet à Trinité-et-Tobago. Avez-vous été en mesure de confirmer ces allégations?

M. Chris Vickery: Les allégations concernant Trinité-et-Tobago...

M. Charlie Angus: Oui, auprès de fournisseurs Internet. N'y avez-vous pas fait référence sur Twitter?

M. Chris Vickery: Je crois que nous sommes en possession de preuves qui confirment ces allégations. Nous n'avons pas encore tiré nos conclusions finales, mais effectivement, il y a un projet à Trinité-et-Tobago qui s'appuie sur des renseignements qui permettent d'identifier un grand nombre d'utilisateurs.

● (1030)

M. Charlie Angus: Vous pouvez affirmer qu'AIQ, cette base de données, contient des renseignements bruts obtenus auprès de fournisseurs d'accès Internet à Trinité-et-Tobago?

M. Chris Vickery: Je ne sais pas si les renseignements ont été obtenus auprès de fournisseurs Internet ou autrement...

M. Charlie Angus: Cela peut être par d'autres moyens, oui.

M. Chris Vickery: ...nous n'avons pas encore tiré nos conclusions finales, mais oui, il y a des données permettant d'identifier...

M. Charlie Angus: D'accord. Permettez-moi de reformuler ma question. La base de données d'AIQ contenait des renseignements qui auraient pu influer sur le résultat des élections à Trinité-et-Tobago.

M. Chris Vickery: Oui, absolument.

M. Charlie Angus: Très bien, merci.

Vous avez parlé de la cryptomonnaie et des réseaux publicitaires que ces groupes mettaient en place. Cela me préoccupe, car Christopher Wylie a entre autres affirmé que les élections n'étaient pas la véritable vache à lait. C'est surtout après qu'il y a de l'argent à faire. Il a parlé de la possibilité d'influencer le gouvernement, si le bon gouvernement est en place. Pensez-vous que la base de données d'AggregateIQ soit encore utilisée à des fins commerciales, en vue de servir d'autres intérêts?

M. Chris Vickery: C'est une possibilité.

Je tiens à souligner que je vois davantage AggregateIQ comme une division d'une plus grande entité. Je comparerais cela au département de développement d'une grande entreprise.

M. Charlie Angus: Quelle est cette grande entreprise?

M. Chris Vickery: Il est probable que ce soit SCL. Les objectifs et les résultats finaux des deux entités sont parallèles.

M. Charlie Angus: Merci.

Le président: Merci, monsieur Angus.

La parole est à M. Picard pour sept minutes.

[*Français*]

M. Michel Picard (Montarville, Lib.): J'aimerais revenir sur le thème de notre étude, c'est-à-dire les renseignements que nous qualifions de personnels et ce que nous en faisons. Au-delà des différents scénarios possibles, je crois que l'utilisation de ces renseignements par une compagnie n'est qu'une dimension accessoire du problème essentiel que nous devons étudier.

J'ai deux questions, que je vais illustrer de deux scénarios. J'aimerais que vous me fassiez part de vos commentaires sur ma compréhension du problème en fonction de ces scénarios.

Mes questions sont les suivantes. Le rôle du gouvernement est-il de définir en détail ce qui constitue des renseignements personnels? Ou le rôle du gouvernement serait-il plutôt d'interdire toute transaction qui contient ces renseignements personnels?

Voici maintenant mes deux scénarios.

Dans le premier, je fais affaire avec un fournisseur de livres: la compagnie Amazon pour ne pas la nommer. Il est normal — et je m'y attends — que, dès l'achat de mon premier livre ou à l'occasion d'une visite subséquente, Amazon me suggère un certain nombre d'autres livres en fonction des préférences d'autres lecteurs ou acheteurs ou, plus simplement, en fonction de mon propre historique d'achats de livres chez Amazon. En établissant ma relation avec cette compagnie, je lui ai communiqué un certain nombre de renseignements personnels pour qu'elle me donne un service découlant de son expertise en la matière.

Voici mon autre scénario. J'ai la naïveté d'annoncer que, dans un mois, je partirai en croisière pendant une semaine. Il ne serait pas étonnant qu'un utilisateur qui lit mon fil Facebook et qui travaille dans une agence de voyage communique avec moi pour m'informer de certaines aubaines liées à des croisières. Il ne faudrait pas non plus que je m'étonne du risque de me faire cambrioler pendant mon absence annoncée d'une semaine. Tant le criminel que l'agent de voyage ont utilisé mes renseignements personnels, mais je les avais rendus publics. Ce sont des renseignements personnels que j'ai communiqués sur Facebook pour les diffuser à mes amis et abonnés, ce qui correspond au service qu'offre ce réseau social. J'ai donc rendu ces renseignements publics.

Je reviens à mes questions. Ces deux scénarios décrivent des situations réalistes. À qui revient-il de définir la granularité des renseignements personnels? Chaque type de compagnie va exiger différentes catégories de renseignements. Par ailleurs, dans la mesure où une transaction dépend de l'expertise de l'entreprise — comme Amazon — dont je suis client, je ne m'attends pas à ce que cette compagnie vende mes renseignements personnels à une autre société à des fins, notamment de sollicitation commerciale, autres que celles établies dans ma relation avec Amazon, c'est-à-dire l'achat de livres.

Quel serait selon vous le meilleur des deux rôles, ou devrions-nous plutôt envisager un mélange des deux?

Monsieur Therrien pourrait peut-être répondre en premier.

M. Daniel Therrien: Je vais renchérir sur vos questions. Si je les interprète mal, veuillez me le dire.

À la base, l'individu donne certains renseignements pour obtenir un service. Une des conséquences en est la communication de renseignements au moment de l'offre du service. Dans le cas d'Amazon, par exemple, la compagnie utilise les renseignements de gens qui vous ressemblent ou qui partagent vos intérêts, c'est-à-dire de personnes qui ont aimé tel ou tel livre. Je dirais que cela aussi, jusqu'à un certain point, c'est un renseignement personnel au sens de la définition du terme.

La conclusion qu'Amazon tire de vos intérêts, par exemple que vous aimez les romans policiers, résulte effectivement de vos renseignements personnels, mais cette conclusion elle-même est un de vos renseignements personnels: votre intérêt réel ou présumé pour les romans policiers est un renseignement personnel qui vous concerne.

Le rôle de l'État est de définir ce qu'est un renseignement personnel. À cet égard, je pense que la loi fait un travail correct, parce qu'elle ratisse très large et me permet l'interprétation que je vous donne.

Est-ce le rôle du gouvernement d'interdire l'utilisation de renseignements personnels? Non. Cette utilisation devrait être réglementée, mais ce ne devrait pas être interdite.

Ai-je répondu à votre question?

● (1035)

M. Michel Picard: Oui. Merci.

Monsieur Vickery, voulez-vous ajouter quelque chose?

[*Traduction*]

M. Chris Vickery: D'abord, je suis d'accord pour dire qu'il faut définir ce qui constitue des renseignements personnels. Les règles doivent être claires pour tout le monde; il ne doit y avoir aucune ambiguïté. Alors oui, je crois que les définitions doivent être claires et que tout le monde doit se conformer aux mêmes règles. L'utilisation qu'en fait Amazon n'est pas malicieuse; elle vise à offrir une meilleure expérience à l'utilisateur, et pas du tout à l'exploiter. Mais encore là, c'est une question d'interprétation...

Par contre, si vous publiez quelque chose sur Facebook, c'est un peu différent, parce que vous avez choisi de le faire. Facebook ne l'a pas fait pour vous. Vous l'avez vous-même publié sur votre mur Facebook. Il n'y a pas d'ambiguïté; vous avez choisi de le montrer au monde. Quand on diffuse un peu trop d'information, on peut s'attendre à recevoir quelques appels d'un agent de voyages. Vous allez peut-être vous abstenir à l'avenir, mais au départ, c'était votre décision. Ce n'est pas une entreprise qui a décidé de publier tout cela à votre place.

M. Michel Picard: Si une entreprise analyse mon fil de nouvelles des deux dernières années et conclut que j'ai telle ou telle habitude, et qu'un tiers entre en communication avec moi en fonction de mon contenu public, cela signifie qu'il n'y a pas eu d'intention malicieuse ni d'un côté ni de l'autre. L'utilisateur final n'a rien fait de mal; il n'a qu'utilisé le contenu mis à sa disposition.

M. Chris Vickery: C'est un terrain très glissant. Dites-vous que le contenu que vous choisissez de rendre public devrait être hors limite? Que n'importe qui peut faire n'importe quoi avec ce que vous publiez volontairement sur Internet? Les gestes posés par les entreprises par rapport aux données disponibles pourraient être mal perçus, et leur réputation pourrait en prendre un coup selon ce qu'elles choisissent d'en faire.

M. Michel Picard: Merci.

Le président: Merci, monsieur Picard.

M. Daniel Therrien: Monsieur le président, si je peux...

Le président: C'est tout le temps que nous avions, monsieur Therrien. Je suis désolé. Avez-vous un bref commentaire à formuler?

M. Daniel Therrien: Monsieur le président, j'aimerais expliquer brièvement la notion de données accessibles au public.

Il y a bien des aspects à considérer, mais il faut entre autres retenir ceci: la personne qui a rendu ses données accessibles au public savait-elle vraiment que c'est ce qu'elle faisait? Il s'agit encore une fois de bien informer les gens, de façon à ce qu'ils soient en mesure de donner leur consentement en toute connaissance de cause. Bien des gens n'ont aucune idée de ce qu'ils font. C'est une chose.

L'autre chose que je dirais rapidement, c'est qu'il existe actuellement une réglementation au Canada qui définit la notion de données accessibles au public. Ces définitions sont dépassées. Je vous encourage à les examiner.

● (1040)

Le président: Merci. Je sais que c'est difficile d'être bref avec ce sujet.

Monsieur Erskine-Smith, vous avez à peine 20 secondes, et si vous pouviez être plus rapide encore, ce serait merveilleux.

M. Nathaniel Erskine-Smith: Monsieur Vickery, vous avez dit avoir téléchargé les informations en question à partir de GitHub. Vous avez indiqué aujourd'hui qu'il pouvait être illégal d'utiliser des informations à des fins autres que celles pour lesquelles elles ont été recueillies. Avez-vous signalé la chose aux autorités concernées, y compris à notre commissaire à la protection de la vie privée? Sinon, seriez-vous prêt à le faire?

Le président: Rapidement, s'il vous plaît.

M. Chris Vickery: J'ai immédiatement communiqué avec les autorités fédérales de mon pays, et je suis tout à fait disposé à collaborer aux enquêtes pertinentes au Canada.

Le président: Merci, monsieur Vickery.

Nous allons faire une pause et discuter ensuite des travaux du Comité. Je prierais tous les invités de quitter la salle le plus rapidement possible. Je vous en serais très reconnaissant.

Encore une fois, merci à M. Vickery et à M. Therrien d'avoir témoigné devant nous aujourd'hui.

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