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 102 • 1re SESSION • 42e LÉGISLATURE

TÉMOIGNAGES

Le jeudi 26 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 jeudi 26 avril 2018

● (0845)

[*Traduction*]

Le président (M. Bob Zimmer (Prince George—Peace River—Northern Rockies, PCC)): Nous allons commencer la réunion de ce matin du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, la réunion numéro 102. Conformément au sous-alinéa 108(3)h)(vii), nous étudions l'atteinte à la sécurité des renseignements personnels associée à Cambridge Analytica et Facebook.

Ce matin, nous accueillons Colin J. Bennett, professeur au Département de science politique à l'Université de Victoria, et Thierry Giasson, professeur au Département de science politique à l'Université Laval, qui comparaissent tous les deux à titre personnel. Durant la deuxième heure, nous recevrons Marshall Erwin, de la Mozilla Corporation.

Nous allons commencer ce matin par la déclaration de M. Bennett.

M. Colin Bennett (professeur, Département de science politique, University of Victoria, à titre personnel): Merci, monsieur le président.

Pouvez-vous m'entendre?

Le président: Oui, nous vous entendons très bien.

M. Colin Bennett: Bonjour. Je suis ravi d'être à nouveau parmi vous et de comparaître avec mon collègue, M. Giasson.

Je suis professeur de sciences politiques à l'Université de Victoria. Depuis une trentaine d'année, j'étudie les questions relatives à la vie privée et je publie des ouvrages portant sur ces questions, au Canada et à l'étranger. En 2012, j'ai corédigé un rapport à l'intention du Commissaire à la protection de la vie privée sur l'utilisation des données personnelles par les partis politiques canadiens. Depuis, j'effectue des travaux de recherche sur la nature et l'influence des élections guidées par les données au Canada et à l'étranger et tente de sensibiliser les gens à leurs répercussions sur la protection de notre vie privée et d'autres valeurs démocratiques.

Le dossier controversé que vous étudiez à l'heure actuelle met en lumière un certain nombre de problèmes interreliés, qu'il importe de différencier. Il y a le pouvoir monopolistique conféré à des sociétés comme Facebook dans notre économie axée sur les plateformes, la collecte de renseignements sur les utilisateurs des réseaux sociaux par des applications tierces, les infractions aux limites de dépenses électorales, les questions entourant la transparence des publicités politiques ciblées, les cybermenaces à l'intégrité des élections, la grande question du rôle de l'analyse des mégadonnées dans les élections et, ce dont je veux vraiment parler aujourd'hui, le rôle des partis politiques dans les élections guidées par les données et leur lien avec notre régime de protection de la vie privée.

Cambridge Analytica et Aggregate IQ sont deux acteurs du vaste secteur de l'analyse des électeurs. De nombreuses autres sociétés, surtout des États-Unis, ont profité des normes moins rigoureuses en matière de protection de la vie privée dans ce pays et de leur capacité de traiter d'énormes quantités de renseignements personnels tirés de sources publiques et commerciales afin de cibler les consommateurs de manière plus granulaire.

On a fait tout un plat de l'importance des mégadonnées dans les élections, et de récents travaux scientifiques ont remis en doute l'influence réelle de l'analyse des données sur les résultats électoraux. Tout de même, la compétitivité caractéristique de la course électorale se solde toujours en une pression énorme sur les grands partis politiques de la plupart des démocraties pour qu'ils continuent d'avoir recours à l'analyse des données pour distancer leurs adversaires. De fait, un plus grand nombre de données sur les électeurs sont recueillies et ces données sont échangées à plus grande échelle au moyen d'un réseau vaste et compliqué d'organismes, dont des sociétés aux affaires douteuses qui jouent des rôles importants à titre d'intermédiaires entre les électeurs et les représentants élus.

Ce marché est plus restreint au Canada, mais compte tout de même une vaste gamme d'entreprises offrant des services de cette nature: sondages, analyse de données, élaboration de logiciels, annonces publicitaires numériques, campagne sur les médias sociaux, etc. Nous ne comprenons pas entièrement le rôle que jouent les données personnelles dans le processus politique canadien ni n'avons une réelle idée du marché. Je vais laisser le soin à mon collègue, M. Giasson, de vous en parler plus en détail.

J'ai suivi vos audiences avec grand intérêt. L'étude est un bon point de départ, mais ce n'est qu'un début, et nous devons effectuer de nombreuses autres analyses. J'aimerais soulever trois points généraux sur l'élaboration des politiques à l'avenir.

Mon premier point est l'importance cruciale d'arrimer la législation en matière de protection de la vie privée au règlement général sur la protection des données, le RGPD. La société Facebook a récemment décidé de transférer les données de ses utilisateurs non européens de l'Irlande aux États-Unis, clairement mue par un désir d'échapper aux règles plus restrictives du RGPD. Pour décourager cette recherche du ressort le plus favorable, il est primordial que le Canada relève ses normes pour que ce genre de comportement devienne impraticable. Le rapport que vous avez publié en février est un excellent premier pas.

Il est particulièrement important en matière de traitement des renseignements sur les politiques, qui sont qualifiées de données sensibles dans le RGPD, de prendre les mesures suivantes: premièrement, rendre les dispositions sur le consentement de la LPRPDE plus rigoureuses; deuxièmement, intégrer des dispositions sur la transparence des algorithmes, comme vous le suggérez; troisièmement, faire de la protection de la vie privée à dessein ou à défaut un principe législatif central dans la LPRPDE; quatrièmement, renforcer les pouvoirs en matière d'audit et de sanction du commissaire à la protection de la vie privée; et dernièrement, clarifier les diverses catégories de données personnelles de nature délicate, dont celles sur les opinions politiques.

Mon deuxième point est qu'il y a un besoin pressant d'assujettir les partis politiques à la législation canadienne en matière de protection de la vie privée. J'ai témoigné à ce sujet devant vous dans le passé. L'une des meilleures façons d'empêcher ce type d'abus que nous voyons à l'étranger est de fixer des règles claires et uniformes quant aux catégories de données auxquelles peuvent avoir recours les partis politiques dans le cadre de leur campagne électorale. Il faut établir des règles du jeu équitables qui interdiraient aux sociétés comme Cambridge Analytica de reproduire au Canada leurs pratiques telles que celles observées ailleurs.

● (0850)

Le Canada est l'un des seuls pays démocratiques avancés dont la législation en matière de protection de la vie privée ne vise pas les partis politiques. La majorité ne sont pas régis par la LPRPDE. Comme il ne s'agit pas d'organismes gouvernementaux, ils ne sont pas régis par la Loi sur la protection des renseignements personnels. Ils sont également en grande partie exemptés de l'application de la nouvelle loi antipourriel et de nombreux règlements concernant les abonnés exclus administrés par le CRTC. Il y a bien quelques règles afférentes à la protection de la vie privée et de la sécurité dans la Loi électorale du Canada, mais elles ne s'appliquent qu'aux listes d'électeurs et sont sans effet sur les autres sources de renseignements personnels.

Par conséquent, en ce qui concerne les partis politiques, les Canadiens n'ont pas les droits légaux qu'ils ont en ce qui concerne les organismes gouvernementaux et les activités commerciales.

De plus, bien que le commissaire à la protection de la vie privée puisse mener une enquête sur Facebook, il ne peut pas passer au crible les pratiques de nos partis politiques. Il lui est donc impossible de se faire une idée globale de la situation, comme peut le faire par exemple la commissaire à l'information du Royaume-Uni, et il fait l'objet d'une enquête par cette dernière.

Il y a quatre options législatives concernant la réglementation des partis politiques fédéraux: la Loi sur la protection des renseignements personnels, la Loi électorale du Canada, la LPRPDE et des mesures législatives distinctes. Il est nécessaire de procéder à une analyse juridique et constitutionnelle sérieuse des diverses options législatives, chaque approche ayant ses avantages et ses inconvénients. Je pourrai les passer en revue durant la période de questions, si vous voulez.

En revanche, il ne fait aucun doute que le statu quo est irrecevable. D'abord, le recours aux données personnelles dans le cadre des élections ne fera que gagner en publicité d'ici les élections fédérales de 2019, surtout en ce qui a trait au ciblage politique sur Facebook.

Ensuite, il convient de noter que les partis politiques doivent tout de même respecter la Loi sur la protection des renseignements personnels de la Colombie-Britannique. Le commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique s'attache d'ailleurs à examiner les pratiques des partis politiques de la province. Je crois comprendre que les partis politiques fédéraux sont aussi soumis à ce texte législatif dans la mesure où ils recueillent des renseignements sur les électeurs britanno-colombiens. Ainsi, si les partis fédéraux doivent se soumettre à la législation en matière de protection de la vie privée, qui va dans le même sens que la LPRPDE, il n'y a donc pas de motif raisonnable empêchant l'extension de ces pratiques à l'échelle du pays.

Enfin, j'ai aussi le sentiment que les partis fédéraux reconnaissent de plus en plus l'importance de souscrire à de bonnes pratiques de gestion des renseignements personnels pour leur propre intérêt et celui des citoyens.

Pour terminer, mon troisième point est que les partis politiques devraient s'autoréglementer pour améliorer leurs politiques et leurs pratiques en matière de protection de la vie privée. Le processus de modifications législatives ne se fera vraisemblablement pas du jour au lendemain. D'ici à ce que la législation ait été modifiée, il y a de nombreuses mesures que les partis peuvent adopter pour s'autoréglementer et rétablir la confiance du public à leur égard.

J'ai analysé les politiques en matière de protection de la vie privée de divers partis provinciaux et fédéraux, et nombreux sont ceux qui ont déjà pris un engagement en ce sens. J'ai remis ce document au Comité, et je crois savoir qu'il est en train d'être traduit.

La situation s'est quelque peu améliorée depuis notre rapport en 2012, mais il y a encore beaucoup à faire. Aucun parti ne s'est engagé clairement à respecter les 10 principes énoncés dans la norme nationale en matière de protection des renseignements personnels, la pierre angulaire de la LPRPDE.

Je ne comprends pas pourquoi les partis ne pourraient pas souscrire à ces principes et adhérer à un code de protection de la vie privée commun qui énoncerait en détail des protections nécessaires des renseignements personnels sous leur commande. C'est trop peu, mais, déjà, cela créerait des règles du jeu équitables. En 2013, le directeur général des élections a recommandé que le respect d'un tel code devienne une condition à l'obtention de la liste électorale. Il y a fort à parier qu'un parti ne s'imposera pas lui-même cette exigence. Il faudra donc le leadership du directeur général des élections et du Commissaire à la protection de la vie privée.

À mon avis, pour ce qui est des changements qui devraient être apportés, il devrait y avoir une plus grande transparence quant aux sources des données recueillies directement ou indirectement que saisissent les partis dans leurs systèmes de gestion des relations avec les électeurs; un engagement collectif que les partis n'achètent pas et n'achèteront pas auprès de sources commerciales des données nominatives; une entente quant à l'utilisation des plateformes de médias sociaux aux fins électorales, surtout en ce qui a trait aux robots automatisés; un engagement envers la reddition de comptes en matière de protection de la vie privée, dont la désignation de chefs de la protection des renseignements personnels, et une formation plus poussée sur la protection de la vie privée et la sécurité offerte aux employés et bénévoles; l'intensification des efforts visant l'octroi de droits d'accès et de mesures de correction aux particuliers; une meilleure gestion des listes internes de numéros exclus et leur tenue à jour; un engagement collectif d'offrir une option qui permettrait aux destinataires de se désabonner des envois de courriels ou de messages textes; une meilleure gestion de l'accès aux bases de données des partis; et la clarification des politiques quant aux mesures à prendre en réponse à une atteinte à la vie privée.

Aucune de ces mesures ne devrait être difficile ou controversée, et je pense que ce devrait être un dossier politique. Il incombe notamment aux partis politiques d'éduquer et de mobiliser l'électorat, mais ces derniers doivent savoir concilier leurs intérêts, leurs rôles et les droits à la vie privée des Canadiens.

● (0855)

Aucun organisme n'aime les atteintes à la vie privée — demandez à Facebook. Il faut plutôt réfléchir aux ramifications potentielles s'il fallait qu'un parti politique porte une atteinte majeure à la vie privée dans le cadre d'une campagne électorale.

Merci beaucoup de l'attention que vous m'avez accordée.

Le président: Merci, monsieur Bennett.

Nous allons maintenant entendre M. Giasson, pour 10 minutes, s'il vous plaît.

[*Français*]

M. Thierry Giasson (professeur titulaire, Département de science politique, Université Laval, à titre personnel): Monsieur le président et membres du Comité, je vous remercie de me recevoir.

Je m'appelle Thierry Giasson. Je suis professeur titulaire au Département de science politique de l'Université Laval. Je suis également directeur du Groupe de recherche en communication politique.

Je tiens à vous remercier de cette invitation à venir partager avec vous les conclusions de certains de mes travaux sur la collecte et l'utilisation que font les partis politiques des données tirées des médias et des outils numériques. Je tiens à souligner l'importance de la réflexion que vous avez initiée il y a quelques semaines dans la foulée des révélations médiatiques entourant l'affaire Cambridge Analytica et de ses possibles ramifications pour les citoyens du Canada.

Afin d'éviter de répéter des informations qui vous ont été présentées par mon collègue Colin Bennett, je vais limiter mon intervention à la présentation des pratiques de collecte et d'analyse de données numériques qu'emploient présentement les partis politiques au Québec et au Canada.

Plusieurs d'entre vous connaissent évidemment ces pratiques. Toutefois, comme vos travaux sont publics et que ces pratiques sont moins bien connues des citoyens canadiens, il me semble judicieux de les exposer à l'ensemble de nos concitoyens.

Ma présentation va aborder trois éléments.

Premièrement, je vais exposer certaines des pratiques courantes de collecte d'informations personnelles que mènent les partis politiques à des fins de marketing électoral et de communication politique. Je vais donc répondre à la question suivante: « Quelles sont les données personnelles qu'utilisent les partis politiques et comment sont-elles colligées? »

Deuxièmement, je vais présenter les objectifs qui sont liés à l'analyse de ces données, ainsi que les méthodes d'analyse qui sont privilégiées par les partis pour traiter ces données. Je vais ainsi répondre à la question suivante: « Pourquoi les partis analysent-ils les données des électeurs canadiens? »

En conclusion, je vais soulever certains risques que l'utilisation des données personnelles numériques des Canadiens fait courir à la démocratie de notre pays.

En premier lieu, quelles sont les données colligées par les partis politiques et comment sont-elles recueillies?

D'abord et avant tout, il est important de dire que la collecte et l'analyse de données personnelles sur les Canadiens que font les partis politiques s'inscrivent dans le processus de marketing politique qui s'est institutionnalisé au Canada depuis plus de 30 ans, mais qui a connu une accélération importante depuis près de 15 ans.

Le marketing politique implique une analyse très fine des composantes de la population afin de prendre des décisions électorales qui vont permettre d'identifier les circonscriptions électorales, mais aussi les segments de la population dans lesquels les partis vont investir de façon plus ciblée pendant la campagne électorale afin de générer des votes. Tout le processus a pour objectif d'aider les partis à faire des gains électoraux.

On fait donc du marketing politique pour produire une communication électorale mieux ciblée et, ultimement, pour gagner les élections. Plus les données sont précises et nombreuses, plus la qualité de l'analyse va être importante. Les partis ont commencé par mener leur marketing électoral à partir de données de sondages et de groupes de discussion, mais, depuis 10 ans, ces partis intègrent des données personnelles tirées du Web pour la principale raison que ces données sont géolocalisées.

En effet, quand une personne a un compte sur une plateforme de médias sociaux, elle inscrit souvent son code postal, par exemple, et ce renseignement permet de la localiser très précisément. Cela fournit aux partis politiques un très grand degré de précision, presque granulaire, sur les composantes de l'électorat. Ces multiples données sont intégrées dans des plateformes d'analyse qui sont ensuite traitées selon des procédures mathématiques ou algorithmiques. Nous en parlerons tout à l'heure.

Ainsi, les partis politiques recueillent les données personnelles des citoyens auprès de trois sources principales. Premièrement, quelques mois avant le déclenchement d'un scrutin, Élections Canada et les autres organismes provinciaux de réglementation électorale donnent accès aux partis à l'ensemble des données personnelles qui sont consignées dans la liste électorale. Cette liste comprend, entre autres, les noms et les adresses des citoyens. À ces premières données électorales, les partis combinent ensuite des informations agrégées qui proviennent non seulement de sondages nationaux d'opinion menés pour ces partis par des firmes spécialisées, mais aussi de rapports de recherche produits par des organisations comme Statistique Canada. Enfin, depuis 10 ans, les partis tirent également des informations personnelles des citoyens à partir d'Internet. Ces informations peuvent être fournies volontairement aux partis politiques ou obtenues à l'insu des citoyens.

D'une part, les partis politiques vont recueillir de l'information lorsque, par exemple, les électeurs leur fournissent leur adresse courriel, leur code postal ou leur numéro de téléphone lorsqu'ils visitent le site Web du parti ou qu'ils participent en personne à un événement partisan, ou quand ils signent une pétition en ligne que va faire circuler le parti sur un sujet précis.

Ces informations sont bel et bien accordées volontairement aux formations politiques par les citoyens. Néanmoins, l'usage que celles-ci en font demeure inconnu de la grande majorité de la population. Par ailleurs, comme l'a bien souligné mon collègue Colin Bennett, les partis ne sont pas tenus d'expliquer aux citoyens ce qu'ils vont faire précisément de ces données.

● (0900)

Ensuite, les partis peuvent recueillir de l'information sur les électeurs en étudiant les statistiques de circulation des internautes sur leurs comptes de médias sociaux. Toutes les grandes entreprises de médias sociaux, comme Facebook, Google et Twitter, offrent aux organisations qui sont de leurs clients de nombreuses informations statistiques agrégées sur les réactions que génèrent les messages que diffusent les partis sur les plateformes de médias sociaux. Ces entreprises offrent aussi des services-conseils aux partis politiques afin de développer des campagnes de communication ciblées qui visent certains sous-groupes.

Enfin, mais ce serait plus rare au Canada, les partis politiques peuvent aussi acheter des informations numériques personnelles sur les Canadiens par le biais d'entreprises spécialisées dans ce genre de transaction. Ces dernières vendent des données sur, par exemple, les habitudes de consommation ou le niveau d'endettement de clients de diverses entreprises. Ces courtiers en informations numériques sont des intermédiaires commerciaux qui génèrent des bases de données de diverses façons, plus ou moins légalement et presque toujours à l'insu des citoyens dont les informations sont vendues.

C'est ce que faisait notamment AggregateIQ, l'intermédiaire de l'entreprise Cambridge Analytica, en colligeant des informations personnelles sur les utilisateurs d'une application numérique liée à Facebook, données que Cambridge Analytica revendait ensuite à ses clients pour effectuer de la segmentation et du ciblage électoral.

Pourquoi les partis politiques font-ils ce genre de collecte et comment les données sont-elles analysées?

En tant que parlementaires et membres actifs de vos formations respectives, vous n'êtes pas sans savoir que les partis politiques canadiens sont confrontés à une baisse de leur financement et du nombre de leurs membres, tout comme à un électorat dont l'attachement partisan est plus flexible et qui est plus critique envers les institutions politiques.

Plusieurs stratèges que j'ai interrogés dans le cadre de mes recherches m'ont confié que les dirigeants des formations politiques canadiennes devaient désormais relever un défi organisationnel majeur afin de remporter des élections. Ils se sont tournés, au cours des 20 dernières années, vers le marketing électoral et la communication numérique pour tenter de générer de nouvelles ressources, qu'elles soient financières ou humaines.

L'intégration du marketing politique dans l'élaboration des campagnes électorales contemporaines au Canada se déroule également dans un contexte de transformations technologiques. La préparation électorale et le marketing politique se vivent maintenant dans un contexte de cohabitation entre des modes traditionnels et émergents d'organisation politique qui, vous le savez, sont réalisés sur une diversité de plateformes en ligne et hors ligne.

Influencés par l'innovation technologique déployée dans le cadre des campagnes présidentielles américaines de 2008, de 2012 et aussi de 2016, les partis politiques accordent maintenant un rôle prédominant aux outils numériques dans leurs opérations de planification électorale. Cela a mené à la création d'une nouvelle catégorie de stratèges politiques, qui sont des spécialistes en médias sociaux, des informaticiens, des mathématiciens et des ingénieurs en logiciel, toute une cohorte de spécialistes en analyse des données. Ces gens ne travaillaient pas pour les partis politiques il y a 15 ans, ou alors ils étaient responsables de créer des sites Web ou de diffuser du contenu, par exemple. Ils n'étaient pas nécessairement responsables de penser de façon concertée les campagnes électorales. Ces stratèges numériques sont maintenant au coeur des processus organisationnels et des campagnes électorales.

En 2004, le Parti conservateur du Canada a été la première formation à se doter d'un système d'analyse de l'électorat lié à une base de données constituée d'informations personnelles sur les électeurs canadiens. En prévision de l'élection de 2015, le NPD et le Parti libéral ont eux aussi créé des bases de données pour faire du ciblage, ainsi que de la collecte et de l'analyse de données sur les citoyens. Ils voulaient ainsi faire du profilage de segments par le biais d'algorithmes informatiques programmés pour relever la cooccurrence de caractéristiques sociodémographiques et politiques chez les électeurs dont les informations étaient colligées dans les bases de données.

Les partis recueillent maintenant ces informations sur les électeurs de façon permanente, en particulier par le biais de publicités sur le Web et par l'utilisation d'applications socionumériques comme Twitter ou Facebook. Les partis politiques paient ces entreprises pour avoir accès aux métadonnées de leurs abonnés. Les informations géolocalisées tirées des médias sociaux fournissent aux formations politiques les caractéristiques sociodémographiques des utilisateurs, leurs habitudes de fréquentation de la plateforme et ce qu'ils aiment ou partagent.

Le recours au marketing politique pousse par contre les partis à développer des programmes électoraux plus ciblés et plus individualisés. Le positionnement du parti répondra aux priorités d'électeurs précis. Ces cibles du parti seront identifiées lors de l'étude de marché et sélectionnées sur la base de leur potentiel de réaction positive. À titre d'exemple, cette approche de ciblage a mené les conservateurs fédéraux à présenter des engagements très spécifiques, comme le crédit d'impôt pour l'achat d'outils, destiné aux travailleurs manuels, la Prestation universelle pour la garde d'enfants ou l'élimination du registre fédéral des armes d'épaule.

Ici encore, les technologies numériques contribuent à une communication hyperciblée des messages. Le ciblage de sa communication électorale assurera au parti que ses messages atteindront les micropublics auxquels ils sont exclusivement destinés.

● (0905)

Toutes les actions qui sont menées en ligne, y compris la collecte et l'analyse de données numériques personnelles sur les Canadiens, ont donc pour finalité de permettre aux partis d'entrer en contact direct avec les électeurs et de les persuader d'aller voter. Vous comprenez donc que l'obsession de la victoire électorale domine toujours et encore les actions des partis, incluant la collecte et l'utilisation des données personnelles.

En conclusion, cela nous amène à réfléchir finalement au risque pour la démocratie canadienne que ces pratiques peuvent poser. Bien qu'elles aident les formations politiques à surmonter les défis dont je vous parlais tout à l'heure, les pratiques émergentes d'organisations électorales compromettent, selon moi et selon plusieurs autres chercheurs canadiens, la qualité de notre démocratie et la pratique de la citoyenneté. L'utilisation croissante du marketing politique et de l'analyse des données personnelles des électeurs s'exécute largement en secret, à l'insu des Canadiens. Cela impose aussi des restrictions à la représentation des intérêts comme à la diffusion d'informations et, ce faisant, cela élimine progressivement les notions de bien commun et de débat public.

L'exercice de la citoyenneté et les choix électoraux...

[*Traduction*]

Le président: Monsieur Giasson, vous avez dépassé le temps de parole d'une minute. Avez-vous presque terminé?

M. Thierry Giasson: J'ai presque terminé.

Le président: Vous avez encore 30 secondes, puis nous devrions passer aux questions. Merci.

[*Français*]

M. Thierry Giasson: C'est parfait.

Malgré un intérêt médiatique croissant consacré au rôle de l'utilisation des données personnelles et des algorithmes dans les campagnes électorales, tout ce qui se passe, incluant l'affaire Cambridge Analytica, se fait largement à l'insu des Canadiens et dans un contexte où les Canadiens ignorent tout de l'étendue et de l'utilisation que font les partis de leurs données privées. Cela a une incidence importante sur la démocratie.

Je vous appelle donc, membres du Comité qui vous penchez sur ces questions, à tenter de fournir des avenues de réflexion importantes au gouvernement, de manière à pouvoir mieux encadrer cet usage et à assurer que les Canadiens comprennent bien ce pour quoi on utilise leurs données.

Je vous remercie.

● (0910)

[*Traduction*]

Le président: Merci.

Le premier intervenant est M. Erskine-Smith, pour sept minutes.

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

Je veux commencer par parler de la transparence dans les publicités. Ma question s'adresse à M. Bennett, ou à vous deux, en fait. Lorsqu'il est question de la nature des publicités, nous avons toujours ciblé les publicités en politique de différentes façons. Les gens font de la publicité dans des magazines précis car ils savent que les lecteurs seront plus susceptibles de réagir au message, comme vous l'avez signalé dans vos déclarations liminaires. S'il y a un problème particulier qui pourrait intéresser les Canadiens parce qu'ils ont des enfants ou qu'ils possèdent une arme, ou peu importe la situation, les messages sont ciblés et l'ont toujours été. C'est souvent des renseignements qui ne sont pas colligés de façon numérique, mais recueillis à la porte. Un vrai problème semble être la transparence de la nature ciblée de ces publicités.

Je ne sais pas si vous le savez, mais M. Wylie a comparu récemment au Congrès et a proposé des recommandations relativement à la transparence dans les publicités politiques. Vous pourriez peut-être tous les deux vous prononcer sur l'importance de la transparence et expliquer comment elle se traduit dans la pratique.

M. Colin Bennett: Je demanderais peut-être à Thierry de répondre en premier.

[*Français*]

M. Thierry Giasson: Je vous remercie de votre question.

Je pense que c'est le coeur de l'enjeu qui vous intéresse et qui intéresse, je pense, toute la population. Il n'y a pas de transparence en ce moment. Est-ce que vous m'entendez?

[*Traduction*]

Est-ce que vous m'entendez?

M. Nathaniel Erskine-Smith: Je n'ai pas l'interprétation.

M. Thierry Giasson: Je vais répondre en anglais. C'est correct.

La question fondamentale qui est au coeur du débat que nous tenons en ce moment, c'est qu'il n'y a pas de transparence. Les gens ne savent pas ce que font les partis. Le fait que les partis effectuent un ciblage n'est pas forcément un énorme problème. Cependant, le fait que les citoyens ne savent pas ce que font les partis avec les données qu'ils recueillent est un problème, et c'est le problème fondamental. Les partis doivent s'assurer que lorsque les citoyens donnent l'accès à toute forme de donnée qui pourrait être utilisée à des fins de ciblage politique, ils doivent en être informés.

Le président: Désolé, monsieur Giasson. Vous pouvez parler en français à nouveau. Votre anglais est excellent, mais l'interprétation fonctionne maintenant.

[*Français*]

M. Thierry Giasson: Alors je disais que le coeur de la question c'est l'enjeu de la transparence. Il y a toujours eu, en effet, de la communication ciblée.

[*Traduction*]

Entendez-vous quelque chose?

M. Nathaniel Erskine-Smith: Je n'entends rien. Je ne sais pas pourquoi.

En ce qui concerne la transparence, je vais proposer deux solutions. L'une est que, lorsque les partis politiques affichent des publicités en ligne, il y a un dépôt central qui est accessible aux membres du public, qui peuvent voir toutes les publicités qui ont été affichées. Les campagnes peuvent les soumettre publiquement à Élections Canada, qui les affichera dans un dépôt central. Il y a différentes solutions, mais toutes les publicités doivent être accessibles aux personnes qui s'inquiètent au sujet de la nature ciblée de ces publicités.

De plus, si je reçois une publicité ciblée sur Facebook ou ailleurs, je devrais être en mesure de voir les caractéristiques sous-jacentes du ciblage, que ce soit parce que je suis âgé de 30 ou 40 ans, que je suis un homme de race blanche ou que je m'intéresse au baseball. Je devrais être en mesure de voir les caractéristiques précises que la campagne a choisies pour m'interpeller.

Pensez-vous que ces deux solutions sont suffisantes et, si non, quelles autres mesures devrait-on prendre?

M. Colin Bennett: Je vais répondre. Je crois savoir que Facebook a commencé ce processus à titre expérimental au Canada pour relever les sources de publicités qui sont ciblées au pays. J'approuve ce processus. Il convient également de noter que ces types de procédures doivent être conformes au RGPD si elles sont mises en oeuvre, et elles le sont en Europe. C'est un point important à souligner.

J'ajouterais un dernier point concernant les répercussions sociales associées au manque de transparence. Bien entendu, cela incite les candidats à dire une chose à un groupe d'électeurs et une autre chose à un autre groupe d'électeurs, car le processus n'est pas transparent. On a également constaté que ce manque de transparence crée un phénomène que l'on appelle la bulle de filtres, où il n'y a pas de discours commun au sein d'un système politique sur les solutions aux problèmes publics.

● (0915)

M. Nathaniel Erskine-Smith: C'est ma dernière question, puis je vais céder la parole à ma collègue, Mme Fortier. Lequel d'entre vous connaît le mieux la LPRPDE?

M. Colin Bennett: C'est probablement moi.

M. Nathaniel Erskine-Smith: Des représentants de Facebook ont comparu devant nous, et ils ont dit que 272 Canadiens ont donné leur consentement à une demande pour divulguer les renseignements personnels de plus de 600 000 Canadiens, dont peut-être des messages privés.

À votre avis, à la lumière de votre interprétation de la LPRPDE, est-ce conforme à la loi existante?

M. Colin Bennett: Non, je ne pense pas. De plus, Facebook fait l'objet d'une enquête menée par le Commissariat à la protection de la vie privée depuis 2009. Toute la question de l'accès aux renseignements personnels des gens par l'entremise d'applications tierces a fait l'objet d'une enquête à l'époque. On a ordonné la tenue de vérifications, mais le problème persiste. Je ne crois pas que c'est conforme. C'est une collecte de données non consensuelle sur les Canadiens, et je suis d'avis que cela irait à l'encontre de la LPRPDE, mais il faudra attendre les conclusions du commissaire de la protection de la vie privée. Cela va certainement à l'encontre du RGPD.

[*Français*]

Mme Mona Fortier (Ottawa—Vanier, Lib.): Je vous remercie.

Je vais poser une brève question.

Lors de l'élection partielle que j'ai remportée, l'an dernier, dans Ottawa—Vanier, un incident est survenu entre un tiers parti et l'une de mes opposantes qui voulait mettre en avant un certain dossier.

Croyez-vous que ce genre de comportement pourrait poser un risque lors d'une campagne électorale? Croyez-vous qu'au cours de leurs campagnes les tiers partis vont utiliser davantage les plateformes en ligne ou est-il difficile de suivre ce type de coordination?

M. Thierry Giasson: C'est une excellente question.

Évidemment, la communication électorale des tiers partis est encadrée par la Loi électorale du Canada. En fait, les tribunaux ont rendu de nombreuses décisions qui ont forcé Élections Canada, au tournant des années 2000, à revoir une partie de sa législation sur cette question.

Je pense que le numérique complexifie la tâche des dirigeants des agences de supervision électorale comme Élections Canada, Élections Ontario et Élections Québec. Je pense qu'ils seront les premiers à reconnaître qu'ils n'ont pas nécessairement les ressources humaines nécessaires pour faire ce travail. Je pense qu'il faudrait revoir les ressources que l'on alloue à ces organisations d'évaluation électorale, de manière à pouvoir leur donner toutes les ressources dont elles ont besoin pour faire cet important travail de veille médiatique. C'est bien d'avoir une diversité de plateformes où la communication politique va s'exprimer, mais cela implique, pour des officiers de régulation électorale, de pouvoir avoir les ressources pour investiguer toutes ces plateformes. Il y a donc une multiplication des plateformes, ce qui, à mon avis, complexifie le travail de veille des agents électoraux.

[*Traduction*]

Le président: Merci.

Le prochain intervenant est M. Kent, pour sept minutes.

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

Merci à vous deux d'avoir accepté de participer par vidéoconférence.

J'ai amorcé ma carrière politique à un stade plus avancé de ma vie, en 2006, et depuis, à chaque élection, de nouvelles technologies ont été utilisées. Il y avait de nouvelles façons d'accumuler, d'analyser et d'utiliser les données afin d'identifier les électeurs partisans et ceux qui ne le sont pas. Dans le cadre de cette étude sur la vulnérabilité de notre processus électoral démocratique par rapport à l'utilisation inappropriée des données personnelles par Cambridge Analytica ou Facebook, on nous dit que cette utilisation inappropriée dépasse la limite.

Selon mon expérience, les choses se déroulent comme l'a souligné le professeur Giasson — on identifie les électeurs par l'entremise de la liste électorale, des réponses ou des clics sur les médias sociaux ou les sites Web des partis politiques où les gens fournissent volontairement leurs renseignements.

Selon vous, quelle devrait être la limite relativement à l'accumulation de points de données sur les électeurs canadiens? On nous dit que Facebook et Cambridge Analytica ont accumulé dans leur soi-disant entrepôt d'information jusqu'à 5 000 points de données sur plus de 230 millions d'Américains, des données qui, bien entendu, peuvent être utilisées pour compromettre le processus démocratique ou y faire interférence en ciblant les vulnérabilités ou préférences de ces utilisateurs des médias sociaux. Selon vous, quelle devrait être la limite au Canada?

● (0920)

[*Français*]

M. Thierry Giasson: Je vais vous inviter à être de votre temps et à comprendre que mener des élections en 2018, en 2019 ou en 2020, ce n'est plus comme mener des élections en 1998. Je pense que vous l'avez très bien résumé, monsieur le député.

Il y a des choses que les partis politiques pourraient décider de ne plus faire ou qu'on pourrait décider de ne plus permettre aux partis politiques de faire. Je pense, personnellement, que l'utilisation des données des médias sociaux devrait être interdite. Je pense que toutes les données qui sont colligées auprès des citoyens, par des visites sur le site Web de vos organisations, par les pétitions que vous lancez en ligne, devraient comprendre un encadré où vous indiquez ce que vous ferez éventuellement de ces données. De cette manière, les citoyens sauraient clairement que, lorsqu'ils vous laissent leur numéro de téléphone, leur adresse de courriel et leur code postal, ce sera intégré dans une base de données, que vous allez faire du ciblage de manière à pouvoir déterminer s'ils sont des électeurs intéressants ou non pour vos campagnes.

Les citoyens n'ont pas accès à cela et vous ne le leur dites pas, ce qui amène un certain nombre de médias et de chercheurs comme moi à dire que les partis politiques, d'une certaine façon, espionnent des citoyens, colligent de l'information à leur insu et utilisent cette information de manière à pouvoir jouer avec l'opinion publique pendant la campagne électorale.

Je pense qu'une loi électorale de son temps devrait encadrer très strictement le recours aux données tirées des médias sociaux. Vous avez déjà suffisamment de données à votre disposition pour pouvoir faire le ciblage dont vous avez besoin, sans nécessairement colliger, en plus, cette information et l'intégrer à vos bases de données.

[*Traduction*]

L'hon. Peter Kent: Merci. Je suis certainement d'accord avec vous, et je crois que mes collègues autour de cette table le seront aussi, que la transparence par rapport à l'utilisation acceptable des données des électeurs permettrait de calmer les préoccupations des gens qui soupçonnent que ces données sont mal utilisées. En 2015, si je ne m'abuse, *L'actualité* a essentiellement accusé tous les partis politiques canadiens d'espionner les Canadiens.

Dans votre exposé, vous avez parlé de courtiers en données, non pas d'accumulateurs de données, mais bien de courtiers qui trouvent des façons d'utiliser ces données pour influencer les résultats d'élections. Vous dites que ces intermédiaires créent des bases de données et utilisent diverses méthodes qui sont plus ou moins légales. Êtes-vous au courant de cas où les bases de données des partis politiques au Canada auraient été utilisées de façon illégale?

M. Colin Bennett: Un des problèmes avec le manque de transparence, c'est qu'on ne sait pas vraiment quel geste illégal a été posé. Il y a certainement beaucoup de zones grises.

Toutefois, pour répondre à votre question, j'aimerais brièvement souligner deux points.

Il est très important pour le Comité de comprendre que Cambridge Analytica n'est qu'une de plusieurs compagnies qui se livre à ce genre d'activité. Il n'est pas inhabituel qu'une entreprise possède 5 000 points de données sur des citoyens. Je pourrais vous nommer plusieurs entreprises aux États-Unis qui font ce genre de choses. Ce qui a attiré l'attention du public et des médias sur Cambridge Analytica, c'est le fait que l'entreprise ait eu recours à la psychographie, ce qui, de l'avis de la plupart des Canadiens, dépasse les bornes. Toutefois, encore une fois, je ne suis pas convaincu que cela soit illégal.

À mon avis, les 10 principes de la LPRPDE nous guident dans ce dossier. Dans le document que j'ai remis au Comité, je passe en revue ces 10 principes et explique ce que nos organisations politiques peuvent faire, et devraient faire, pour les respecter. Dans une certaine mesure, les partis les respectent déjà, mais il y a encore du travail à faire. Mon argument n'est pas uniquement en faveur de la transparence, mais également en faveur de l'uniformité, en ce sens qu'un accord commun pourrait être conclu entre les principaux partis politiques fédéraux sur ce qui constitue une pratique acceptable, tant en ligne que hors ligne, par rapport aux sources de renseignements personnels recueillis sur les Canadiens.

● (0925)

Le président: Il vous reste 10 secondes.

L'hon. Peter Kent: Je vais garder ma question pour la prochaine série de questions.

Monsieur Giasson, auriez-vous quelque chose à ajouter?

M. Thierry Giasson: Oui. Selon les recherches et entrevues que j'ai menées auprès de stratégistes des partis politiques fédéraux et du Québec, l'achat de données auprès de tierces parties ou de courtiers en données est très rare. Le seul cas documenté par certains de mes collègues, c'est lorsque les conservateurs ont acheté certaines données auprès d'une tierce partie sur les habitudes de consommation des citoyens. Nous ignorons si ces données ont été recueillies de façon illégale, mais je suppose que non.

Selon les témoignages que j'ai recueillis dans le cadre de mes recherches, il s'agit d'une pratique très exceptionnelle. Ce n'est pas courant.

Le président: Monsieur Masse, vous avez la parole pour sept minutes.

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

Merci, messieurs, d'avoir accepté notre invitation.

J'aimerais revenir aux 10 principes. Malheureusement, nous n'avons pas votre document devant nous. Dans votre document, avez-vous accordé une note aux différents partis politiques? Est-il juste de dire que les grands partis politiques sont avantagés ou à tout le moins qu'il est plus probable qu'ils puissent satisfaire ces normes en raison de leur capacité financière, qu'ils auraient les fonds nécessaires pour avoir un soutien interne et s'assurer que ces normes sont respectées?

Plus précisément, comment un nouveau parti peut-il être créé au Canada si cet engagement est trop important? Comment faire pour ne pas bafouer la démocratie?

M. Colin Bennett: C'est une bonne question. Je n'accorde aucune note aux partis politiques. C'est très difficile à faire avec une norme commune.

L'expérience menée en Colombie-Britannique, où les partis politiques ont dû respecter la législation qui s'appuie en grande partie sur les principes de la LPRPDE, a donné des résultats encourageants. Cette législation oblige notamment les partis politiques à tenir compte de toutes les différentes sources internes de renseignements personnels.

À mon avis, l'une des difficultés au niveau fédéral, c'est le manque de clarté sur ce qui est assujetti à ces politiques de la protection de la vie privée. Certaines s'appuient sur des données recueillies par l'entremise de sites Web, alors que d'autres sont plus générales.

Pour répondre à votre question au sujet des partis politiques moins importants, je crois qu'il s'agit d'une façon d'uniformiser les règles du jeu et de permettre à des partis politiques plus petits de voir le jour plus efficacement. C'est également l'une des conséquences des médias sociaux. Cet exercice de conformité ne devrait pas être coûteux.

Bien entendu, de l'autre côté, il y a le coût associé à l'atteinte à la sécurité des données. Toute organisation ayant souffert une atteinte majeure à la sécurité de ses données sait que les coûts en question, qu'ils soient financiers ou pour sa réputation, dépassent largement les fonds investis pour développer un code de protection de la vie privée clair et offrir une certaine transparence aux yeux de l'électorat canadien.

Monsieur Masse, vous posez une très bonne question. Celle-ci demande une analyse beaucoup plus approfondie, mais, pour le moment, c'est ma réponse.

M. Brian Masse: J'en suis à mon sixième mandat et j'ai été témoin de fraude électorale évidente ayant entraîné la démission de certains députés à la Chambre.

Cela permettrait-il d'améliorer notre réponse démocratique? Je sais que nous manquons cruellement de fonds pour le commissaire à la protection de la vie privée, le Bureau de la concurrence et le directeur général des élections, mais si, par exemple, des règles établies par un organisme indépendant, comme le directeur général des élections, accompagnées d'un mécanisme d'application sur la façon d'accumuler et d'utiliser les données et de règles connexes dont l'infraction serait punissable par la loi, dans un monde idéal, cela permettrait-il de gérer un ensemble de règles applicables aux partis politiques établis et à ceux qui tentent de voir le jour dans la démocratie canadienne?

M. Colin Bennett: Il s'agit d'une approche possible, oui, mais je plaiderais en faveur d'une analyse juridique plus détaillée sur la question. À mon avis, le dilemme est que le directeur général des élections connaît les partis politiques et les règles qui s'appliquent à eux, mais il n'a pas nécessairement les ressources et la capacité nécessaires pour traiter des questions relatives à la protection de la vie privée. Le commissaire à la protection de la vie privée a les compétences et les ressources, mais pas le mandat législatif. Nous sommes un peu entre deux chaises. Bien entendu, l'autre institution ayant certaines responsabilités à cet égard, c'est le CRTC.

À mon avis, il faudra effectuer une analyse législative et constitutionnelle très rigoureuse sur la question. D'ici là, je ne vois aucune raison pour ne pas adopter un code de pratique, sous l'égide du commissaire à la protection de la vie privée et du président-directeur général, peut-être conjointement, qui aurait pour effet d'uniformiser les règles du jeu, d'accroître la transparence et de préparer le terrain en vue de l'adoption de règles législatives.

● (0930)

M. Brian Masse: Auriez-vous quelque chose à ajouter, monsieur Giasson?

M. Thierry Giasson: Je suis d'accord avec M. Bennett.

M. Brian Masse: Que pensez-vous de l'utilisation par des tierces parties des données recueillies par les partis politiques? Une des choses qui m'inquiètent, et je crois qu'il en va de même pour les Canadiens, concernant Facebook et d'autres modèles de collecte de données, c'est que l'on ignore où et comment ces données peuvent être utilisées. Il faudrait un effort important de la part des forces de l'ordre pour faire appliquer de telles lois.

Peu importe, selon vous, à quel point est-ce grave pour la démocratie que les partis politiques puissent faire appel à des tierces parties pour accroître, soutenir et utiliser les données qu'ils possèdent?

M. Colin Bennett: Pour répondre à votre première question au sujet des transferts des données, je crois que c'est à ce niveau que les règles relatives au RGPD sont si pertinentes. Bien entendu, les Européens insistent pour que toute donnée transférée au Canada fasse l'objet de restrictions drastiques en matière de transfert. Facebook et d'autres organisations du secteur privé doivent respecter ces règles. C'est la première chose.

Concernant les règles relatives au consentement et aux partis politiques, à mon avis, le fait d'assujettir l'ensemble de l'écosystème à des règles semblables permettrait à une organisation comme le commissaire à la protection de la vie privée d'avoir une idée générale de la situation, un peu comme peut le faire la commissaire à l'information au Royaume-Uni, Elizabeth Denham.

Le président: Il vous reste 30 secondes.

M. Brian Masse: Vous avez parlé d'espionnage. L'espionnage est davantage une approche proactive par opposition à une approche destinataire relativement aux données. Pourriez-vous nous expliquer, selon vous, dans quelle mesure les partis politiques font de l'espionnage? À mon avis, une telle activité demande un effort évident par rapport à la simple accumulation et utilisation de données.

M. Thierry Giasson: Allez-y, Colin.

M. Colin Bennett: Bien entendu, on en entend parler dans les médias, mais ce n'est pas nécessairement exact. À mon avis, ce genre de conversation découle d'un manque de transparence et de confiance. Les partis politiques ont un rôle fondamental et important à jouer dans notre démocratie et ils ont besoin de renseignements personnels pour communiquer avec les Canadiens. Toutefois, il doit y avoir un certain équilibre. À mon avis, les principes de la LPRPDE fournissent les règles nécessaires pour avoir cet équilibre. En outre, lorsque ces principes ont été élaborés dans les années 1990 — et j'ai participé à ce processus —, l'application de ces principes dans de telles situations avait été prévue. Ensuite, ils ont été ajoutés à la LPRPDE.

Voilà ma réponse à votre question.

Le président: Merci, monsieur Masse.

Monsieur Saini, vous avez la parole pour sept minutes.

M. Raj Saini (Kitchener-Centre, Lib.): Bonjour messieurs. Merci beaucoup d'avoir accepté notre invitation.

Monsieur Giasson, j'aimerais d'abord m'adresser à vous.

Je me suis beaucoup intéressé à une étude que vous avez menée et dont les résultats ont été publiés dans le *Canadian Journal of Communication*. Elle a été réalisée dans le cadre de la campagne électorale de 2011. À l'époque, vous avez présenté à des élèves de l'Université McGill différentes publicités politiques, à la fois négatives et positives, et avez mesuré leur réaction physiologique et cognitive.

Pourriez-vous nous parler des résultats de cette expérience et des différences précises que vous avez relevées dans les réactions aux publicités positives et négatives?

[*Français*]

M. Thierry Giasson: D'accord.

Nous avons mené une expérience pour essayer de voir si la publicité électorale négative générait des réactions différentes chez les gens, comparativement à de la publicité que nous, les chercheurs, appelons de la « publicité promotionnelle » et que vous venez d'appeler de la « publicité positive »: le parti, plutôt que d'attaquer ses adversaires, mène alors un exercice de mise en valeur de son programme, de son bilan ou de son équipe. Or nous avons observé que la publicité négative génère une attention plus soutenue chez les gens. Leur rythme cardiaque augmentait.

Nous avons mesuré le rythme cardiaque des gens, ainsi que la sudation cutanée. Nous avons aussi demandé aux gens d'énoncer spontanément, après chacune des publicités, leurs premières impressions. Nous appelons cela les « réponses cognitives spontanées ». C'est une méthode utilisée de façon très courante en psychologie sociale pour essayer de mesurer le niveau d'engagement cognitif des gens.

Nous nous sommes rendu compte que la publicité électorale, en particulier celle qui attaquait le parti duquel l'électeur était un partisan, générait des processus cognitifs de la protection de l'ego. On tentait donc de trouver des arguments pour démolir l'argumentaire négatif qui était présenté. Nous nous sommes rendu compte par l'augmentation de la conduction cutanée, mais aussi par l'augmentation du rythme cardiaque, que le niveau d'attention des gens était plus soutenu devant la publicité négative.

Pour résumer, c'est la conclusion à laquelle nous sommes arrivés dans ces travaux. Le type de publicité auquel on est exposé génère chez nous des réactions physiologiques et cognitives différentes.

● (0935)

[*Traduction*]

M. Raj Saini: Après avoir lu votre article, j'ai remarqué, et vous en avez parlé plus tôt, que les participants redoublaient d'attention pour les publicités négatives. On remarque qu'il y a beaucoup de publicité négative dans Internet ces temps-ci.

J'aimerais connaître votre opinion sur certains points pour voir quel genre de réaction ces publicités extrêmes pourraient susciter. J'ai visité la Lettonie avec un autre comité avant que des Forces canadiennes soient déployées dans ce pays. L'une des choses que l'on nous a dites, c'est que nous serions confrontés à de la désinformation lors de notre visite et d'en être conscients. Nous avons été témoins de certaines désinformations qui ont circulé dans Internet où des soldats canadiens étaient accusés de certains gestes. Nous avons vu la même chose au Nigeria lors de la campagne électorale au pays, alors que certaines images horribles ont été utilisées contre un parti politique en particulier.

Si ces publicités négatives attirent davantage l'attention, quelle pourrait être la réaction de ceux qui les regardent?

[*Français*]

M. Thierry Giasson: Cela concentre notre attention, mais cela nous amène souvent à rapidement déployer des mécanismes qui viennent protéger noter opinion partisane.

Si on est confronté à une publicité électorale qui attaque le parti pour lequel on a l'intention de voter, ou duquel on est un membre ou un militant, on déploie, dans notre processus cognitif, ce qu'on appelle des mécanismes de protection de l'ego, qui viennent déconstruire l'argumentaire présenté. Cela concentre donc notre attention et nous amène à engager un processus cognitif plus rigoureux, mais cela n'a pas nécessairement un effet d'entraînement. Si la protection de l'ego fonctionne, cela va plutôt nous amener à asseoir de façon plus convaincante notre opinion partisane et à nous protéger de l'effet potentiel de persuasion que véhicule la publicité.

Évidemment, je n'ai pas étudiés les cas que vous me présentez. Je ne pourrais donc pas statuer là-dessus. Dans le cas africain dont vous parlez, on pourrait présumer que les citoyens qui sont des partisans du parti attaqué dans la publicité vont déployer un argumentaire, de façon plus ou moins consciente, de manière à protéger leurs convictions politiques envers le parti qui fait l'objet d'une attaque.

[*Traduction*]

M. Raj Saini: Me reste-t-il encore du temps?

Le président: Il vous reste deux minutes.

M. Raj Saini: La raison pour laquelle j'ai trouvé votre document intéressant — et j'aimerais également obtenir l'opinion de M. Bennett à ce sujet —, c'est que nous avons ce forum appelé Internet et au fur et à mesure que la technologie devient de plus en plus précise, des renseignements que nous détenons sont utilisés pour cibler avec plus de précision certains individus. Ce qui m'inquiète, c'est que ce ciblage puisse être utilisé pour influencer quelqu'un à poser des actes répréhensibles, qu'il s'agisse d'activités terroristes ou autres. Devrions-nous nous inquiéter que ce ciblage précis puisse influencer quelqu'un, comme vous le dites, et accroître sa réaction et son niveau d'attention? Peut-on faire quelque chose à cet égard? Que conseilleriez-vous? Est-ce une chose qui vous inquiète, vous aussi?

● (0940)

M. Colin Bennett: Nous devons faire la distinction entre les diverses formes de microciblage. Bien entendu, la forme la moins inoffensive est celle où un segment de la population est ciblé pour un message concernant une proposition de politiques. À première vue, un tel ciblage n'a rien de controversé. J'aimerais juste souligner que le modèle d'affaires utilisé par Cambridge Analytica s'appuyait sur la croyance selon laquelle différentes personnes ayant des caractéristiques psychologiques différentes auraient une réaction émotive différente à des messages semblables relativement à des politiques, qu'elles soient négatives ou positives. La plupart des Canadiens ne voudraient pas que de telles pratiques soient utilisées au pays.

Les normes de publicité constituent un élément clé. Il s'agit d'une partie de la réponse, mais, bien entendu, un autre élément clé est ce que les partis politiques peuvent et ne peuvent pas faire avec des sources de données commerciales et les entreprises concernées dans le cadre de leurs campagnes électorales. Il s'agit d'une image complexe à laquelle s'appliquent diverses normes législatives au Canada et à laquelle participent diverses institutions.

Le président: Merci, monsieur Saini.

M. Bernier sera notre dernier intervenant. Vous avez la parole pour cinq minutes.

[*Français*]

L'hon. Maxime Bernier (Beauce, PCC): Je vous remercie, monsieur le président.

Ma question s'adresse à vous, monsieur Giasson. Dans vos remarques du début, vous avez dit que la démocratie a évolué et que les partis politiques se servent d'informations un peu plus sophistiquées pour arriver à leurs fins. Avant cela, il y avait les sondages. D'ailleurs, les partis en font encore pour savoir ce qui est populaire et ce qui ne l'est pas, afin d'être élus et de mieux représenter les électeurs. Cela fait partie de la démocratie. Qu'on essaie de savoir quelles politiques veulent les électeurs afin de gagner l'élection et de mieux les représenter peut être vu comme étant positif pour la démocratie.

Normalement, quand une firme mène un sondage auprès de la population, elle doit se nommer. La personne au bout du fil sait qu'un sondage est fait par telle société pour tel parti politique. Maintenant, c'est plus sophistiqué. On va sur Internet et les médias sociaux pour trouver de l'information en vue d'avoir des politiques très ciblées. Cela peut permettre d'avoir une meilleure représentation démocratique.

Le problème que vous avez soulevé a trait au fait qu'il n'y a pas de transparence. Les gens ne savent pas que les partis politiques, pour être élus, utilisent de l'information pour « mieux les représenter » et leur présenter des politiques qui font leur affaire.

Quelles sont les meilleures pratiques en la matière? Tantôt, il a été question de transparence. Pour permettre aux partis politiques de continuer à sonder les électeurs — ce qui est positif pour la démocratie —, comment pourrait-on faire pour s'assurer d'une meilleure transparence? Quelles lois ou quels règlements canadiens faudrait-il modifier pour que les gens sachent à quoi s'en tenir, lorsqu'ils cliquent sur une pétition électronique ou quelque chose du genre?

M. Thierry Giasson: Les guillemets que vous avez utilisés pour parler de mieux représenter les citoyens sont importants, car c'est une vue de l'esprit. Certaines personnes diraient que les données ne sont pas utilisées pour représenter les citoyens, mais plutôt pour bien les cibler. Encore une fois, il est question de « certains » citoyens. Vous jouez un peu avec les mots, monsieur Bernier. Ce n'est pas l'ensemble de l'électorat.

Vous savez très bien comme moi que, quand un chef de parti politique se présente devant les Canadiens, il ne parle pas à tous les Canadiens et à toutes les Canadiennes, mais à certains Canadiens de certains enjeux qui sont importants pour ces électeurs. Il ne parle pas à plusieurs autres Canadiens et plusieurs autres Canadiennes. Les analyses qui ont été faites à partir de données de sondage et de données personnelles lui permettent de savoir que ces autres Canadiens et ces autres Canadiennes présentent un potentiel de réaction positive moins élevé à l'égard de ce parti. On joue un peu sur les mots, et les guillemets sont très importants dans ce que vous venez de dire.

Effectivement, il se fait de l'utilisation de données et la transparence est très importante en la matière. C'est l'élément qui est au coeur du problème auquel nous sommes confrontés aujourd'hui. On doit revoir la Loi électorale du Canada, d'une part en ce qui a trait à la manière dont les partis politiques peuvent colliger des données et, d'autre part, tout le volet qui porte sur la recherche. La Loi reconnaît aux partis politiques le droit de faire des dépenses électorales pour de la recherche, mais elle ne balise pas très clairement ce qu'on entend par recherche.

Si on décide de permettre aux partis de mobiliser des données personnelles sur les électeurs canadiens, que ce soit bien consigné et que ce soit balisé, tant dans la Loi électorale du Canada que dans la Loi sur la protection des renseignements personnels.

Il va falloir que les partis politiques soient assujettis à la réglementation en matière de protection de la vie privée et de gestion des données personnelles. Il y a des lois qui balisent les activités de plusieurs organisations relativement à ces enjeux, mais les partis politiques ne sont pas assujettis à ces lois. On doit les réintégrer dans le périmètre réglementaire canadien de manière à s'assurer que l'utilisation qui est faite des données est balisée et qu'elle répond aux principes fondamentaux de la Loi électorale du Canada. Il faut aussi mettre en avant des mécanismes qui vont assurer davantage de transparence dans les pratiques des partis.

Tout à l'heure, en réponse à une question de votre collègue M. Kent, j'ai donné l'exemple de quelqu'un qui visite le site du Parti conservateur du Canada. Lorsqu'on va sur votre site ou sur celui de tous les autres partis, une fenêtre nous accueille et on nous demande de laisser notre adresse de courriel et, parfois, notre numéro de téléphone et notre code postal. Ces informations sont colligées, mais on ne nous dit pas à quoi elles vont servir. Il pourrait y avoir tout simplement une petite fenêtre avec « Oui, j'accepte » ou « Non, je n'accepte pas » en guise d'avertissement rappelant au citoyen ce à quoi le parti pourrait éventuellement s'engager à faire avec ses données.

Pour l'heure, c'est un peu le far west et on ne sait pas ce que vous faites. Il faut donc fournir des clés d'information aux citoyens, mais aussi s'assurer que, dans le périmètre réglementaire électoral et en matière de protection de la vie privée, les partis politiques seront dorénavant assujettis à de nouvelles dispositions.

● (0945)

L'hon. Maxime Bernier: J'aimerais vous poser rapidement une brève question.

À l'avenir, pour gagner des élections, les partis politiques devront-ils de plus en plus cibler des groupes d'intérêt particuliers, des groupes de pression ou des Canadiens qui veulent obtenir des avantages spécifiques de l'État? Est-ce l'avenir de la politique ou un politicien pourrait-il avoir de l'avenir en prônant des politiques plus globales sans cibler les groupes de pression?

M. Thierry Giasson: L'un n'empêche pas l'autre.

[*Traduction*]

Le président: Une réponse brève, s'il vous plaît.

[*Français*]

M. Thierry Giasson: Je peux vous dire que les partis politiques, le vôtre inclus, le font déjà.

L'hon. Maxime Bernier: Je vous remercie.

[*Traduction*]

Le président: Merci.

La dernière question reviendra à M. Baylis.

M. Frank Baylis (Pierrefonds—Dollard, Lib.): Monsieur Bennett, vous avez proposé trois idées stratégiques. La première, si j'ai bien compris, c'est que la politique canadienne devrait être conforme à ce que propose le RGPD. La deuxième, c'est que les partis politiques soient assujettis à la LPRPDE. Quelle était la troisième? Ai-je bien compris que vous souhaiteriez l'adoption d'un code de déontologie volontaire? Est-ce que c'est ce que vous proposez?

M. Colin Bennett: À mon avis, la législation est nécessaire, mais je crois qu'il est tout aussi nécessaire d'effectuer une certaine analyse. La LPRPDE s'applique principalement aux organisations commerciales. Les partis politiques ne sont pas des organisations commerciales. Certains avancent que lorsque les partis politiques achètent des données commerciales sur les consommateurs, ils deviennent assujettis à la LPRPDE, en ce sens qu'ils effectuent des transactions, mais cela pourrait prêter à controverse.

Ce que je veux dire, c'est qu'il y a quatre façons de procéder, quatre régimes législatifs: la Loi électorale du Canada, la Loi sur la protection de la vie privée, la LPRPDE, et une loi distincte. La LPRPDE offre les principes dont nous avons déjà parlé, mais j'aimerais que le commissaire à la protection de la vie privée effectue une analyse de la question et formule des recommandations, peut-être conjointement avec le directeur général des élections. Un tel exercice prendra un certain temps. En guise de préparation à cet exercice, j'aimerais que les partis politiques déclarent publiquement qu'ils respecteront les 10 principes de protection de la vie privée stipulés dans la norme nationale. Si je ne m'abuse, le NPD l'a déjà fait, mais je ne pourrais vous le confirmer.

Le dernier point que j'aimerais souligner, c'est que lorsque nous avons appris que M. Wylie avait travaillé pour le Parti libéral, la question a immédiatement fait surface dans les médias. Cela a entraîné une réaction différente de la part des divers partis politiques sur ce qu'ils font et ce qu'ils ne font pas. Le processus visant à être plus transparent est déjà amorcé et j'aimerais qu'il soit élargi de façon à ce que les partis politiques examinent attentivement les données politiques qu'ils recueillent sur les Canadiens et comment ces données sont recueillies en ligne et hors ligne et qu'ils fassent preuve de la même diligence raisonnable en matière de gestion de la protection de la vie privée à laquelle on s'attend du secteur commercial.

● (0950)

M. Frank Baylis: Dans ce cas, j'ai une simple question: considérez-vous un engagement à respecter ces principes comme une étape intermédiaire d'ici l'adoption d'une mesure législative adéquate?

M. Colin Bennett: J'aimerais qu'il y ait un code de pratique. Cette recommandation figurait d'ailleurs dans le rapport du directeur général des élections publié il y a quelques années. Le respect de ce code de pratique serait une condition pour obtenir la liste électorale.

C'est une mesure provisoire. Je ne pense pas que cela suffise, parce qu'une tierce partie, par exemple le commissaire à la protection de la vie privée, devrait avoir le pouvoir d'enquêter en cas de plainte. Toutefois, je ne vois pas pourquoi on ne pourrait pas commencer par là. Si j'ai bien compris ce que le ministre Scott Brison a dit publiquement, le gouvernement envisage cette option. Je pense que cela pourrait être une première étape importante.

Je tiens à souligner ce que j'ai dit sur la Colombie-Britannique. Les partis politiques de la Colombie-Britannique subiront des pressions croissantes pour se conformer en raison de notre loi, ici dans la province. Si cela se produit, il serait tout à fait logique qu'ailleurs au pays, les partis politiques respectent les mêmes normes. Cela ne devrait pas être difficile ni litigieux, mais je suis conscient que ces arguments ont été avancés pour d'autres enjeux.

M. Frank Baylis: Merci.

Madame Vandenbeld, allez-y.

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

Monsieur Giasson, vous avez parlé du RGPD, je crois, notamment de la transparence algorithmique. Quel usage les partis font-ils des algorithmes? En quoi consisterait cette transparence?

[*Français*]

M. Thierry Giasson: C'est plutôt M. Bennett qui parlait du règlement général sur la protection des données dans sa présentation, mais c'est moi qui, dans la mienne, parlais de l'analyse algorithmique des données.

Comme je vous l'ai expliqué, les partis colligent des données de diverses sources. Ces données sont agrégées dans des bases de données et sont ensuite traitées au moyen de processus algorithmiques, d'analyses statistiques en sciences sociales et de régressions logistiques. On croise un certain nombre de caractéristiques sociodémographiques de manière à pouvoir établir des profils d'électeurs selon des caractéristiques politiques et sociodémographiques, notamment.

On détermine la proximité entre ces divers profils d'électeurs et les électeurs traditionnels du parti. Dans la base de données, les partis ont des informations sur leurs propres électeurs. Cela leur permet de déterminer les profils qui sont le plus proches de leurs électeurs, d'un point de vue sociopolitique, et de faire ensuite un choix des électeurs qui, si on leur proposait certaines politiques, pourraient éventuellement voter pour eux.

Les algorithmes servent entre autres à traiter un volume de données disparates et de leur donner un sens, en fait, de façon à ce qu'il soit possible de faire du profilage d'électeurs. Essentiellement, c'est à cela que se consacrent maintenant les stratèges numériques, les ingénieurs en logiciels ou les informaticiens qui travaillent dans les partis politiques.

[*Traduction*]

Le président: Merci, madame Vandenbeld.

Nous sommes dans les temps; nous avons peut-être débordé légèrement, puisque nous avons commencé un peu plus tard. Merci à tous. Je tiens particulièrement à vous remercier, monsieur Bennett. Vous êtes étonnamment en forme pour quelqu'un qui s'est levé très tôt pour témoigner à 5 h 45 du matin. Monsieur Giasson, je vous remercie d'avoir comparu au Comité.

Nous allons suspendre la séance pour environ cinq minutes pour permettre au prochain témoin de s'installer. À la fin, nous réserverons un peu de temps pour les travaux du Comité.

● (0950)

(Pause)

● (0955)

Le président: Nous reprenons. Bienvenue encore une fois au Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique.

Représentant Mozilla Corporation, nous accueillons M. Marshall Erwin, directeur, Fiducie et Sécurité.

Monsieur Erwin, la parole est à vous, pour 10 minutes.

M. Marshall Erwin (directeur, Fiducie et Sécurité, Mozilla Corporation): Merci.

Le monde de l'Internet traverse une période difficile, particulièrement en ce qui a trait à la collecte, l'utilisation et l'échange des renseignements personnels des gens à partir de sites Web, comme le démontre l'abus de confiance mettant en cause Facebook et Cambridge Analytica. Cela dit, ce n'est pas le propre de ces deux entreprises.

Il incombe aux acteurs de l'industrie, en partenariat avec les gouvernements et les comités comme le vôtre, de faire d'Internet un milieu plus sain dans lequel les gens peuvent exercer un contrôle significatif pour la protection de leurs renseignements personnels. Chez Mozilla, nous sommes heureux de constater l'importance qu'accorde le Comité à cet enjeu, et nous vous remercions de l'invitation à présenter notre point de vue.

Je m'appelle Marshall Erwin, et je suis directeur de la fiducie et de la sécurité à Mozilla Corporation. Mon rôle consiste surtout à travailler avec nos équipes de concepteurs et de génie pour acquérir une compréhension des propriétés de confidentialité du navigateur Firefox afin de veiller à l'application, dans ce navigateur, des mêmes principes de protection de la vie privée que ceux que nous prônons au quotidien.

Je vais d'abord parler de l'approche de Mozilla à l'égard de la protection des renseignements personnels, avant de présenter notre point de vue plus général sur l'état actuel de l'industrie.

Mozilla est une société qui se dévoue à sa mission, qui est de créer un Internet réellement axé sur les gens, où les utilisateurs peuvent créer leur propre expérience, ont un impact, sont en sécurité et sont indépendants. C'est d'ailleurs en raison de cet engagement à l'égard de notre mission que nous avons pris la décision de suspendre nos activités publicitaires sur Facebook lorsque le scandale concernant Facebook et Cambridge Analytica a éclaté. Ces activités sont toujours suspendues.

Cet engagement à l'égard de notre mission se reflète également dans la conception de notre navigateur Firefox, qui est utilisé par des centaines de millions de personnes dans le monde. Nous avons intégré dans ce navigateur une série de principes en matière de protection des données qui orientent nos pratiques de collecte de données.

Firefox est essentiellement votre porte d'accès à Internet. Par conséquent, le navigateur, le logiciel que vous utilisez dans votre ordinateur ou votre téléphone, gère et a accès à une grande quantité de renseignements de nature délicate sur vous et sur les sites Web que vous consultez. Ces données demeurent dans votre appareil; Mozilla ne les collecte pas. Nous sommes les concepteurs du navigateur, mais nous n'avons pas beaucoup de renseignements sur les habitudes de navigation ou les intérêts de nos utilisateurs. Il s'agit d'un important défi pour nous, mais c'est le choix que nous avons fait. Si vous utilisez le navigateur Firefox pour des activités de nature délicate ou personnelle sur Internet, vous pouvez être certains que Mozilla n'en a pas connaissance.

Mozilla collecte par défaut un ensemble de données limitées à l'aide du navigateur. Cela nous permet essentiellement de comprendre comment les gens utilisent la technologie. À titre d'exemple, nous collectons des renseignements sur les fonctionnalités du navigateur que les gens utilisent. Cela dit, nous tenons à préciser que cela n'est aucunement lié aux pages Web que les gens consultent.

Mozilla a établi un ensemble de politiques et de processus pour ses activités de collecte de données. Je peux vous donner plus de détails à ce sujet, mais je pense qu'il est important que le Comité sache qu'il est possible de créer un produit qui collecte par défaut certaines données sur des centaines de millions d'utilisateurs, tout en respectant le droit à la protection des renseignements personnels des utilisateurs et sans porter atteinte à leur vie privée. Voilà ce que nous avons réussi à faire, chez Mozilla, avec notre navigateur Firefox.

Il peut être difficile de trouver le juste équilibre entre la protection des renseignements personnels et les fonctionnalités que veulent les gens. Ce n'est pas facile, mais nous croyons y être parvenus avec notre navigateur. Malheureusement, on ne peut en dire autant du reste de l'industrie aujourd'hui.

Parlons maintenant de l'industrie des technologies, de ses points forts et des améliorations nécessaires.

Les entreprises du secteur technologique, en particulier les plus importantes, offrent à leurs utilisateurs des mesures de contrôle de la vie privée assez efficaces. L'utilisateur de Facebook qui veut protéger ses renseignements personnels peut prendre des mesures pour restreindre les données pouvant être collectées par l'entreprise et communiquées à des tiers. J'aimerais toutefois attirer votre attention sur les trois aspects pour lesquels l'industrie faillit à la tâche.

Ces paramètres de confidentialité sont souvent cachés et difficiles à trouver. L'industrie ne prend aucune mesure proactive pour aider les gens à comprendre et à utiliser les paramètres de confidentialité. Par conséquent, même si les utilisateurs disposent de moyens techniques pour protéger leurs renseignements personnels, ils n'exercent pas un contrôle significatif à cet égard.

Deuxièmement, les paramètres par défaut de ces contrôles ne sont pas raisonnables et ne correspondent pas aux attentes des utilisateurs quant à ce qui se passe réellement lorsqu'ils utilisent un produit ou un service. Les utilisateurs consentent par défaut à la collecte et à la communication de données délicates, ce qui va à l'encontre de ce que nous appelons le principe des réglages raisonnables à la base même de Firefox. Ces paramètres sont rarement utilisés dans l'industrie actuellement.

Troisièmement, les modalités de la collecte et du partage de données liées à ces paramètres de confidentialité sont toujours larges et permissives. Le principe de la collecte limitée de données de base que nous appliquons chez Mozilla n'est pas une pratique commune dans l'industrie.

Si vous examinez les problèmes liés à Facebook et à Cambridge Analytica, vous verrez que ces trois aspects sont en jeu.

Je tiens à attirer l'attention du Comité sur un enjeu qu'il convient d'examiner plus attentivement: la collecte et l'utilisation de données sur les habitudes de navigation des gens sur Internet, qu'on appelle parfois le suivi entre les sites sur Internet. Ce type d'activité est souvent associé au bouton « j'aime » de Facebook.

● (1000)

Si ce bouton se trouve sur un site Web que vous consultez, peu importe que vous ayez cliqué dessus ou non, Facebook pourrait collecter des données sur la page que vous avez consultée et l'utiliser pour faire de la publicité ciblée.

Les trois problèmes que j'ai soulevés concernant l'industrie se posent aussi dans ce cas. Les utilisateurs n'ont pas un contrôle important sur les activités de suivi. Il arrive qu'ils n'en aient même pas connaissance. Le paramètre par défaut est de suivre l'activité des utilisateurs sur Internet et les restrictions sur la collecte de données dans le cadre de ses activités sont peu nombreuses. Ces activités de suivi posent problème, car ils entraînent des risques d'atteinte à la vie privée et minent la confiance de base des gens à l'égard de la navigation en ligne.

Il y a deux semaines, devant le Congrès américain, Facebook a fait valoir que ses activités de suivi sont en tous points identiques aux activités quotidiennes d'entreprises comme Twitter, Pinterest et Google. C'est tout à fait juste. Il s'agit d'une pratique commune dans l'ensemble de l'industrie; ce n'est absolument pas unique à Facebook. Nous sommes toutefois rendus à un point charnière important. Les entités comme Facebook devraient se demander ce qu'elles peuvent faire pour inciter l'industrie à ne pas surveiller les activités des gens sur Internet sans leur donner un contrôle important les modalités de suivi.

Les comités comme le vôtre ont un rôle fondamental à jouer pour forcer Facebook et d'autres sociétés à justifier leurs activités de suivi entre les sites, d'affirmer clairement leur conviction qu'ils considèrent que les utilisateurs ont une compréhension et un contrôle adéquat de la nature du suivi, et de s'engager à améliorer le bilan de l'industrie à cet égard.

Je tiens encore une fois à remercier le Comité de nous avoir invités à comparaître aujourd'hui. C'est avec plaisir que je répondrai à toute question que vous pourrez avoir sur l'approche générale de Mozilla en matière de protection de la vie privée ou sur nos observations concernant l'industrie.

● (1005)

Le président: Je vous remercie de votre témoignage.

Je veux simplement rappeler aux membres du Comité que nous devrons être concis, étant donné le temps dont nous disposons. Quatre fois sept minutes, cela donne 28 minutes.

Nous commençons par M. Picard.

M. Michel Picard (Montarville, Lib.): Merci d'être ici.

Je suis heureux d'entendre parler du fonctionnement de Firefox, car c'est le navigateur que j'utilise. Cela me permet de me rendre à diverses pages, comme Facebook, Amazon, peu importe. Quel est le rôle de Firefox lorsque je consulte ces pages? Le logiciel est-il toujours actif? Mes activités sont-elles surveillées? Puisque j'utilise votre navigateur, peut-on savoir, premièrement, si je suis sur Facebook et deuxièmement, ce que j'y fais?

M. Marshall Erwin: Lorsque vous utilisez Firefox pour vous rendre sur Facebook, le navigateur est toujours actif; il fonctionne en arrière-plan sur votre ordinateur. Cela signifie que le navigateur Firefox sait ce que vous faites sur Facebook et pourrait, potentiellement, nous fournir ces informations. Je dis « potentiellement », encore une fois, car ce n'est pas la nature de nos activités. Nous évitons sciemment de le faire, car nous estimons que ce n'est pas la raison d'être d'un navigateur. Voilà pourquoi nous avons adopté un ensemble de politiques pour gouverner nos activités de collecte de données, c'est-à-dire les données recueillies par Firefox sur vos activités sur Facebook, et sur les données que Firefox — le logiciel installé sur votre appareil — transmet à Mozilla.

Comme je l'ai indiqué, même si tout navigateur pourrait servir à suivre vos activités sur Internet puis à les divulguer à l'entreprise qui l'a conçu, ce n'est ni ce que nous faisons ni ce que nous voulons. Nous ne voulons pas connaître la nature de vos activités sur Facebook.

M. Michel Picard: Permettez-moi de poser la question en français.

[*Français*]

À l'heure actuelle, le mot « potentiellement » est dangereux dans l'industrie. En effet, il ouvre la porte à toute possibilité de développement technologique.

Quel genre de données, autres que celles des utilisateurs en temps réel, Firefox ou Mozilla obtiennent-ils de tierces parties pour développer leur propre marketing?

[*Traduction*]

M. Marshall Erwin: Il existe plusieurs types de données qui pourraient — potentiellement, encore une fois — être obtenus par l'intermédiaire de Firefox. Nous répartissons les données en trois catégories. Il y a d'abord ce que nous appelons les données techniques. À titre d'exemple, ce sont des données sur le système d'exploitation que vous utilisez avec Firefox. La deuxième catégorie, ce sont les données d'interaction, c'est-à-dire les données sur l'utilisation du navigateur lui-même. La troisième catégorie, ce sont les données sur l'activité en ligne, comme les adresses URL des sites que vous consultez ou le fait que vous êtes connecté à Facebook.

Par défaut, nos activités de collecte de données sont concentrées sur les deux premières catégories. Un exemple utile à cet égard est le bouton « précédent » du navigateur. Nous collectons des données à partir de Firefox pour comprendre comment les gens utilisent le navigateur. Donc, si vous cliquez sur le bouton « précédent », les données recueillies nous permettent de savoir que vous utilisez cette fonction. Toutefois, nous ne collectons aucune donnée sur la page que vous consultiez au moment où vous avez cliqué sur ce bouton ni sur la page à laquelle vous retournez. Nous voulons connaître l'utilisation que vous faites du navigateur. Nous ne voulons pas d'informations sur les sites Web que vous consultez ni sur votre activité sur ces sites.

● (1010)

[*Français*]

M. Michel Picard: Si j'ai bien compris, les différentes visites d'un utilisateur sur divers sites ou pages est la troisième catégorie de données pour laquelle vous ne gardez pas d'information. En d'autres termes, la technologie existante permet de suivre l'activité d'une personne sur les différents sites qu'elle va visiter.

Cette donnée est-elle disponible? Je vais maintenant donner un exemple extrême lié aux activités criminelles. Si on a besoin de savoir si telle personne visite tel genre de site, cette donnée devient disponible, puisque votre technologie permet de le faire.

[*Traduction*]

M. Marshall Erwin: Il est important d'établir la distinction entre nous et l'entité avec laquelle vous pourriez interagir sur un site Web. Si un organisme d'application de la loi demandait à Mozilla de fournir des informations sur les activités en ligne de certaines personnes, nous ne pourrions pratiquement jamais satisfaire à cette demande, étant donné que nous ne collectons pas ces données. Nous n'avons pas de telles données. Il y a parfois le suivi entre les sites dont j'ai parlé plus tôt, mais c'est le fait de tierces parties qui utilisent Firefox. Ces entités pourraient avoir ces données, et c'est à eux que les organismes d'application de la loi devraient les demander.

[*Français*]

M. Michel Picard: Pourquoi devrais-je donner de l'information personnelle, quelle qu'elle soit, à un service duquel je ne reçois pas d'offre de services ou de produits? Je m'explique. Si j'utilise un fureteur de chez Mozilla et que j'échange sur un réseau social, comme Facebook, j'utilise un service pour parler à des gens, pour obtenir de l'information.

En soi, je n'ai pas de retour commercial. C'est le contraire lorsque je m'inscris, par exemple, au site virtuel de ma banque et que j'achète des livres sur Amazon, puisque j'ai besoin qu'on me livre la marchandise. Comme j'ai besoin de faire des transactions auprès de ma banque, c'est normal que je donne de l'information personnelle.

Pourquoi, au départ, devrais-je donner de l'information? Si je n'ai pas besoin de donner de l'information pour ce genre de services, pourquoi le fournisseur prend-il des moyens pour capter un minimum d'information auxquels je n'ai jamais consenti?

[*Traduction*]

M. Marshall Erwin: Vous voulez savoir pourquoi Firefox aurait les moyens de le faire? Nous ne le faisons pas. Firefox est un logiciel installé sur votre ordinateur. Il a donc le potentiel de faire toutes sortes de choses, à l'instar de tout logiciel installé sur votre ordinateur. La question est de savoir ce qu'il fait. Ce logiciel ne collecte aucune donnée.

[*Français*]

M. Michel Picard: Votre pratique commerciale semble être marginale par rapport au reste du marché.

Préconisez-vous que le genre de service que vous offrez soit un modèle à recommander aux fournisseurs de services sans objectifs commerciaux? Dans le cas d'un réseau social, contrairement à un magasin en ligne, la collecte de données personnelles n'est pas justifiée. Dans votre cas, de toute évidence, vous pouvez fonctionner sans avoir accès à cette information.

[*Traduction*]

M. Marshall Erwin: Je pense que les enjeux de protection de la vie privée liés à notre technologie sont très différents de ceux d'un réseau social. Je dirais toutefois que tous les principes que nous préconisons sur les enjeux de protection de la vie privée s'appliquent dans les deux cas. Sur le plan pratique, cela exige qu'une entreprise définisse les données à recueillir et les modalités de son modèle de consentement. Ces principes s'appliquent tant à Mozilla qu'aux autres sociétés.

Au cours des deux dernières décennies, essentiellement, nos efforts concrets pour intégrer ces principes dans la conception du navigateur nous ont permis de créer un produit qui protège très bien la vie privée des gens. À mon avis, si les autres entreprises s'inspiraient de ces principes dans la conception de leurs technologies, elles parviendraient aussi à ce résultat.

La technologie elle-même pourrait soulever un ensemble de questions sur la forme du modèle de contentement, la nature des données recueillies et les choses dont l'entreprise prend connaissance ou non. Les réponses varieront selon la technologie, mais je pense que les principes s'appliqueraient toujours. Je répète que l'application de ces principes nous a permis de créer un navigateur qui, à notre avis, assure une excellente protection de la vie privée.

● (1015)

Le président: Merci, monsieur Picard.

Nous passons à M. Kent, pour sept minutes.

L'hon. Peter Kent: Nous vous remercions de votre présence ici aujourd'hui.

Au cours des dernières années, mais surtout au cours des six à huit dernières semaines, on a beaucoup parlé de l'empressement des entreprises de médias sociaux à utiliser les nouvelles technologies, les technologies en évolution et l'intelligence artificielle pour améliorer leurs plans d'affaires et leur rentabilité.

Les cinq principes de Mozilla sur la protection des données et la contrainte que vous avez décrite, visant à ne pas faire la même chose que les autres entreprises, ont certainement eu une incidence sur votre rentabilité. Où se situe Mozilla par rapport à Facebook sur le plan des revenus annuels?

M. Marshall Erwin: Je dirais que c'est une technologie différente, et les revenus sont grandement inférieurs à ceux de Facebook.

Notre modèle de revenus est quelque peu différent. Nous avons des partenariats avec des fournisseurs de moteurs de recherche. Lorsque vous effectuez une recherche dans Firefox, vous arrivez sur une page de recherche et nous recevons une partie des revenus générés par ces recherches. Nos revenus sont de loin inférieurs à ceux de Facebook.

L'hon. Peter Kent: Quelle était la principale raison de Mozilla pour retirer sa publicité de Facebook? Est-ce que c'était pour vous dissocier de l'entreprise au fil de l'évolution du scandale ou est-ce que vous aviez peur des abus possibles?

M. Marshall Erwin: Je dirais que c'est pour une raison quelque peu différente. Nous avons examiné les paramètres de la plateforme Facebook relatifs au partage des données avec les tiers lorsque la nouvelle est sortie et il était évident qu'à tout le moins, ces paramètres n'étaient pas suffisants ou transparents, et qu'ils étaient peut-être aussi inadéquats.

De plus, comme je l'ai dit plus tôt, partout dans l'industrie, les paramètres par défaut représentent un problème. C'est ce qu'on a pu constater ce jour-là. Selon les paramètres par défaut, l'entreprise pouvait partager un grand nombre de données avec les développeurs des applications.

Lorsque nous avons examiné ces paramètres, nous avons conclu que leur niveau n'était tout simplement pas assez élevé. Ils ne semblaient pas être exacts ni transparents, et les possibilités de partage étaient encore trop importantes. C'est à ce moment-là que nous avons pu prendre position et dire: « Nous n'allons plus faire de publicité chez vous, du moins jusqu'à ce que vous régliez ces problèmes. »

L'hon. Peter Kent: Selon votre biographie, vous avez commencé votre carrière dans le domaine du renseignement. Vous avez travaillé pendant cinq ans à titre d'analyste dans les domaines de la lutte contre le terrorisme et de la cybersécurité, et vous avez aussi travaillé pour le Service de recherche du Congrès de l'Agence de sécurité nationale sur les fuites de renseignements et les changements législatifs.

Selon votre expérience, considérez-vous le scandale de Cambridge Analytica et Facebook comme un enjeu de sécurité nationale aux États-Unis ou au Canada?

M. Marshall Erwin: Ce n'est pas comme cela que je...

L'hon. Peter Kent: Je veux dire, en ce qui a trait à l'interférence — ou à la tentative d'interférence — avec les élections démocratiques.

M. Marshall Erwin: Dans l'ensemble, si l'on regarde ce qui s'est passé avec les élections, on comprend qu'il y a certains problèmes critiques avec nos processus démocratiques, qui représentent certainement des défis en matière de sécurité nationale. Je n'ai pas vraiment réfléchi aux particularités du scandale de Facebook et Cambridge Analytica, alors je ne pourrais pas dire si ces enjeux précis relèvent de la sécurité nationale.

Dans l'ensemble, le niveau de la collecte de données sur Internet de même que les nouvelles façons de cibler les gens pour leur passer un message ont soulevé de nombreuses questions dans nos institutions démocratiques. Il est certain que ces préoccupations sont devenues réalité en ce qui a trait aux enjeux de sécurité nationale.

L'hon. Peter Kent: L'entreprise Facebook a clairement établi — bien que ses réponses n'étaient pas claires du tout — qu'elle n'aimait pas le RGPD. Je crois que M. Chan, le représentant canadien de Facebook, a dit que l'entreprise accepterait certains règlements, mais il a clairement dit qu'elle ne se conformerait pas au RGPD. Est-ce que Mozilla accepterait ce règlement, qui entrera en vigueur la semaine prochaine en Europe?

M. Marshall Erwin: Puisqu'il entrera en vigueur en Europe, nous allons l'accepter.

Votre question et la question que le Comité...

● (1020)

L'hon. Peter Kent: L'accepteriez-vous aux États-Unis?

M. Marshall Erwin: Ce que nous voulons en matière de régime réglementaire, c'est une approche fondée sur les principes, qui ne microgérera pas les décisions techniques que prendront les entreprises. C'est le premier point que nous considérons être une priorité.

Le deuxième point vise un régime d'application solide qui donne du mordant à ces exigences réglementaires. Lorsqu'on pense aux États-Unis, au Canada et à l'Europe, la question qu'on se pose est: est-ce qu'on applique le bon ensemble de principes? Est-il en place et est-ce que la structure d'application est en place?

En ce qui a trait au Canada de façon précise, je ne suis pas un expert de la LPRPDE, mais je crois qu'elle constitue un fondement solide. On pourrait apporter certaines modifications pour harmoniser la LPRPDE au RGPD, mais je crois qu'il est important d'avoir une bonne base de référence, ce qu'il n'y a pas vraiment aux États-Unis pour le moment.

L'hon. Peter Kent: Le problème, c'est l'application.

M. Marshall Erwin: Si le Comité veut vraiment changer les choses, il faudrait miser sur l'application de la loi au Canada. Encore une fois, je crois que la LPRPDE est un bon cadre, auquel on pourra apporter quelques changements, mais il sera utile de renforcer l'application de la loi...

L'hon. Peter Kent: Il ne me reste qu'une minute.

En ce qui a trait à la propriété des données de navigation, M. Zuckerberg n'a pas été tout à fait clair, mais dans le cadre de son témoignage à Washington, il a dit que le contenu généré par un utilisateur appartenait à l'utilisateur. Toutefois, il a été très approximatif au sujet de l'historique de navigation. Est-ce que l'historique de navigation de Mozilla est pleinement protégé ou y a-t-il moyen pour les tiers de le retracer et de l'utiliser?

M. Marshall Erwin: Encore une fois, nous ne recueillons pas l'historique de navigation. Il reste sur votre ordinateur. Cela signifie qu'il est protégé contre une utilisation de Mozilla, en gros. Nous pourrions toujours modifier le navigateur, mais nous nous sommes engagés à ne pas le faire.

J'ai dit que le suivi entre les sites qui se fait dans l'industrie donne à diverses parties un accès aux activités de navigation des gens. Ces tiers ne peuvent accéder à votre historique de navigation dans le navigateur Firefox. Si vous visitez une page en particulier puis que vous passez à une autre page, et si ces deux pages utilisent des technologies pour le suivi entre les sites, alors les tiers pourront savoir que vous avez visité ces deux pages. Au fil du temps, cela permet à ces tiers de bâtir un ensemble de données assez vaste sur les activités de navigation des gens.

L'hon. Peter Kent: Merci.

Le président: Merci, monsieur Kent.

La parole est maintenant à M. Masse. Vous disposez de sept minutes, monsieur.

M. Brian Masse: Votre décision d'adopter ce modèle et de ne pas recueillir ni utiliser ces données est une décision d'affaires, que vous avez prise pour diverses raisons... pour des raisons d'éthique et pour les personnes qui se soucient de la protection de leur vie privée. Est-ce exact? Est-ce une décision d'affaires plutôt qu'une question de capacité?

M. Marshall Erwin: J'aborderais la question autrement. Qu'est-ce qui nous motive à faire la bonne chose? Ces incitatifs ne se limitent pas aux questions d'affaires. Mozilla Corporation est une entreprise d'intérêt public. Nous n'avons pas un ensemble d'actionnaires qui nous poussent à maximiser nos revenus. C'est l'une des raisons pour lesquelles au bout du compte, nous prenons ce genre de décisions.

De plus, nos utilisateurs se soucient grandement de la protection de la vie privée, tout comme les développeurs qui travaillent avec nous. Ce facteur a une grande incidence sur les décisions que nous prenons.

L'un des plus grands défis auxquels est confrontée notre industrie, c'est que jusqu'à maintenant, trop peu d'utilisateurs prenaient des décisions en fonction de la protection de leur vie privée. C'est un peu moins vrai dans notre cas, parce qu'en utilisant Firefox, notre base d'utilisateurs a démontré que c'est une chose qui la préoccupait, mais pour le reste de l'industrie, cela n'a pas été le cas jusqu'à maintenant. Nous en sommes peut-être à un point critique où les choses vont changer. Je crois que nous aimerions tous voir un changement à cet égard.

Toutefois, en ce qui a trait aux incitatifs, il sera difficile pour une entreprise comme Facebook d'offrir mieux en matière de protection de la vie privée, à moins que les utilisateurs ne l'exigent. Nos utilisateurs exigent une meilleure protection de la vie privée. Ils s'attendent à mieux, et nous pouvons leur offrir mieux.

M. Brian Masse: Ce n'est pas tant pour la capacité que pour tout le reste.

Lorsque nous avons travaillé à la question des microbilles, nous avons tout de suite constaté que bon nombre d'entreprises voulaient faire la bonne chose et restreindre la taille des microbilles. Ce sont les petits additifs de plastique qui se trouvent dans les shampoings, le dentifrice, etc. Bon nombre des entreprises voulaient prendre les bonnes décisions, mais l'organisme de réglementation n'avait pas établi un ensemble de règles uniformes, ce qui permettait au modèle de subvention d'accroître la marge de profit au détriment de l'environnement. Comment peut-on être concurrentiel dans un tel environnement?

Dans le même contexte, est-ce que les entreprises hésitent à adhérer au RGPD en partie parce qu'il n'y a pas moyen de le faire respecter? Certaines entreprises pourraient dire qu'elles respectent le Règlement en principe, mais dans les faits, l'absence d'un modèle d'incitatifs pourrait restreindre leurs capacités en matière de publicité, de vente, d'extraction et de gestion des données en ce qui a trait aux sources tierces, ce qui ne serait pas logique sur le plan économique. Est-ce que les autres entreprises se conformeraient s'il y avait un modèle d'application qui assurait une certaine normalisation?

● (1025)

M. Marshall Erwin: C'est une façon pratique de voir les choses. Quels sont les incitatifs qui poussent les entreprises à faire mieux? Encore une fois, notre base d'utilisateurs se préoccupe grandement de ces questions. Nous avons un modèle. Nous sommes une entreprise d'intérêt public. Ces facteurs motivent nos décisions.

Vous me demandez quels seront les incitatifs pour les autres entreprises? On pourrait créer deux mesures incitatives qui n'existent peut-être pas encore. Premièrement, si les utilisateurs exigent quelque chose, cela aura une grande incidence sur les incitatifs. Deuxièmement, si un régime réglementaire est en place et qu'il est appliqué rigoureusement, les entreprises y porteront attention.

Il y a un grand malaise autour du RGPD. En gros, les entreprises s'inquiètent des redevances de 4 % prévues dans le RGPD. C'est probablement une bonne chose puisque cela forcera les entreprises à s'améliorer. Le problème avec le RGPD pour bon nombre d'entreprises, à mon avis, c'est le manque de clarté au sujet de ce que doivent faire les entreprises pour le respecter et ne pas s'exposer à une amende. Le facteur de motivation associé à cette amende est sain et est utile pour l'industrie.

M. Brian Masse: Enfin, en ce qui a trait à Firefox, vous avez dit que le développement, la mise en oeuvre et la culture d'entreprise associés à cet élément motivaient l'entreprise à assurer la protection de la vie privée, et elle y arrive assez bien. Je veux être clair: tout cela pourrait changer à tout moment si le navigateur Firefox était acheté ou si l'entreprise décidait de changer de cap. L'entreprise a choisi d'adopter ces politiques et cette culture afin d'offrir ses services de cette façon; elle ne le fait pas en fonction de ses capacités technologiques.

Est-ce exact?

M. Marshall Erwin: Encore une fois, plusieurs facteurs motivent notre approche. Vous me demandez s'il est facile de changer cela?

M. Brian Masse: Vous êtes bon pour résumer mes propos.

M. Marshall Erwin: Certaines questions relèvent tout simplement des politiques tandis que d'autres relèvent de la loi. La culture d'entreprise est assez difficile à changer. C'est la culture de Mozilla depuis deux décennies. Même si nous le voulions, nous ne pourrions pas changer la mentalité de l'entreprise à cet égard. C'est une bonne chose. Nous voulons que cela reste ainsi et notre base d'utilisateurs aussi. C'est notre plus important incitatif: l'engagement que nous avons pris auprès de nos utilisateurs, auxquels nous devons rendre des comptes.

M. Brian Masse: Mis à part cet engagement...

Désolé, je ne sais pas s'il me reste du temps.

Le président: Il vous reste 30 secondes.

M. Brian Masse: La partie la plus importante de votre témoignage avait trait aux paramètres par défaut. Vous avez remarqué ces paramètres et avez décidé de ne pas les exploiter. Vous aviez la capacité nécessaire, mais vous avez choisi de ne pas le faire.

Est-ce exact?

M. Marshall Erwin: Vous parlez des paramètres par défaut dans le navigateur Firefox?

M. Brian Masse: Vous avez dit au début de votre témoignage que vous aviez remarqué les paramètres ouverts par défaut, dont vous auriez pu tirer profit avec la fuite de données, mais vous avez décidé de ne pas le faire.

M. Marshall Erwin: Nous examinions les paramètres par défaut de façon générale. Ce sont les paramètres par défaut associés aux développeurs tiers qui ont motivé notre choix de ne plus faire de publicité sur cette plateforme. Ces paramètres étaient inexacts et semblaient transmettre les données aux développeurs. C'est la décision que nous avons prise au sujet de la plateforme Facebook. Nous n'avons jamais été en position de recueillir ces données. Il n'était pas question pour nous d'avoir accès ou non à ces données; il était seulement question de déterminer si l'approche adoptée par Facebook était la bonne pour ses utilisateurs.

● (1030)

M. Brian Masse: Merci.

Le président: Merci, monsieur Masse.

Monsieur Erwin, je tiens à vous remercier pour votre témoignage. Je vous remercie de vous être déplacé jusqu'ici.

M. Marshall Erwin: Merci.

Le président: Nous allons suspendre à nouveau la séance quelques minutes jusqu'à ce que nos invités soient partis, puis nous poursuivrons à huis clos pour discuter des travaux du Comité pendant une quinzaine de minutes.

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