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 121 • 1re SESSION • 42e LÉGISLATURE

TÉMOIGNAGES

Le jeudi 18 octobre 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 18 octobre 2018

● (1115)

[*Traduction*]

Le vice-président (M. Nathaniel Erskine-Smith (Beaches—East York, Lib.)): Je m'excuse de commencer en retard.

Nous accueillons la Banque du Canada, le Bureau de la concurrence et le CST. Je vous remercie tous d'être là.

Nous allons commencer par l'exposé du Bureau de la concurrence.

[*Français*]

M. Anthony Durocher (sous-commissaire, Direction des pratiques monopolistiques, Bureau de la concurrence): Monsieur le président, je vous remercie de nous donner l'occasion de comparaître devant vous aujourd'hui.

Je m'appelle Anthony Durocher et je suis le sous-commissaire responsable des pratiques monopolistiques au Bureau de la concurrence. Je suis accompagné de ma collègue Mme Alexa Gendron-O'Donnell, sous-commissaire déléguée à la Direction de l'analyse économique du Bureau.

Le Bureau de la concurrence est un organisme d'application de la loi indépendant qui veille à ce que les entreprises et les consommateurs canadiens prospèrent dans un marché concurrentiel et innovateur.

Le Bureau assure et contrôle l'application de la Loi sur la concurrence du Canada, notamment en menant des enquêtes et en réglant les problèmes relatifs à l'abus de position dominante, aux fusions anticoncurrentielles, à la fixation des prix et aux pratiques commerciales trompeuses.

L'application de la loi en matière de concurrence ne peut reposer uniquement sur des principes théoriques. Nous utilisons une approche fondée sur des données probantes. Il faut donc que nos décisions soient fondées sur des preuves crédibles qui pourront résister au contrôle judiciaire.

Il importe également de souligner que notre rôle est d'appliquer la Loi sur la concurrence et non de faire de l'arbitrage ou de prendre des décisions judiciaires. La Loi nous oblige à respecter plusieurs normes et critères, par exemple en prouvant que quelque chose a occasionné un tort considérable à la concurrence.

Peu importe notre volonté de judiciariser une affaire donnée, nous sommes guidés par les décisions des tribunaux et du Tribunal de la concurrence.

[*Traduction*]

Il est difficile d'allumer la télévision ou de lire les journaux sans constater le rôle croissant des données dans notre économie. Le pouvoir que les données représentent maintenant et le contrôle que les plateformes numériques exercent sur elles méritent un examen attentif. Le Bureau reconnaît le rôle important qu'il doit jouer dans ce domaine et s'efforce d'être un chef de file, tant grâce à son travail d'application de la loi, qu'à son travail stratégique, et nous avons l'intention de vous parler des deux aujourd'hui.

Nous croyons savoir que le Comité s'intéresse particulièrement à la protection de la vie privée. C'est important pour moi de dire d'entrée de jeu que la protection des renseignements personnels n'est pas un objectif explicite au titre de la Loi sur la concurrence, de sorte que notre rôle est limité à cet égard. Cependant, la protection de la vie privée peut être pertinente à notre travail de deux façons. Premièrement, si des entreprises se livrent concurrence pour attirer de nouveaux utilisateurs en offrant une protection de la vie privée, cette dimension de la concurrence peut être un facteur pertinent dans l'examen des activités anticoncurrentielles. Deuxièmement, si une entreprise trompe des consommateurs quant au fait que leurs données seront utilisées ou à la façon dont elles le seront, une telle situation pourrait également soulever des préoccupations liées à la Loi sur la concurrence.

Il y a de nombreux avantages évidents associés à la collecte et l'analyse de données, particulièrement pour favoriser l'innovation, mais il y a aussi des risques. Le Bureau a le mandat de protéger la concurrence dans l'économie numérique, et nous continuons de faire ce travail en priorité. Cependant, il est important de reconnaître que la Loi sur la concurrence a ses limites. Ce n'est pas une solution miracle pour les menaces générales que les données et les plateformes fondées sur des données peuvent représenter pour la société, comme les violations de la vie privée, l'ingérence dans des élections ou la manipulation de l'opinion publique. Ces risques dépassent notre mandat juridique. Malgré tout, nous sommes heureux de mettre notre expertise en matière de concurrence au service de cette importante discussion puisque ce sont des enjeux transversaux qui bénéficieront d'un travail de collaboration pangouvernemental pour protéger les Canadiens.

Il y a un peu plus d'un an, le Bureau a publié un livre blanc intitulé « Mégadonnées et innovation: conséquences sur la politique en matière de concurrence au Canada ». L'objectif de ce document était de mobiliser les intervenants en suscitant une discussion sur la façon dont l'émergence des mégadonnées devrait influer sur l'application de la législation sur la concurrence.

Après de longues consultations, le Bureau a constaté qu'il n'est pas nécessaire de prendre des mesures précipitées dans ce domaine. Le cadre actuel est à la hauteur de la tâche, mais nos outils doivent évoluer pour faire face aux enjeux complexes découlant des plateformes numériques, comme celles qui monétisent les données des utilisateurs par la publicité en offrant des services gratuits aux consommateurs.

● (1120)

L'une des préoccupations récurrentes dont nous entendons parler, c'est la taille et la croissance de certaines entreprises de technologie, mais la taille n'est pas nécessairement quelque chose de mal. Grossir, c'est la récompense qu'une entreprise peut obtenir lorsqu'elle réussit à offrir un produit novateur. Nous ne devrions pas punir la réussite. C'est seulement lorsqu'on trouve des preuves qu'une grande entreprise s'adonne à un comportement anticoncurrentiel préjudiciable que nous devrions intervenir.

Il est important de trouver le juste équilibre entre la prévention de tout comportement concurrentiel néfaste pour les consommateurs canadiens et une surapplication indue de la loi et le tort involontaire que cela pourrait causer à l'innovation et à l'économie. Certains des enjeux dont nous avons entendu parler relativement à l'économie numérique et notre surveillance incluent le fait que des entreprises achètent des concurrents émergents ou excluent ceux qui causent des perturbations. Des entreprises peuvent utiliser l'intelligence artificielle ou des algorithmes pour s'entendre et fixer des prix, et d'autres peuvent tromper les consommateurs quant à savoir si leurs données seront utilisées et la façon dont elles le seront. Si nous trouvons des preuves du fait que ces pratiques contreviennent à la Loi sur la concurrence, le Bureau prendra des mesures pour protéger les Canadiens.

Nous avons déjà mené plusieurs enquêtes importantes dans le domaine de l'économie numérique, y compris sur Google relativement à un abus présumé de pouvoir sur le marché lié à son moteur de recherche, et sur le Toronto Real Estate Board, le TREB, au sujet de ses données immobilières.

Notre cause contre le TREB est un excellent exemple. Nous avons pu l'empêcher de cacher des données immobilières à des agents qui voulaient offrir des services en ligne novateurs aux acheteurs et aux vendeurs de maisons. Ce cas montre bien de quelle façon nous nous assurons que les consommateurs canadiens bénéficient de l'innovation dans l'économie numérique.

Nous sommes heureux d'avoir l'occasion de discuter plus en détail du livre blanc du Bureau ainsi que de ces récentes affaires durant la période de questions et de réponses.

[*Français*]

L'économie numérique est l'une des grandes priorités du Bureau. Nous continuerons à surveiller le marché en ligne, y compris les comportements des grandes entreprises technologiques.

Nous continuerons également à travailler de près avec nos partenaires canadiens et étrangers et à évaluer attentivement les mesures prises par nos homologues internationaux. Toutefois, les lois et les dynamiques concurrentielles varient parfois considérablement d'un pays à l'autre, et nous devons garder ces différences en tête.

Par ailleurs, nous encourageons tous les Canadiens à communiquer avec nous s'ils ont des preuves qu'une infraction à la Loi sur la concurrence a été commise.

Avant de répondre à vos questions, je tiens à préciser que la Loi sur la concurrence oblige le Bureau à mener ses enquêtes en privé et à protéger la confidentialité des renseignements qu'il obtient. Cette obligation pourrait nous empêcher de discuter d'enquêtes actuelles ou antérieures.

Nous sommes ravis d'avoir cette occasion de comparaître devant vous pour discuter de notre travail et attendons avec impatience vos questions.

Je vous remercie.

[*Traduction*]

Le vice-président (M. Nathaniel Erskine-Smith): Merci beaucoup. Nous vous sommes très reconnaissants.

La prochaine déclaration est celle du Centre de la sécurité des télécommunications.

Vous avez 10 minutes.

M. Dan Rogers (chef adjoint, SIGINT, Centre de la sécurité des télécommunications): Merci et bonjour, monsieur le président, et bonjour aux membres du Comité.

Je m'appelle Dan Rogers. Je suis chef adjoint du Renseignement électromagnétique étranger au Centre de la sécurité des télécommunications. Je suis responsable du programme de renseignement électromagnétique étranger du CST. Je suis accompagné aujourd'hui par mon collègue, André Boucher, sous-ministre délégué des Opérations du Centre canadien pour la cybersécurité.

Le Centre canadien pour la cybersécurité, qui fait partie du CST, est l'autorité nationale en matière de cybersécurité et d'intervention en cas de cybermenaces. C'est avec plaisir que je me présente aujourd'hui devant vous tandis que vous poursuivez votre étude.

En ce qui a trait à l'incident impliquant Cambridge Analytica et Facebook, le CST n'a pas le mandat de réglementer les médias sociaux et n'est pas un organisme d'application de la loi. Le CST n'a pas la responsabilité de surveiller ces entreprises. Il incombe toutefois au Centre de repérer et de contrer les cybermenaces qui planent sur le processus démocratique du Canada. Pour cette raison, mon allocution portera sur ces menaces et sur les façons de les contrer en appliquant des mesures robustes de sécurité informatique et physique.

J'espère aussi vous éclairer sur les fonctions du CST et sur les changements qu'il a vécus depuis la dernière fois que des représentants de l'organisme se sont présentés devant le Comité, en 2017.

Le CST est l'organisme national du renseignement électromagnétique en matière de renseignements étrangers et l'expert technique de la cybersécurité et de l'assurance de l'information. Je tiens à préciser que les activités de renseignement électromagnétique du CST ciblent uniquement les communications étrangères. La loi interdit en effet à l'organisme de viser des Canadiens, où qu'ils soient, ou toute autre personne se trouvant au Canada.

Le CST adapte ses activités au contexte actuel de la menace. Il contribue à assurer la prospérité, la sécurité et la stabilité du Canada en fournissant des renseignements sur les activités terroristes menées à l'étranger ou sur les menaces qui pèsent sur les Canadiens à l'extérieur du pays, ainsi qu'en défendant le Canada contre des cyberattaques.

Récemment, le CST a été chargé d'aider la ministre des Institutions démocratiques à remplir son mandat qui consiste à diriger les efforts du gouvernement du Canada en vue de défendre le processus électoral canadien. Plus précisément, la lettre de mandat adressée à la ministre des Institutions démocratiques précisait que celle-ci devait demander au CST d'analyser les risques que représentent les pirates informatiques contre les activités politiques électorales du Canada, de diffuser les résultats de l'évaluation au grand public et de conseiller les partis politiques canadiens et Élections Canada concernant les pratiques exemplaires en matière de cybersécurité.

Le CST a donné suite à sa demande en publiant, en juin 2017, un rapport sur les cybermenaces qui planent sur le processus démocratique du Canada. Le rapport est non classifié, mais les principales conclusions de l'évaluation sont fondées sur de nombreuses sources, notamment des renseignements classifiés obtenus grâce à l'expertise unique du CST dans les domaines de la cybersécurité et du renseignement étranger. Le CST a étudié les cybermenaces qui pèsent sur les processus démocratiques partout au Canada, dans les ordres de gouvernement fédéral, provincial ou territorial ainsi que municipal. Il a fait la même chose dans le reste du monde. Le rapport porte sur les types d'auteurs de menaces, les cibles qu'ils sont susceptibles de choisir et les méthodes qu'ils pourraient privilégier pour cibler leurs victimes.

Selon l'évaluation du CST, lors des élections fédérales de 2015, le processus démocratique du Canada a été ciblé par des activités de cybermenace peu perfectionnées, probablement perpétrées par des cyberactivistes et des cybercriminels. Ces activités n'ont eu aucune incidence sur les résultats de l'élection ni sur la protection des renseignements personnels des Canadiens. Le CST estime que, à l'échelon fédéral, les partis politiques, les politiciens, les médias traditionnels et les médias sociaux sont plus vulnérables aux cyberattaques que les activités liées aux élections.

Comme les processus démocratiques de partout dans le monde sont de plus en plus ciblés par des activités de cybermenace, le CST s'attend à ce que de nombreux groupes de cyberactivistes recourent à des moyens informatiques pour tenter d'influencer le processus démocratique durant les élections fédérales de 2019. Le CST estime que les cybermenaces seront probablement peu perfectionnées, mais bien planifiées et qu'elles cibleront plus d'un aspect du processus démocratique.

Le CST a reçu pour consigne de poursuivre son analyse. Il s'attend à publier une mise à jour de son rapport de 2017.

Même si le rapport sur les cybermenaces n'a pas comme mandat de prodiguer des conseils sur les mesures d'atténuation, pour satisfaire à la demande de la ministre Gould, nous avons tenu des séances d'information à l'intention des membres des partis politiques, des greffiers provinciaux et territoriaux et des employés d'Élections Canada afin de leur faire part des pratiques exemplaires en matière de cybersécurité.

Le principal message véhiculé durant ces séances d'information, c'était que les mesures de protection des systèmes devraient arrêter la plupart des activités qui seraient malveillantes, mais que la sécurité informatique ne dépend pas seulement de la technologie. Les utilisateurs doivent aussi être vigilants et adopter de saines habitudes en matière de cybersécurité afin de freiner les menaces d'aujourd'hui et de rester en amont des menaces de demain.

Le CST a publié sur son site Web plusieurs documents portant, entre autres, sur les 10 mesures de sécurité des TI, le Guide d'hygiène informatique, les pratiques exemplaires en matière de cybersécurité et sur la sécurité des appareils mobiles à l'intention des TI organisationnelles et d'autres ressources contenant des pratiques exemplaires à l'intention des utilisateurs. Nous serons heureux de parler de ces ressources plus en détail durant la période de questions et de réponses.

● (1125)

La cybersécurité est un sport d'équipe. Le CST continue donc de travailler de concert avec Élections Canada pour assurer la protection des élections et pour faire en sorte qu'elle reste un aspect du processus démocratique dans lequel la population a confiance.

Le CST continuera de travailler en collaboration avec la ministre Gould et d'autres intervenants, au besoin, pour assurer la protection des institutions démocratiques du Canada ainsi que du processus électoral contre les cybermenaces.

Le 1er octobre, le ministre de la Défense nationale a annoncé la création officielle du Centre canadien pour la cybersécurité, l'autorité nationale en matière de cybersécurité et d'intervention en cas de cybermenace. Le Centre pour la cybersécurité, hébergé par le CST, réunit l'expertise du CST et celle de ses collègues de Sécurité publique Canada et de Services partagés Canada sous le même toit. Le Centre représente une source unifiée d'avis et de conseils spécialisés pour les entreprises privées, les propriétaires et les exploitants des infrastructures essentielles ainsi que le public canadien. Il contribuera à la sécurité du cyberespace.

Grâce à la mise en place du nouveau Centre canadien pour la cybersécurité, il sera plus facile de coordonner les efforts visant à protéger les institutions démocratiques du Canada contre les cybermenaces, et cela inclut la période précédant les élections fédérales de 2019.

Encore une fois, nous vous remercions de nous avoir invités aujourd'hui. Nous serons heureux de répondre à vos questions.

● (1130)

Le vice-président (M. Nathaniel Erskine-Smith): Merci beaucoup.

La dernière présentation est celle d'Eric Santor, de la Banque du Canada.

Merci beaucoup de vous joindre à nous aujourd'hui. Vous avez 10 minutes.

M. Eric Santor (directeur général, Analyses de l'économie canadienne, Banque du Canada):

Bonjour, monsieur le président, et bonjour aux membres du Comité. Je vous remercie beaucoup de m'avoir invité ici aujourd'hui.

En tant que directeur général du service des Analyses de l'économie canadienne de la Banque du Canada, je suis heureux de présenter le point de vue et les observations de la Banque relativement à la diminution de la concurrence dans les économies avancées. Je parlerai aussi des répercussions, tant pour ce qui est de la concurrence que du dynamisme de l'économie à long terme, de l'émergence des grandes entreprises de hautes technologies et ainsi que de l'importance croissante des mégadonnées.

Pour tenter d'atteindre son objectif qui consiste à maintenir l'inflation à un niveau bas, stable et prévisible, la Banque du Canada doit absolument comprendre l'incidence de la numérisation sur l'économie canadienne. Comme le mandat de la Banque ne prévoit aucun rôle de réglementation concernant la confidentialité des données des citoyens, vous comprenez, j'en suis convaincu, que je ne pourrai pas aborder les répercussions de ces questions sur le plan de la protection de la vie privée.

La numérisation de l'économie canadienne avance rapidement. Ce changement devrait, globalement, favoriser le progrès économique. Il entraîne la création d'entreprises ainsi que la transformation d'entreprises actuelles, qui doivent revoir leur fonctionnement en raison des nouvelles technologies. Les consommateurs, pour leur part, peuvent se procurer en tout temps une gamme apparemment sans cesse croissante de biens et de services, et ce, 24 heures sur 24 et 7 jours sur 7, produits partout au Canada et dans le monde entier.

[*Français*]

La numérisation contribuera à faire augmenter la productivité, et donc le niveau de vie, au cours des années et des décennies à venir.

Beaucoup de personnes s'inquiètent de l'avènement des robots et du fait qu'ils pourraient remplacer des travailleurs. Naturellement, nous avons tendance à nous focaliser sur cet effet initial, mais il faut savoir qu'un robot ne peut pas remplacer un travailleur du jour au lendemain.

[*Traduction*]

Il est néanmoins évident que certaines personnes seront touchées par ces changements, mais la société aura le temps de s'adapter. Les travailleurs concernés auront besoin de soutien. La formation professionnelle et un robuste filet de sécurité sociale sont donc essentiels.

De plus, il ne faut pas oublier que la numérisation crée de nouveaux types d'emplois, et en créera d'autres que nous n'avons même pas encore imaginés. Ces emplois favoriseront la croissance de l'économie. Ils procureront de nouveaux revenus qui seront dépensés non seulement dans la sphère numérique, mais dans tous les secteurs, ce qui aidera aussi les travailleurs occupant des emplois traditionnels.

L'utilisation à diverses fins commerciales de l'intelligence artificielle et de l'apprentissage machine de pair avec les mégadonnées est au coeur de la numérisation. L'IA et l'AM accroissent la productivité des entreprises de trois grandes façons: ils les aident à fabriquer de meilleurs produits et à améliorer l'expérience client, ils contribuent à l'élaboration plus efficace et rapide de produits et de services et, finalement, ils permettent aux entreprises de conquérir de nouveaux marchés et de nouveaux clients.

[*Français*]

Les applications de ces technologies sont pratiquement infinies. En voici quelques exemples.

Des agriculteurs utilisent des systèmes de pilotage automatique par GPS pour conduire leurs tracteurs et optimiser l'utilisation de fertilisants et de pesticides; des robots travaillent dans des usines et des entrepôts et « conduisent » des chariots élévateurs pour déplacer la marchandise; une intelligence artificielle peut vous suggérer des produits ou des services à acheter; et des agents intelligents et des robots-conseillers de sites Web sont prêts à répondre à vos questions.

[*Traduction*]

En combinant IA et l'AM aux mégadonnées, les entreprises peuvent obtenir un avantage concurrentiel parce qu'elles pourront, au bout du compte, offrir un meilleur produit ou un meilleur service à plus bas prix. Une des caractéristiques de l'IA, de l'AM, des mégadonnées et des effets de réseau, c'est qu'il y a toujours de grands avantages liés au fait d'être le premier à les utiliser. En fait, la concentration du marché est un phénomène qui se produit naturellement dans les secteurs d'activités caractérisés par d'importants effets de réseau et d'autres formes d'économies d'échelle.

Dans le contexte actuel, cette dynamique peut mener à la création d'entreprises phares. Ces entreprises ont généralement un effectif moins nombreux que les entreprises traditionnelles et elles peuvent dégager d'énormes bénéfices grâce à leur activité monopolistique.

La nouveauté, c'est que cette impression selon laquelle le gagnant rafle toute la mise s'amplifie dans une économie numérique, car les données des utilisateurs deviennent une autre source de monopole. Les données d'un grand réseau créent dès lors un obstacle considérable à l'entrée de concurrents sur le marché. Un autre obstacle peut résider dans la stratégie de certaines entreprises, qui étant en mesure de contrôler l'accès à des services en ligne essentiels, exploitent cette situation pour entraver leurs concurrents et freiner l'innovation. Dans ces circonstances, nous sommes d'avis que les politiques en matière de concurrence peuvent être adéquatement modernisées afin de veiller à ce que nous tirions pleinement parti de la numérisation.

Que savons-nous? Quelles données probantes avons-nous au sujet de la concentration du marché, des marges bénéficiaires et des prix?

Ces dernières années, les économistes ont porté une attention considérable à la hausse séculaire de la concentration du marché dans les économies avancées. Ils ont notamment mis au point des modèles qui relient cette hausse à la numérisation. Plus particulièrement, les entreprises phares sont en mesure d'accroître leur part de marché grâce aux progrès technologiques — comme l'utilisation de l'IA ou de l'AM et des mégadonnées —, augmentant ainsi la concentration sectorielle. Elles détiennent aussi une part élevée des profits, ce qui peut entraîner une baisse de la part du revenu du travail.

De façon générale, la plupart des secteurs ont vu leur concentration augmenter ces 15 dernières années. Même si les données d'observation ne sont pas encore concluantes, la hausse généralisée de la concentration sectorielle dans l'ensemble des pays porte à croire que ce sont les changements technologiques, c'est-à-dire la numérisation, et non des facteurs propres à chaque pays, qui en sont le principal vecteur.

L'une des préoccupations que suscite chez nous la domination des entreprises phares tient au fait que celles-ci disposent d'un pouvoir plus important quand il s'agit de fixer leurs prix, ce qui pourrait faire augmenter les prix. C'est pourquoi les économistes se penchent aussi sur la hausse séculaire du pouvoir de marché des entreprises, que l'on mesure par des marges bénéficiaires. Ainsi les chercheurs ont noté une hausse des marges moyennes aux États-Unis entre 1980 et 2014. Ils constatent également une augmentation des marges partout. Ce mouvement se manifeste aussi au Canada. Ici, les chercheurs observent une tendance générale très semblable à celle des États-Unis, ce que confirme d'ailleurs le Fonds monétaire international, ce qui donne à penser que le pouvoir du marché s'accroît dans de nombreux pays depuis plusieurs décennies.

La question qui se pose ensuite est de savoir si la numérisation a eu une incidence sur les prix à la consommation. C'est qu'on appelle couramment l'« effet Amazon », selon lequel la concurrence exercée par des détaillants en ligne ferait baisser les prix. Il peut sembler paradoxal que la numérisation fasse à la fois augmenter les marges et baisser les prix. Toutefois c'est simplement que les avantages de la technologie profitent en partie aux clients, qui obtiennent des baisses de prix, mais aussi aux entreprises, dont les marges sont plus élevées en raison de la diminution des coûts.

Même si les observations directes de l'effet de la numérisation sur l'inflation sont contrastées, elles tendent effectivement à indiquer une pression à la baisse. Dans les études publiées l'an dernier, les chercheurs de la Banque ont conclu que les observations directes faisaient état d'un léger effet négatif de la numérisation sur l'inflation. Autrement dit, la numérisation freinait la hausse des prix, au lieu de l'alimenter. Les indications tirées des données sur les prix en ligne, par exemple celles obtenues dans le cadre du Billion Prices Project, sont-elles aussi contrastées. Selon certaines, les prix en ligne ont tendance à se comporter de façon comparable aux prix des magasins ayant pignon sur rue, tandis que, selon d'autres, on constate des répercussions importantes à la baisse sur l'inflation année après année. Comme on le devine facilement, cette situation s'explique entre autres par la possibilité que nous avons tous de comparer les prix des concurrents au moyen d'un téléphone intelligent avant de passer à la caisse.

Enfin, lorsque nous utilisons le cadre sur lequel reposent les principaux modèles de la Banque pour évaluer les voies par lesquelles la numérisation pourrait agir sur l'inflation, nous constatons que la plupart des dynamiques associées à la numérisation exerceraient une pression à la baisse sur l'inflation.

En somme, la question de l'effet de la numérisation sur la concentration du marché et, par conséquent, sur la concurrence, reste entière. La Banque continuera d'étudier l'influence de la numérisation sur l'économie canadienne dans le cadre de son mandat, qui consiste à favoriser la prospérité économique et financière du pays.

● (1135)

[*Français*]

Je vous remercie encore de votre invitation.

[*Traduction*]

Le vice-président (M. Nathaniel Erskine-Smith): Merci à vous tous de vos exposés.

Nous allons commencer notre tour de sept minutes.

Les sept premières minutes vont à M. Saini.

M. Raj Saini (Kitchener-Centre, Lib.): Bonjour.

Merci à vous tous d'être là.

Je ne peux pas m'empêcher de poser une question à M. Santor.

L'inflation n'est peut-être pas un sujet à la mode, mais je sais que les banques centrales du monde entier ont fixé un taux d'inflation de moins de 2 %. Maintenant, vous faites entrer les détaillants dans la danse. Il y a deux modèles: les détaillants qui ont pignon sur rue, et les détaillants en ligne. Il y a une différence de prix. Je l'ai vu moi-même en me rendant au magasin. Certains de ces produits ne sont pas calculés dans votre indice des prix à la consommation, alors comment pouvez-vous mesurer avec exactitude ce qui se passe sur le marché? Le marché lui-même a changé.

M. Eric Santor: Notre mandat consiste à maintenir une cible d'inflation à 2 %, dans une fourchette de 1 % à 3 %. L'IPC lui-même est construit par Statistique Canada, alors c'est à ces personnes que vous devez poser votre question quant à savoir si l'indice reflète ou non ces faits nouveaux.

Je sais qu'ils sont conscients de cette question. Cela fait assurément partie de leur programme.

M. Raj Saini: Cela ne vous complique-t-il pas la tâche lorsque vous faites vos évaluations?

M. Eric Santor: Ce que nous observons, c'est l'IPC, et ce dernier contient des prix de détaillants qui ont pignon sur rue et des prix en ligne. Nous avons l'indice à l'oeil. Puisque nous savons que les prix en ligne exercent une pression à la baisse sur les prix des détaillants qui ont pignon sur rue, c'est une réalité qui serait déjà intégrée dans l'IPC tandis que l'effet de la concurrence s'applique. Lorsque nous parlons à [*Note de la rédaction: difficultés techniques*] dans nos sondages, ils nous disent que, oui, ils ressentent une pression à la baisse des prix en raison de la concurrence en ligne, et donc, c'est pris en considération dans une certaine mesure.

M. Raj Saini: D'accord.

Monsieur Rogers, je vais m'entretenir avec vous un peu ce matin.

De quelle façon évalueriez-vous le niveau de menace actuel pour le processus démocratique canadien, surtout pour ce qui est des élections de 2019? Dans votre déclaration préliminaire, vous avez parlé de 2015, élections durant lesquelles il y a eu un faible niveau d'activité, mais, maintenant, nous nous dirigeons vers les élections de 2019 et, évidemment, il y aura plus d'intervenants en jeu. De quelle façon évaluez-vous le niveau de menace actuellement?

M. Dan Rogers: Je suis heureux de répondre à la question et je vous en remercie. C'est une question qui a été abordée dans le dernier rapport. Je sais que notre centre de cybersécurité prépare un nouveau rapport qui portera sur la question.

Je peux peut-être demander à André de vous répondre.

● (1140)

[*Français*]

M. André Boucher (sous-ministre adjoint, Opérations, Centre canadien pour la cybersécurité, Centre de la sécurité des télécommunications): D'accord.

Dans notre rapport de juin 2017, il était déjà indiqué que nous nous attendions à une hausse de l'utilisation du cyberespace et à ce que cette hausse entraîne différents types de menaces.

Une mise à jour de ce rapport est prévue pour le début de l'année prochaine, mais je vais me permettre de vous dire maintenant ce qu'on peut attendre de cette mise à jour.

Effectivement, il y a une augmentation des menaces. Le principal changement a trait à la vitesse à laquelle les menaces ont augmenté. Nous nous attendions à ce qu'elles augmentent, mais cela s'est fait plus rapidement. Cela s'applique aussi au Canada. Personne n'en sera surpris, compte tenu de ce qui se passe à l'international.

[*Traduction*]

M. Raj Saini: Cela m'amène à ma deuxième question. Y a-t-il un risque que les listes électorales canadiennes ou celles des partis politiques canadiens soient compromises? Nous avons vu l'exemple d'une telle situation durant les élections de 2016 du côté du DNC et de la campagne de Clinton. Où en sommes-nous à ce sujet à l'heure actuelle?

[*Français*]

M. André Boucher: Je vous remercie de cette question, monsieur Saini.

Nous sommes réellement aux aguets, car nous savons de ce qui est arrivé à l'échelle internationale. Nous avons commencé à travailler très tôt avec les gens d'Élections Canada afin de nous assurer que les réseaux, les systèmes et les procédures mis en place étaient de taille à faire face aux menaces grandissantes dont je viens de parler. Je suis tout à fait convaincu que les mesures, les processus et les technologies mis en place permettront au Canada de faire face aux menaces en ce qui touche les listes des électeurs.

[*Traduction*]

M. Raj Saini: Je ne veux citer personne, mais il est évident qu'il y a certains acteurs étatiques dans le monde dont on sait qu'ils se livrent à des activités visant à perturber les élections. L'une des choses qui me préoccupent, c'est que, parfois, les acteurs étatiques ne se manifestent pas d'eux-mêmes. Ils utilisent d'autres entités, d'autres organisations et d'autres groupes agissant en leur nom pour perturber non seulement les élections, mais aussi d'autres activités dans d'autres pays.

Je ne veux pas que vous compromettiez vos tactiques à cet égard, mais comment composer avec une telle situation? Il s'agit là selon moi d'un problème. On note une importante prolifération. Comment faire face à tout ça? Il y a certaines entités que vous connaissez, et les gens savent que vous les connaissez, mais elles misent sur une foule de sous-entités indépendantes qui oeuvrent pour contribuer à la destruction d'une campagne. De quelle façon vous attaquez-vous à ce problème?

[*Français*]

M. André Boucher: Dans notre rapport de juin 2017, nous classons les menaces par catégories.

Je vais donner un exemple qui rejoint votre question. Effectivement, il y a de la synchronisation ou de la sous-traitance entre des États et peut-être entre des entités criminelles.

En réalité, nous surveillons toujours toutes les menaces. Les mesures de prévention et de détection des menaces et la façon d'y réagir sont en fonction de chaque groupe et non d'un groupe plus dominant. Nous surveillons tous les groupes. Certes, nous observons des interconnexions qui n'existaient pas auparavant. Des gens employés par d'autres deviennent des menaces et ne le savent pas. Il y a même des firmes qui croient fonctionner tout à fait légalement en exécutant un contrat, mais qui, en réalité, sont utilisées pour faire de la recherche pour d'autres. Ce phénomène est réel et nous sommes au courant. Nous faisons ce que nous pouvons.

Monsieur Rogers, voulez-vous ajouter quelque chose au sujet des menaces?

[*Traduction*]

M. Raj Saini: Monsieur le président, combien de temps me reste-t-il?

Le vice-président (M. Nathaniel Erskine-Smith): Vous avez 40 secondes.

M. Raj Saini: C'est ma dernière question puisque je manque de temps.

Évidemment, il y a maintenant différentes façons de communiquer avec le public. Nous utilisons des plateformes de médias sociaux comme Facebook et Twitter.

Travaillez-vous en collaboration avec ces entreprises de façon concertée pour vous assurer que, s'il y a des menaces, elles peuvent être rapidement éliminées, de façon à ce qu'elles ne prolifèrent pas au point où elles peuvent avoir un réel impact sur l'issue d'une campagne, qu'on parle de robots, de trolls ou de désinformation? Vous avez une relation avec ces entreprises? Selon moi, ce serait essentiel pour s'assurer qu'il n'y a pas de désinformation en ligne.

[*Français*]

M. André Boucher: Absolument. Pour protéger les Canadiens, le Centre canadien pour la cybersécurité utilise un modèle de collaboration, où tous les intervenants travaillent de concert. Cela passe par l'usager, comme M. Rogers l'a dit, par le manufacturier, par les gens qui produisent les codes sources et les logiciels et va jusqu'au fournisseur Internet. Ce dernier a aussi une responsabilité sociale et nous le traitons comme une entreprise canadienne. Si nous découvrons qu'il se passe quelque chose d'inhabituel, nous l'en avisons immédiatement. S'il ne l'a pas déjà détecté, il sera très réceptif et prendra immédiatement des mesures.

● (1145)

[*Traduction*]

M. Raj Saini: Merci.

Le vice-président (M. Nathaniel Erskine-Smith): Merci beaucoup.

Je crois savoir que M. Kent nous quittera bientôt, mais nous lui accorderons sept minutes avant son départ.

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

Je tiens à remercier tous les témoins qui ont comparu ce matin.

Je comprends que le Bureau de la concurrence et la Banque n'ont que des suggestions périphériques pouvant s'appliquer aux recommandations que nous ferons au gouvernement une fois que nous aurons terminé le rapport sur la vulnérabilité numérique du système électoral canadien ou les menaces qui pèsent sur le système électoral canadien. Par conséquent, je veux consacrer tout mon temps aux témoins du CST aujourd'hui.

En tant que politicien, je suis actif sur les médias sociaux presque uniquement pour des raisons politiques, et il y a d'importants avantages à utiliser Facebook, Instagram et les autres médias sociaux... Twitter.

Cette semaine, j'ai vécu tout personnellement la menace numérique lorsque mon compte Instagram a été piraté par quelqu'un à l'étranger. Mon compte Facebook a été piraté et il a fallu un certain temps pour que je puisse le récupérer.

Ça m'a rappelé la fameuse astuce de Beyoncé, dont des témoins ont déjà parlé devant le Comité. Aux États-Unis, dans le cadre des dernières élections fédérales, une page Facebook a été créée pour rendre hommage à Beyoncé. La page a accumulé des millions d'abonnés. Puis, dans les derniers jours de la campagne électorale — et tout ça avait été mis en place, d'après ce que j'ai compris, par des Russes d'un niveau ou d'un autre —, des messages ont été envoyés, et on a conclu au bout du compte que ces messages visaient à décourager les électeurs noirs d'aller voter dans le cadre de la campagne ou dans le cadre de certaines campagnes.

Nous avons demandé à l'un de nos témoins précédents, M. Ben Scott, de quelle façon les Canadiens pouvaient se protéger contre le genre de bombes à retardement que constitue ce genre de cheval de Troie des médias sociaux, cette bombe qui devait exploser au moment de la période électorale où les gens prennent leur décision. Il a laissé entendre que les organismes comme le CST utiliseraient l'approche de l'« équipe rouge » comme il l'a appelée, le jeu de la guerre froide dans le cadre duquel on tente de prévoir les menaces, de déterminer de quelle façon y réagir, la façon dont on pourrait considérer qu'il s'agit de tentatives frauduleuses de s'ingérer dans le processus électoral. Essentiellement, il a dit que les agences responsables de la sécurité ont la capacité — et je comprends que vous n'avez aucun pouvoir relativement aux médias sociaux —, c'est assurément le cas des agences de sécurité américaines, de déceler les interventions étrangères ou les acteurs étrangers présents dans les médias sociaux.

Pouvez-vous me dire ce que fait le CST dans ce domaine?

M. Dan Rogers: Certainement. Merci de poser la question.

Je répondrai du point de vue du renseignement étranger, ce qui relève de mon domaine. Ensuite, j'inviterai André à vous parler de certaines des consignes que nous donnons aux Canadiens pour leur permettre de faire face à ce genre de problèmes.

En tant qu'organisation responsable du renseignement étranger, nous suivons des cibles dans l'infrastructure de l'information mondiale, qui comprend les médias sociaux. Si le gouvernement nous donne des priorités en matière de renseignement, qui peuvent comprendre des activités comme la surveillance de pays étrangers qui auraient intérêt à perturber nos systèmes électoraux, nous examinons l'ensemble de l'infrastructure de l'information mondiale afin de déterminer quelles sont les activités, les capacités et les intentions de ces États étrangers.

Dans ce contexte, je ne peux pas expliquer de façon détaillée comment nous le faisons, mais je peux assurément affirmer qu'il s'agit d'une partie active de notre rôle consistant à observer ces activités dans la mesure où nous le pouvons. Nous regroupons ensuite cette information pour former des produits de renseignement étranger à fournir à nos partenaires du gouvernement et à l'équipe d'André, qui s'en servent pour éclairer certains de leurs conseils en matière de cybersécurité et leur travail auprès des personnes qui pourraient être touchées par ces activités.

André, souhaitez-vous prendre la parole à ce sujet?

M. André Boucher: Absolument.

Bien entendu, nous donnons déjà des conseils et des consignes sur la façon de sécuriser et d'utiliser les appareils, et ainsi de suite. Je laisserai cette question de côté. Simplement pour donner suite aux propos de Dan, une fois que les équipes sont informées du fait que des activités étrangères ont lieu, je pense que cela nous ramène à la question précédente. Voilà l'occasion qui se présente à nous. Nous disons à l'utilisateur de communiquer avec l'entreprise et de l'en informer, mais, comme nous avons également établi ces partenariats, nous informons aussi l'entreprise du fait que nous voyons des données probantes indiquant que quelque chose ne va pas en ce qui a trait aux services qu'elle fournit et qu'elle devrait peut-être diriger son attention là-dessus. Ce que nous tentons de faire, c'est de présenter cette information de la bonne manière aux intervenants qui peuvent vraiment faire quelque chose pour régler le problème.

● (1150)

L'hon. Peter Kent: L'étude que nous menons cette année, depuis qu'a éclaté le scandale de Cambridge Analytica, Facebook et AggregateIQ, comporte une importante quantité de témoignages selon lesquels les entreprises de mégadonnées se préoccupent davantage de l'élaboration de leurs plans d'affaires, de leurs profits et de la concurrence que de la protection des renseignements personnels.

D'après votre expérience d'affaires avec ces entreprises, seront-elles coopératives pour ce qui est de donner suite à vos conseils? Il n'est pas nécessaire que vous nommiez les entreprises, mais, à l'intention du public qui nous regarde, je veux parler de Facebook, d'Amazon, de Google, et ainsi de suite.

[*Français*]

M. André Boucher: La réponse très courte est oui, mais je vais quand même vous donner un peu de contexte.

Il faut être pragmatique. Je rencontre des conseils d'administration ou des présidents de compagnie pour discuter de la mise en place de mesures de sécurité, que ce soit pour protéger la vie privée ou pour assurer la sécurité en général, pour préserver la confidentialité, l'intégrité et la disponibilité des réseaux.

Le fournisseur de services doit atteindre un équilibre entre la rentabilité de son produit et son caractère sécuritaire. Il ne faut pas être naïf. Quand je demande aux gens de compagnies dans tous les domaines de s'assurer que leur produit ou leur service est sécuritaire, je dois leur donner des arguments convaincants pour qu'ils resserrent leurs mesures de sécurité. Le fait d'avoir de l'information pertinente sur une menace donnée nous aide à les convaincre. En fait, nous avons beaucoup de succès à cet égard.

[*Traduction*]

L'hon. Peter Kent: Merci beaucoup.

Le vice-président (M. Nathaniel Erskine-Smith): Les sept prochaines minutes sont accordées à la députée Mathyssen.

Mme Irene Mathyssen (London—Fanshawe, NPD): Merci beaucoup, monsieur le président.

Chers témoins, merci beaucoup de votre présence.

Il s'agit d'une mine d'information, et je vous en suis vraiment reconnaissante. Certains renseignements sont légèrement terrifiants, mais je suis certaine que nous les examinerons et déterminerons quelle est la meilleure façon de nous attaquer à cet enjeu de très grande envergure.

C'est probablement M. Durocher qui pourrait le mieux répondre à cette question. Hier, une poursuite a été intentée contre Facebook. On allègue que l'entreprise a manipulé les chiffres en ce qui concerne le nombre de personnes qui regardaient des vidéos sur son réseau. Bien entendu, il y a des conséquences pour les personnes qui travaillent dans le domaine des médias, celles qui rédigent des textes pour des organes médiatiques, et pour les annonceurs.

Je me demande si vous considéreriez cela comme un abus de pouvoir de marché. Cette manipulation a-t-elle de vastes répercussions en ce qui a trait à cette question?

M. Anthony Durocher: Merci beaucoup de poser la question.

Les dispositions concernant l'abus de pouvoir de marché de la Loi sur la concurrence du Canada visent en réalité les entreprises dominantes qui prennent des mesures visant à miner le processus concurrentiel et à tenir les concurrents hors du marché et à les empêcher de rivaliser avec elles. Si une société adoptait une conduite qui supposerait l'exercice d'un pouvoir sur le marché, comme le fait d'augmenter les prix, cela n'échapperait pas nécessairement au champ d'application de la Loi sur la concurrence. Elle vise en réalité à protéger le processus concurrentiel. Si on parle des grandes entreprises technologiques, notre rôle consiste vraiment à nous assurer que le processus concurrentiel est protégé et que les entreprises ont des possibilités de livrer concurrence à Facebook au moyen de leurs produits et services.

Mme Irene Mathyssen: Évidemment, Facebook profite du nombre de visionnements et de l'achalandage de son site pour vendre des espaces publicitaires. Cela semblait intéressant au vu de cette poursuite, alors je vous remercie de cette réponse.

Cette question s'adresse à la Banque du Canada.

Je me demande si la banque est le moindrement préoccupée par la concentration du marché et les entreprises phares. Vous avez décrit ce phénomène. La plupart de ces sociétés se trouvent aux États-Unis. Cette situation influe-t-elle sur la capacité des Canadiens d'établir un espace commercial numérisé et national de première qualité? Hormis cela, quelles sont les conséquences sur les détaillants?

● (1155)

M. Eric Santor: Merci beaucoup de poser la question. C'en est une bonne.

Ce que nous constatons, actuellement, dans l'économie canadienne, c'est qu'il y a beaucoup d'activités dans l'économie numérique. Même si nous n'avons pas de mesure explicite de cette économie, les éléments que nous examinons montrent l'existence d'une croissance très vigoureuse. Si on prend une mesure, par exemple, si on regarde le PIB par industrie, il y a une catégorie appelée « conception de systèmes informatiques et services connexes ». Elle affiche une croissance supérieure à 7 % par année depuis cinq ans. En valeur ajoutée, elle est aussi importante que les catégories de l'automobile et l'aérospatiale combinées. Alors, il y a une croissance très rapide; il se passe beaucoup de choses.

Si on adopte une approche empirique et qu'on regarde des centres comme Toronto, Montréal, le corridor de Waterloo, Edmonton et d'autres endroits, il y a beaucoup d'activités numériques, et beaucoup d'investissements sont effectués dans la PI ainsi que dans la recherche et développement. En outre, cette situation a suscité l'intérêt de gros joueurs qui apportent des IDE au Canada et s'établissent ici, afin de profiter du bassin de talents dont nous disposons en ce qui a trait aux mégadonnées, à l'IA et à l'AM. Selon un paramètre, le Canada possède le troisième plus grand nombre de chercheurs en IA et en langage machine, alors nous sommes bien placés pour tirer profit de cette situation, et nous la considérons comme un très puissant moteur de l'économie canadienne actuellement.

Mme Irene Mathyssen: Ainsi, l'exode des cerveaux que nous semblons toujours craindre n'est pas une réalité. Nous attirons effectivement des professionnels hautement qualifiés et les gardons.

M. Eric Santor: Oui. Le marché de l'emploi est très concurrentiel pour les scientifiques des données et les personnes qui s'y connaissent en IA et en AM, mais nous sommes très bien placés. Nous produisons beaucoup de talents, nous-mêmes, et nous en attirons également.

Mme Irene Mathyssen: D'accord. Merci beaucoup.

Monsieur Durocher, l'Union européenne a adopté l'approche proactive d'exécution des lois antitrust pour agir contre les monopoles de données comme Google. Je me demande si vous pouvez expliquer la distinction entre les approches canadienne et européenne à cet égard.

M. Anthony Durocher: Bien sûr. Il s'agit d'un élément important, et je peux vous dire que le Bureau de la concurrence surveille de très près ce qui se passe en Europe et ailleurs dans le monde. Quand nous regardons ces grandes entreprises, il s'agit d'un problème mondial, qui n'est pas propre au Canada. Ce qui importe, c'est que nous collaborions. Nous savons ce qui se passe ailleurs, quels outils les autres pays utilisent, et nous pouvons ainsi nous assurer qu'ici, au Canada, nous employons des méthodes de pointe. Le fait que l'Union européenne a intenté deux poursuites contre Google n'est pas un secret. En outre, une enquête a récemment été annoncée contre Amazon. L'autorité allemande en matière de concurrence a elle aussi intenté des poursuites contre Facebook, lesquelles sont toujours en cours.

Ce que je peux vous dire, c'est qu'il importe d'être conscient de la distinction non seulement du point de vue de la dynamique concurrentielle, mais aussi au chapitre des lois entre l'Europe et le Canada. La loi canadienne régissant l'abus de position dominante est bien établie depuis 1986, et il existe une jurisprudence au sujet des éléments qui doivent être présents pour que l'on puisse intenter une poursuite. Tout le travail que nous faisons consiste en réalité à faire appliquer la loi en nous fondant sur des principes et sur des données probantes. Au Canada, les décisions que nous prenons sont vraiment éclairées par les données probantes dont nous disposons et par tout préjudice pour le marché canadien. En ce qui concerne Google en particulier, en 2016, nous avons clos une très longue enquête de trois ans contre cette société, qui portait sur certaines de ses pratiques, et Google a pris un engagement à l'égard d'un problème de concurrence que nous avions cerné. Toutefois, nous surveillons désormais de près nos homologues internationaux et travaillons avec eux dans le but de nous assurer qu'ici, au Canada, nous dominons la situation.

Le vice-président (M. Nathaniel Erskine-Smith): Merci beaucoup.

Nos sept dernières minutes sont accordées à M. Picard.

[*Français*]

M. Michel Picard (Montarville, Lib.): Je vous remercie, monsieur le président.

Ma question s'adresse aux gens du Bureau de la concurrence.

Si Facebook remettait un nombre important de données privées à une partie pour des analyses quelconques et que cette partie concluait un accord avec une tierce partie sur laquelle nous n'aurions aucun contrôle, de l'information serait diffusée partout, sans contrôle. La tierce partie qui mettrait la main sur ces métadonnées en vertu d'une entente cachée ou carrément criminelle — elle n'aurait pas le droit de les vendre mais elle le ferait quand même — exercerait-elle une concurrence déloyale?

● (1200)

Mme Alexa Gendron-O'Donnell (sous-commissaire déléguée, Direction de l'analyse économique, Direction générale de la promotion de la concurrence, Bureau de la concurrence): Je vous remercie beaucoup de votre question.

Permettez-moi de continuer en anglais.

[*Traduction*]

En plus des dispositions dont a parlé mon collègue, le Bureau de la concurrence applique également ce que nous appelons une disposition visant les déclarations fausses ou trompeuses. Quand je parle de déclarations, j'entends par là le matériel de marketing, les annonces en ligne, les messages dans les médias sociaux et même les conditions d'utilisation. L'essentiel, sous le régime de la Loi sur la concurrence, c'est que l'impression générale que vous donnez doit être véridique. La publicité doit contenir des affirmations véridiques. Lorsqu'il s'agit de promouvoir vos intérêts commerciaux ou de recueillir des renseignements sur les consommateurs, vous devez être honnête. Voilà la disposition de la loi qui serait appliquée si une entreprise songeait à adresser un certain genre de déclarations aux consommateurs, qu'il s'agisse de leur vendre un produit ou de leur offrir ce que j'appellerais un produit gratuit en échange de leurs renseignements. Il faut respecter la loi dans ces cas-là.

[*Français*]

M. Michel Picard: Le réseau social qui me demande de lui donner des informations pour m'inscrire est très transparent. Dans ses conditions, il dit clairement que ses partenaires et lui-même ont le droit d'utiliser mes données. C'est très transparent, mais je n'ai aucune idée de qui sont ses partenaires.

Mme Alexa Gendron-O'Donnell: C'est cela. Je vais poursuivre ma réponse.

[*Traduction*]

En réalité, il est question des dispositions relatives à la publicité trompeuse. Nous encourageons les entreprises à être claires, mais, ce qui est le plus important, c'est de ne pas tromper les gens. On ne peut pas dire aux consommateurs qu'on va faire une chose, puis en faire une autre. En réalité, les dispositions relatives à la concurrence visent à garantir que des messages publicitaires véridiques sont adressés à ces consommateurs, de sorte qu'ils sachent, lorsqu'ils sont sur le point d'acheter un produit ou de donner des renseignements, qu'il y a peut-être une possibilité que ces renseignements soient transmis à un tiers ou qu'ils soient utilisés ailleurs.

M. Michel Picard: Toutefois, les entreprises n'assument pas la responsabilité à l'égard des activités du partenaire. Elles n'assument pas la responsabilité à l'égard de ce que fera le partenaire des données qu'elles lui transmettent. Si j'accepte d'échanger mes médias sociaux avec un partenaire et qu'il fait quelque chose d'entièrement différent, je vais en faire part au CST par après. Toutefois, si tout est inscrit dans le contrat, que c'est transparent et que rien n'est trompeur, alors, il s'agit d'une simple omission. À vos yeux, une « omission » est-elle différente d'une information « trompeuse »?

Mme Alexa Gendron-O'Donnell: L'essentiel, en ce qui concerne la commission, c'est qu'il faut simplement s'assurer que la déclaration adressée aux consommateurs est véridique. Il s'agit vraiment du cœur de la loi. Certes, si, à tout moment, l'entreprise secondaire adresse une déclaration aux consommateurs, elle doit absolument s'assurer qu'elle est véridique.

M. Michel Picard: Je m'adresse aux représentants du CST. Disons qu'un tiers, dans une situation hypothétique, détient des millions et des millions de données. Vous avez mentionné que la menace s'accroît, surtout pour 2019. Pouvez-vous préciser la nature de la menace? S'agit-il d'un plus grand nombre de personnes, d'institutions ou d'associations, de sociétés ou de gouvernements, ou bien est-ce l'ensemble des trois premiers sous l'égide d'un gouvernement étranger?

M. Dan Rogers: [*Note de la rédaction: inaudible*]

[*Français*]

M. André Boucher: Il ne faut pas perdre de vue que les menaces sont catégorisées et que nous les examinons en fonction de leur catégorie. Cela nous donne de l'information sur les mesures ou les méthodes que ces entreprises utilisent normalement. Les moyens que nous prenons sont fonction de la catégorie de menaces.

M. Michel Picard: Voici le défi auquel on fait face en ce moment.

Normalement, le CST se concentre sur les sources étrangères, non canadiennes. Or, en renseignement électromagnétique, les signaux n'a pas de citoyenneté. En ce qui concerne les signaux venant d'un pays étranger, on ne sait pas qui est assis au clavier. Cela peut être un Canadien comme un étranger.

Comment peut-on faire la distinction? Comment peut-on identifier la menace pour s'assurer, d'une part, qu'il s'agit bien de signaux étrangers et, d'autre part, qu'on a l'autorité d'agir, puisqu'il faut agir, à un moment donné.

[*Traduction*]

M. Dan Rogers: Vous avez tout à fait raison. Le CST, conformément à son mandat et à la loi, ne peut pas, dans le cadre de ses activités, viser quelque chose ou quelqu'un qui se trouve au Canada. Notre programme de renseignement électromagnétique étranger vise exclusivement les communications étrangères.

Je ne peux pas vous donner de détails sur la façon dont nous le faisons, mais je peux affirmer que, dans les situations où nous recueillons de l'information, c'est conformément aux priorités établies par le gouvernement du Canada. Pour nous, cela signifie que nous commençons toute activité de collecte de renseignement par le volet étranger et qu'à partir de là, nous élaborons nos produits de renseignement. Nous nous attachons d'abord aux cas où nous pouvons déceler une connexion étrangère ou quelque chose, puis nous évaluons la situation à partir de là. Nous ne commençons jamais par un élément canadien ou inconnu qui n'est pas clairement lié à une priorité du gouvernement du Canada en matière de renseignement ou à une organisation ou personne étrangères.

● (1205)

M. Michel Picard: Si vous êtes une entité qui tente de cibler notre démocratie — un processus en général, comme un système électoral —, soit que vous attaquez une personne afin qu'elle perde parce que ses politiques vont à l'encontre de vos intérêts, soit que vous appuyez une personne, qui devra payer quelque chose en retour, parce qu'on ne fait pas de cadeaux.

Une fois que vous repérez l'attaque en soi, allez-vous plus loin, pour demander ce qui se cache derrière tout cela et déterminer ce qui a justifié ce genre d'attaque?

M. Dan Rogers: Oui. Nous produisons du renseignement portant exactement sur ce que demande le gouvernement. Dans la loi, c'est désigné par les termes « capacités », « intentions »... Je ne veux pas me tromper de termes, mais nous examinons les capacités, les activités et les motivations des États étrangers. C'est inclus dans le volet du renseignement étranger. Nous cherchons à trouver le plus possible d'informations riches à ce sujet, à fournir au gouvernement ou à d'autres partenaires qui pourront prendre des mesures afin d'intervenir.

M. Michel Picard: Le SCRS participe-t-il à ces interventions?

M. Dan Rogers: Certainement, nous travaillons avec le SCRS, de même qu'avec Affaires mondiales Canada, la GRC et d'autres partenaires nationaux. Dans le cadre de leur mandat, ils utilisent nos renseignements.

Le vice-président (M. Nathaniel Erskine-Smith): Merci beaucoup.

Nous allons passer à la première période de cinq minutes et donner la parole à M. Gourde.

[*Français*]

M. Jacques Gourde (Lévis—Lotbinière, PCC): Monsieur le président, ma première question s'adresse au Centre de la sécurité des télécommunications, le CST.

Pendant une campagne électorale qui dure de 35 à 40 jours, de nombreuses informations numériques peuvent désormais être affichées sur différentes plateformes. Advenant une attaque, avec quelle rapidité pouvez-vous réagir pour y mettre fin? Si Élections Canada prend deux ou trois jours pour s'apercevoir d'une attaque avant d'émettre un rapport, les dégâts se poursuivent pendant ce temps-là.

Que pouvez-vous me dire pour me rassurer à ce sujet?

M. André Boucher: C'est une excellente question.

Dans les faits, le CST protège déjà le gouvernement canadien. Au fil des ans, il a fallu apprendre à faire face à ce genre de menace. Vous avez entièrement raison. Si cela nous prenait deux jours pour réagir, nous serions dans une très mauvaise posture. Nous avons donc mis en place des systèmes capables de détecter et de suivre une menace à sa vitesse, ce que nous appelons dans notre jargon travailler « à la vitesse de cyber ».

C'est exactement ce qui se passe pour Élections Canada, une agence avec laquelle nous travaillons depuis 2015. Nous l'aidons à sécuriser ses réseaux et nous mettons en place les outils, les systèmes et les processus relationnels requis, ce qui fait que le temps de réaction à une menace se compte en minutes, et non en heures ou en jours.

M. Jacques Gourde: Vous parlez du système d'Élections Canada, mais je m'intéresse plutôt aux fausses informations qui circulent sur certaines plateformes.

On a beau démentir ces fausses informations, cela prend un certain temps et le mal est déjà fait, sans compter que le démenti ne rejoint souvent qu'une proportion minime de l'auditoire qui avait pris connaissance de la fausse nouvelle initiale. Cela s'est beaucoup vu aux États-Unis, où la détermination d'une fausse nouvelle ne survient que trois ou quatre jours après sa diffusion. Peut-on se prémunir contre une pareille situation, ou va-t-on désormais devoir vivre avec cette réalité?

M. André Boucher: Nos responsabilités en cybersécurité en vertu de notre mandat limitent ce que nous pouvons faire pour vous aider. Le mieux que nous puissions faire est d'aider à prévenir les problèmes et de nous assurer que les gens ne se retrouvent pas dans une mauvaise posture.

Vous soulevez un argument très valable. Cependant, une fois que la menace s'est manifestée, le Centre canadien pour la cybersécurité ne peut malheureusement plus y faire grand chose.

M. Jacques Gourde: Quelles seraient nos limites en tant que législateurs si nous voulions modifier certaines lois liées aux télécommunications pour tenter d'améliorer la situation? Notre autorité se limite au Canada, et nos lois ne s'appliquent pas si nous sommes attaqués de l'étranger. Il semble donc que nous soyons limités face à cette réalité.

M. André Boucher: Je ne suis pas un expert en matière juridique. Je peux cependant vous dire que l'expérience démontre que nous avons réussi en vertu des lois actuelles à allier la protection des individus à celle des systèmes pour défendre le gouvernement canadien de façon très efficace. J'espère que cette preuve vous rassure.

● (1210)

M. Jacques Gourde: Pensez-vous que les Canadiens puissent envisager avec confiance le respect de la démocratie lors de la prochaine campagne électorale, compte tenu de la réalité qui existe depuis quatre ou cinq ans?

M. André Boucher: Je suis extrêmement confiant, et je suis convaincu que les Canadiens devraient eux aussi avoir confiance. C'est le message que je donne à mes propres enfants: allez voter en toute confiance, parce que cela fait maintenant des années que de nombreux efforts sont déployés pour garantir la solidité de notre processus démocratique.

M. Jacques Gourde: Je vous remercie.

[*Traduction*]

Le vice-président (M. Nathaniel Erskine-Smith): Merci beaucoup.

Les cinq prochaines minutes sont accordées à Mme Vandenbeld.

Mme Anita Vandenbeld (Ottawa-Ouest—Nepean, Lib.): Merci beaucoup. Ma première question s'adresse à MM. Rogers et Boucher, et elle nous ramène à l'idée de qui est ciblé.

Monsieur Rogers, je crois que vous avez mentionné que c'est plus les politiciens que les élections en tant que telles qui sont ciblés. Trouvez-vous également que les candidates et les politiciennes sont ciblées davantage?

M. Dan Rogers: Mon expérience ne me permet pas de l'affirmer.

Je ne sais pas — André — si vous avez une réponse à fournir.

[*Français*]

M. André Boucher: En fait, l'étude ne va pas à ce niveau de détail. Quand nous avons regardé le problème dans son ensemble, nous nous sommes rendus compte que nous pouvions faire quelque chose du côté d'Élections Canada et de la machinerie pour ce qui est du processus démocratique. Toutefois, c'était dans les politiciens, les partis politique et les médias, des secteurs qui ratissent large, qu'il valait la peine d'investir.

[*Traduction*]

Mme Anita Vandenbeld: D'un point de vue empirique, nous avons entendu beaucoup de témoignages selon lesquels les femmes et les candidates sont ciblées, plus particulièrement par l'intermédiaire des plateformes de médias sociaux. Des données ventilées en fonction du sexe pourraient être utiles au Comité, à un moment donné.

M. Dan Rogers: D'accord.

Mme Anita Vandenbeld: Monsieur Santor, il est question de notre capacité de réglementer notre monnaie, parce que les données, en soi, sont en train de devenir une monnaie. Nous avons vu les échanges: vous recevez un café gratuit si vous nous donnez votre adresse de courriel. Ensuite, bien entendu, les agrégateurs de données achètent et vendent ces renseignements à grande échelle.

Nous avons constaté dans le cadre de notre étude de Cambridge Analytica et de SCL que, d'après certaines des données qui ont été trouvées en ligne, on avait commencé à travailler sur un jeton Midas, une cryptomonnaie.

Quelle est la menace? Si nous commençons à considérer les données comme une monnaie mondiale et qu'il sera peut-être possible d'être payé au moyen de l'une de ces cryptomonnaies, est-ce que cela mine notre capacité de réglementer notre système monétaire?

M. Eric Santor: Non, je ne pense pas que ce soit le cas. C'est une question très intéressante, et je suis certain que nous devrons l'étudier à mesure que la numérisation se produit dans de nombreux différents aspects de notre vie. Toutefois, nous avons pleinement confiance en notre monnaie.

Mme Anita Vandenbeld: C'est très bon à savoir.

Je voudrais aussi aborder la question de la concurrence. En tant que législateurs, nous avons pour mandat d'adopter des lois. En ce qui concerne la Loi sur la concurrence, Monsieur Santor, vous avez affirmé que notre politique en matière de concurrence n'a pas besoin d'être modifiée, qu'il faut simplement y ajouter des outils; toutefois, monsieur Durocher, je pense que vous avez laissé entendre que nous devons apporter certains types de modifications à notre Loi sur la concurrence. Ai-je bien compris?

M. Anthony Durocher: Je pense que, dans ma déclaration préliminaire, j'ai mentionné qu'à la suite de notre étude sur la question, nous avons déterminé que le cadre actuel était à la hauteur.

Ce qui compte, en réalité, ce sont les outils que nous utilisons. Avant de formuler ma réponse, j'affirmerai que le Bureau de la concurrence n'a pas pour mandat d'examiner la politique en matière de concurrence. Notre travail est du côté de l'application de la loi, et c'est Innovation, Sciences et Développement économique qui exerce maintenant la fonction relative à la politique en matière de concurrence. Toutefois, il est certain que notre plus grande priorité est de nous assurer que nous disposons des outils nécessaires pour nous occuper de l'économie numérique, et nous voyons de nouveaux problèmes se présenter. Voilà sur quoi nous nous concentrons, et voilà pourquoi nous établissons beaucoup de priorités, tenons des consultations et restons à l'affût des faits nouveaux aux échelons national et international.

Mme Anita Vandenbeld: Nous avons entendu beaucoup de ces plateformes de médias sociaux, comme Facebook, se faire appeler des monopoles de données — je pense que M. Santor a parlé de « plateformes phares ». Le fait est que les gens n'ont pas vraiment le choix. S'ils sont sur Facebook, toutes leurs données sont sur ce site — leurs photographies, les membres de leur famille, toutes leurs relations, leurs réseaux... Pour se déconnecter de Facebook et aller sur une autre plateforme, tant que ces données sont conservées par Facebook, c'est très difficile pour les gens parce que c'est devenu une partie très importante de notre norme sociale. Ces plateformes sont essentiellement devenues des monopoles.

Je cherche à savoir si les outils dont nous disposons actuellement dans les lois sont suffisants pour nous permettre de faire face à ce nouveau genre de monopole, c'est-à-dire ces vastes plateformes de données.

● (1215)

M. Anthony Durocher: Le cadre de concurrence actuel du Canada n'est pas conçu pour pénaliser les monopoles en soi. Le processus concurrentiel garantit que les sociétés qui innovent, qui investissent et qui procurent aux consommateurs un produit souhaitable ne seront pas punies pour l'avoir fait. Notre tâche consiste à nous assurer que ces marchés demeurent disputables grâce à la concurrence fondée sur le mérite et que les petites sociétés et les entreprises, existantes ou nouvelles ont la possibilité de livrer une concurrence fondée sur le mérite des produits et services qu'elles fournissent aux utilisateurs.

Certes, nous sommes attentifs à ce qui se passe à l'échelon international sur ce front également, et nous avons remarqué que le RGPD contient des dispositions relatives à la portabilité des données, qui valent la peine d'être soulignées du point de vue de la concurrence également. Nous continuons à nous concentrer sur le fait de nous assurer que nous disposons d'outils de pointe pour travailler là-dessus. Dans le cadre de nos très vastes consultations liées à notre document sur les données, nous avons rencontré des représentants des milieux commercial, juridique et universitaire.

Il n'y a pas de réponses à cette question. Il n'existe aucune solution miracle. Toutefois, nous sommes convaincus d'avoir les outils nécessaires pour nous attaquer au problème. Nous allons les tenir à jour.

Le vice-président (M. Nathaniel Erskine-Smith): Merci beaucoup.

Les cinq prochaines minutes seront partagées entre M. Van Kesteren et M. Gourde, mais M. Van Kesteren va commencer.

M. Dave Van Kesteren (Chatham-Kent—Leamington, PCC): Merci, monsieur le président.

Merci à tous de votre présence.

Je ne suis habituellement pas membre de ce comité, mais j'y ai siégé, en fait, la première fois que j'ai été élu, il y a 12 ans, alors c'est pour moi un genre de retour au bercail.

Je pense que la plupart des Canadiens présument que le Centre de la sécurité des télécommunications est digne de confiance. Nous croyons en nos institutions canadiennes, et je souscris à cette opinion. Je pense que vous faites de l'excellent travail.

Je suis curieux. Combien de personnes travaillent pour votre organisme?

M. Dan Rogers: Je pense qu'en ce moment, le nombre s'élève à environ 2 500.

M. Dave Van Kesteren: Combien?

M. Dan Rogers: Deux mille cinq cents.

M. Dave Van Kesteren: Il y en a 2 500. C'est un assez bon nombre, mais, quand on regarde la NSA, par exemple, aux États-Unis, et qu'on examine... tout d'abord, juste à voir la grosseur de leurs immeubles. Ils sont des milliers et des milliers.

Comme je l'ai affirmé dans ma déclaration préliminaire, la plupart des gens font confiance à votre organisation, mais qu'est-ce qui nous assure que des organisations comme la NSA...?

Mark Zuckerberg a comparu devant le Congrès il y a quelques mois, et de vraies accusations avaient été déposées auparavant. Il y avait une collaboration entre cette organisation, la CIA et un certain nombre d'autres. Comment pouvons-nous savoir que tous nos renseignements, tout le travail que nous faisons sur tous nos dossiers, ne sont pas tout simplement transmis là-bas?

M. Dan Rogers: Je vous remercie de la question intéressante et de vos commentaires au sujet de la confiance à l'égard du CST.

Dans notre contexte, nous entretenons une relation très étroite avec nos partenaires du Groupe des cinq et avec nos alliés internationaux dans ce domaine depuis très longtemps, soit 70 ans. Cette alliance repose sur un ensemble de valeurs communes relativement à des éléments comme la protection des institutions démocratiques et l'établissement d'une relation de confiance entre nos pays. Nous avons établi des conventions dans le domaine du renseignement afin que nous ne ciblions pas les citoyens les uns des autres, et chacun de nous s'assure depuis longtemps qu'il prend des mesures de protection de la vie privée à l'égard de ses citoyens et de ceux des autres pays. Dans le milieu du renseignement, il s'agit d'une pratique de longue date qui perdure aujourd'hui.

M. Dave Van Kesteren: J'ai choisi les États-Unis, qui sont le groupe le plus important, selon moi, qui aurait la capacité de faire je ne sais quoi, mais, bien entendu, les Chinois ne sont pas loin derrière, et nous avons récemment entendu des comptes rendus perturbants de... Aidez-moi, quelqu'un.

Mme Irene Mathyssen: Huawei.

M. Dave Van Kesteren: Huawei. Selon moi, ce sont plutôt ces enjeux qui préoccupent les Canadiens d'une certaine manière. Je sais que c'est certainement mon cas.

De quoi disposons-nous, dans notre mécanisme de défense, pour nous protéger contre ce type d'attaque étrangère?

M. André Boucher: Cela concerne le volet sécurité de votre organisation.

Peut-être pourrait-on ajouter un peu aux propos tenus par Dan au sujet de l'équipe et de sa taille. Le pouvoir de 2 500 personnes est en réalité celui de 2 500 plus nos collègues du Groupe des cinq, et cela nous aide à croître, quand nous faisons face à des menaces étrangères de divers types, de tous les genres. Nous travaillons en très étroite collaboration. Nous échangeons des conseils et des consignes, ainsi que les points de vue sur la nature des menaces, les méthodes qui sont employées, et ce qu'il faut faire à ce sujet.

Quant aux technologies et aux pays particuliers, bien entendu, il y a des moments où, au sein du Groupe des cinq, nous pouvons avoir des opinions et des points de vue divergents, mais il faut s'y attendre, car nous venons de pays différents. Nos organisations et nos droits souverains sont différents, de même que nos systèmes, en fait, et nous assurons déjà une présence distincte. Vous nous voyez peut-être parfois tenir des discussions entre nous, car notre situation est différente. Nous prenons des mesures différentes, mais, au bout du compte, dans le cadre de nos négociations, lorsque nous discutons et étudions des situations semblables, nous arrivons toujours à la même conclusion. Là où il pourrait y avoir des différences superficielles, je vous assure que, là où cela compte vraiment, en profondeur, nos opinions concordent parfaitement, et c'est le cas depuis 70 ans.

● (1220)

Le vice-président (M. Nathaniel Erskine-Smith): Monsieur Gourde, vous disposez de 30 secondes.

[*Français*]

M. Jacques Gourde: Je serai bref.

Au Canada, la sécurité des renseignements confidentiels est très importante. Par exemple, si on ne donne pas ses numéros de cellulaire ou ses adresses de courriel, ils resteront confidentiels.

Il y a deux ans, j'étais en Floride, où il y a un répertoire public. Je suis allé sur une plateforme, j'ai tapé mon nom ainsi que mon adresse, car je voulais savoir si un numéro de téléphone apparaîtrait. Tous mes numéros de téléphone cellulaire et toutes mes adresses de courriel sont apparus à l'écran. Nous ne pouvons pas faire cela au Canada. Les renseignements personnels des Canadiens sont sécurisés et confidentiels, mais ils ne le sont pas dans les autres pays.

Y a-t-il quelque chose que nous pouvons faire pour remédier à cela?

M. André Boucher: Dans l'exemple que vous avez donné, c'est un peu comme les anciennes pages blanches et pages jaunes du bottin téléphonique qui était distribué. Il y a différents degrés d'information. Si votre information est apparue sur Internet, alors, elle est partout dans le monde, car elle est sur des serveurs globaux. Si vous aviez fait la même recherche au Canada, vous auriez probablement trouvé la même chose.

Ce qui est privé, c'est l'information qui se trouve sur votre appareil et que vous n'avez pas partagée. Cela revient à des questions antérieures. Il faut être très prudent, lorsqu'on partage de l'information. Il faut lire attentivement les contrats d'utilisation et savoir à quoi on s'engage, parce que c'est un réseau public.

[*Traduction*]

Le vice-président (M. Nathaniel Erskine-Smith): Merci beaucoup.

Les cinq prochaines minutes sont accordées à M. Baylis.

M. Frank Baylis (Pierrefonds—Dollard, Lib.): Merci, monsieur le président.

Monsieur Durocher, vous avez affirmé avoir mené une enquête sur Google. Quel était l'objet de l'enquête? Vous avez dit que la société s'était engagée à arrêter de faire quelque chose. Quelle activité s'est-elle engagée à cesser?

M. Anthony Durocher: Essentiellement, l'enquête était axée sur la publicité dans le moteur de recherche et sur l'affichage publicitaire. De façon générale, nous avons étudié sept hypothèses possibles de façons dont ces éléments pouvaient nuire à la concurrence ou dont les actes de Google faisaient augmenter les coûts de ses rivaux. Selon la prépondérance de la preuve, nous avons conclu qu'une seule de ces hypothèses justifiait la prise de mesures, et elle concernait essentiellement ce qu'on appelle les conditions d'utilisation de l'interface API d'AdWords.

C'est une question d'ordre plutôt technique, mais les annonceurs dans l'économie numérique doivent parfois gérer des campagnes sur diverses plateformes, et, essentiellement, l'inclusion de certaines conditions à cet égard empêchait les annonceurs de le faire efficacement et d'avoir recours aux rivaux de Google. Ce problème a été réglé grâce à un engagement de cinq ans qui prévoyait que la société n'adopterait pas ces conditions au Canada.

Je devrais souligner que la Federal Trade Commission, qui est notre agence sœur aux États-Unis, avait déjà effectué un examen et découvert le même problème, elle aussi.

M. Frank Baylis: Ce qui me préoccupe, comme il a déjà été mentionné, c'est que l'Union européenne et sa commissaire, Margrethe Vestager, qui s'occupe des pratiques anticoncurrentielles, ont infligé une amende de 3,6 milliards de dollars à Google. Elle a dit: « Google a abusé de sa position dominante sur le marché des moteurs de recherche en favorisant son propre service de comparaison de prix dans ses résultats de recherche et en rétrogradant ceux de ses concurrents. »

Tout d'abord, cela a également toutes les apparences d'une activité anticoncurrentielle, selon nos règles. Avez-vous mené une enquête là-dessus?

M. Anthony Durocher: C'est une excellente question.

C'est pourquoi il est important de reconnaître que les dynamiques concurrentielles ne sont pas nécessairement les mêmes dans tous les pays. La Commission européenne a rendu deux décisions concernant Google. Celle que vous avez mentionnée concerne Google Shopping. Google Shopping ne figurait pas en avant-plan dans notre examen, car la nature du service qui a été introduit au Canada était très... Il est arrivé en 2016. La mise en place des services ne se fait pas de la même façon dans tous les pays. C'est pourquoi, lorsque nous examinons ce que font les autres organismes, nous devons admettre que la nature des services qui sont offerts et les dynamiques concurrentielles ne sont pas nécessairement les mêmes qu'au Canada.

● (1225)

M. Frank Baylis: Vous êtes en train de dire que Google ne faisait pas en Europe, ce qu'il faisait au Canada? N'avions-nous pas de lois pour l'empêcher de le faire au Canada?

M. Anthony Durocher: Je dirais que les éléments de preuve portent à croire qu'aux termes de nos lois, le problème ne se posait pas.

M. Frank Baylis: Cela signifie que Google pourrait faire exactement les mêmes choses qu'en Europe qu'ici, mais en Europe, c'est assez grave pour qu'il reçoive une amende de 3,6 milliards de dollars, et on dit qu'ici, il n'est pas touché par nos lois. Ai-je bien compris?

M. Anthony Durocher: Nous sommes un organisme qui se fonde sur la preuve, et je dirais que les éléments de preuve, en ce qui concerne les pays d'Europe, ne sont pas les mêmes que ceux que nous examinerions ici, et c'est pareil pour le contexte commercial...

M. Frank Baylis: Les lois sont structurées de telle sorte que la même chose pourrait se produire en Europe et ici, mais ici ce n'est pas un problème, et là-bas il est question d'une amende de 3,6 milliards de dollars.

M. Anthony Durocher: Pas nécessairement. Si certains éléments de preuve montraient que Google ne se conforme pas à nos dispositions sur l'abus de position dominante, je peux vous assurer que nous prendrions pris des mesures.

M. Frank Baylis: Mais je veux parler des abus — selon nos lois — qui ont lieu là-bas.

M. Anthony Durocher: Oui.

M. Frank Baylis: Plus précisément, si ce qui s'est produit en Europe s'était produit ici, serait-il hors-la-loi et écoperait-il d'une grosse amende comme celle-ci? Oui ou non; c'est une question simple.

M. Anthony Durocher: Je ne peux pas formuler d'hypothèses sur ce que Google a fait en Europe ni vous dire si cela pourrait s'appliquer ici, car c'est...

M. Frank Baylis: D'accord, si vous n'avez pas encore examiné la question...

M. Anthony Durocher: Nous nous fions aux éléments de preuve.

M. Frank Baylis: Combien d'amendes pour pratique anticoncurrentielle sont de l'ordre de 3,6 milliards de dollars? Il ne doit pas y en avoir des dizaines, trop pour que vous puissiez les examiner. Votre bureau n'a pas pris le temps d'examiner ce que Google fait là-bas pour savoir s'il fait la même chose ici. C'est une société multinationale; c'est un moteur de recherche multinational.

Nous allons garder cela en mémoire.

Monsieur Santor, je crois que vous avez dit que les banques pensaient que nos politiques peuvent être modernisées. C'était l'une de vos déclarations. Comment serait-il possible? Que doit-on examiner pour les moderniser?

M. Eric Santor: C'était une déclaration générale, c'est-à-dire que, tant que l'économie évolue et que la numérisation se poursuit, nous ne sommes pas responsables, mais quand de nouvelles formes de concurrences utilisant de nouvelles technologies apparaissent, il serait raisonnable de s'attendre à ce que nous réfléchissions à la meilleure façon de moderniser nos pratiques afin de...

M. Frank Baylis: Si vous pensez que cela devrait être le cas, que devrions-nous faire?

M. Eric Santor: Il appartiendrait au bureau de la concurrence et aux législateurs de le déterminer. Ce que je disais, c'est que l'économie évolue et que nous devons donc faire évoluer nos pratiques également, pour comprendre en quoi les mégadonnées affectent la concurrence, car c'est quelque chose de nouveau.

M. Frank Baylis: Ce qui me préoccupe, c'est de voir qu'un phénomène de cette ampleur se produit. C'est l'une des choses que j'ai entendues. D'autres personnes ont déposé des plaintes contre l'entreprise qui utilise son moteur de recherche pour diriger les utilisateurs vers ce qui l'avantage financièrement, et qui nuirait à ses concurrents. J'ai lu quelque chose sur une personne qui a élaboré un meilleur moteur de recherche, et l'entreprise l'a bel et bien fait disparaître. Elle fait souvent ça.

Je ne peux pas croire que cela se produit seulement en Europe et, si cela se produit seulement en Europe — et je ne le crois pas —, ma préoccupation, c'est que nos lois ne vous permettent pas de faire votre travail. C'est ce que j'essaie de savoir, monsieur Durocher.

Le vice-président (M. Nathaniel Erskine-Smith): Malheureusement, nous avons largement dépassé la limite des cinq minutes.

Merci, monsieur Baylis.

Les trois dernières minutes seront pour Mme Mathyssen.

Mme Irene Mathyssen: Merci.

Je pense que la question la plus logique à poser est la suivante: nos lois vous permettent-elles de faire votre travail?

M. Anthony Durocher: Je pense qu'il est important de dire oui. Les Canadiens seront rassurés de savoir que nous prenons toutes les mesures nécessaires pour enquêter rigoureusement et intervenir s'il y a lieu. Le principe sous-jacent doit être le suivant: nous prenons des décisions fondées sur les principes et sur les éléments de preuve. Nous ne pouvons pas laisser la théorie dicter nos actes au titre de la Loi sur la concurrence. Je vous dirais que c'est une importante leçon à retenir.

L'un de ces géants du numérique a-t-il adopté un comportement qui vise à nuire ses concurrents et qui pourrait très bien soulever des problèmes au titre de la Loi sur la concurrence? Ce sont sur ces types de problèmes que nous allons mener une enquête, mais les éléments de preuve doivent nous y mener.

Mme Irene Mathyssen: Merci. Je pense, en ce qui concerne Huawei, que c'est un peu ce qu'on nous a dit, que l'entreprise nuisait en effet aux sociétés canadiennes. Dans le cas de Huawei, est Nortel, aujourd'hui disparue, qui a été touchée.

Pensez-vous qu'avec le système de cryptage intégré, les actions indirectes des acteurs mal intentionnés risquent de compromettre pour de bon le système de cryptage?

● (1230)

M. Dan Rogers: Désolé, simplement pour préciser, pourriez-vous nous en dire davantage sur les actions indirectes?

Mme Irene Mathyssen: Les acteurs mal intentionnés sont-ils capables d'accéder aux systèmes de cryptage intégré?

M. Dan Rogers: Je peux dire — André, n'hésitez pas à intervenir si vous voulez — que, quand nous observons ce qui se passe dans les services de renseignements étrangers, nous trouvons des États-nations et d'autres acteurs qui profitent des failles dans les logiciels pour déjouer certains mécanismes, comme le cryptage, et pour avoir accès à des communications qui seraient protégées autrement.

Quand nous observons cela dans les services étrangers, nous fournissons des informations de ce type à nos collègues du cybercentre et des autres organismes au Canada. Ils prennent des mesures qui pourraient consister à offrir des conseils en matière d'atténuation ou à informer les fournisseurs pour s'assurer que les actions indirectes fassent l'objet d'un suivi.

Mme Irene Mathyssen: Dans la description de l'ingérence russe dans le système d'élection américain et aux Pays-Bas, on précise que c'était le travail de personnes peu qualifiées. Ce n'était pas le travail de personnes instruites.

Que se passera-t-il quand un groupe de personnes plus instruites arrivera? Vous avez parlé des pratiques exemplaires et de ce que vous avez appelé un guide d'hygiène informatique. Je me demandais si vous pouviez nous expliquer qui utilise ce guide, et en quoi il est efficace. Peut-on s'y fier, sachant que des êtres humains sont concernés? Devrions-nous être rassurés de savoir qu'il existe un guide d'hygiène informatique?

M. André Boucher: Absolument. Une partie du défi du Centre canadien pour la cybersécurité, c'est d'élaborer un ensemble de conseils et de directives pour toutes les personnes qui exercent des activités dans l'environnement cybernétique. Un des éléments clés de l'environnement cybernétique, pour vous et moi et pour les autres utilisateurs, c'est le guide d'hygiène informatique, les conseils sur l'utilisation des appareils mobiles. Il y a un ensemble de connaissances que vous pouvez trouver sur notre site Web. Elles sont également partagées au moyen de campagnes sur la cybersécurité et d'autres campagnes, qui ciblent spécifiquement les mesures simples que tout le monde peut prendre et qui donnent beaucoup d'avantages pour un petit nombre de gestes.

Quand nous rédigeons les conseils et les directives, nous le faisons dans le but d'avoir le plus d'avantages possible en matière de sécurité avec quelques gestes simples.

Mme Irene Mathyssen: Merci.

Le vice-président (M. Nathaniel Erskine-Smith): J'ai quelques questions.

Je veux commencer par vous, monsieur Rogers, et c'est une question très simple.

Les partis politiques se raidissent quand nous parlons de les soumettre potentiellement à un cadre réglementaire relatif aux pratiques en matière de protection des renseignements personnels ou des données. Je suis ravi que vous ayez donné des conseils à tous les partis politiques du Canada.

Ma question ne concerne pas tant la protection des renseignements personnels que l'adoption des pratiques exemplaires de gestion de données. J'ai participé à une table ronde avec un groupe de représentants parlementaires à Washington. Bob Zimmer était également présent. Un certain nombre de représentants affirment que deux facteurs d'authentification sont nécessaires de nos jours, et, si ce n'est pas une règle définie pour les partis politiques, c'est un énorme problème.

J'ai lu votre rapport de juin 2017; et vous dites que vous n'êtes pas inquiet à propos d'Élections Canada, mais plutôt de la vulnérabilité des partis politiques. Quand j'ai lu que le Parti démocrate et le Parti républicain ont tous les deux été piratés et qu'il y a eu une distribution sélective des documents obtenus par piratage, je me dis que les partis politiques doivent redoubler d'efforts en matière de pratiques de gestion de données.

Ne devraient-ils pas être réglementés?

M. Dan Rogers: Je pense que ce n'est pas à nous de dire ce que le gouvernement canadien doit réglementer. André pourrait parler des types de mesures que, à notre avis, tout le monde, les partis politiques et les autres, devraient adopter s'ils veulent avoir de bonnes pratiques d'hygiène informatique.

Le vice-président (M. Nathaniel Erskine-Smith): En d'autres termes, si votre conseil devenait une règle, pensez-vous que ce serait mieux pour la protection de nos informations ou pour la sécurité de nos élections?

M. André Boucher: Si je puis intervenir, étant donné mes années d'expérience, j'aimerais vous donner mon avis sur les règles.

Nous travaillons en collaboration, comme je l'ai mentionné, avec tous les participants. Les gens veulent assurer leur sécurité. Toutes les entités et les partis politiques ont réellement envie de le faire.

Quand je travaille sur un modèle de collaboration et de pratiques exemplaires, j'atteins un certain seuil de réalisations et de résultats. À la minute où j'établis une norme— et il existe un grand nombre de normes dans la fabrication des pièces d'équipement, de tables, de chaises et ainsi de suite —, il y a un nivellement par le bas. Les gens essaient de respecter la norme minimale, car la concurrence entre en jeu. Les pratiques exemplaires sont établies grâce à la collaboration.

Le vice-président (M. Nathaniel Erskine-Smith): Merci beaucoup.

Monsieur Durocher, dans votre rapport, le livre blanc, il est indiqué que l'objectif de la loi et de l'examen... En matière de mégadonnées, le but en réalité est d'assurer une économie novatrice, efficace et prospère. Il y a des discussions sur la substituabilité. Il ne s'agit pas simplement du prix; vous pourriez parler de la qualité.

Nous avons reçu ici certaines personnes qui ont parlé de leurs inquiétudes concernant les antitrusts. C'était lié à notre sujet, et le prix n'avait rien à voir. Les gens se retrouvent dans une position — Mme Vandenbeld a soulevé ce point — où ils sont obligés à traiter avec des sociétés en situation de monopole.

La Banque du Canada laisse entendre que les cinq grandes entreprises technologiques mondiales ont une capitalisation boursière d'une valeur de 3,5 billions de dollars américains. Nous devons traiter dans notre vie de tous les jours avec certaines de ces entreprises. Nous n'avons pas le choix. Nous devons donner quelque chose pour accéder au service. Le prix n'est pas nécessairement pris en considération, mais la qualité l'est. La qualité du service tient en partie aux données et aux renseignements personnels que je fournis potentiellement.

Vous n'en avez pas beaucoup parlé quand vous examiniez l'aspect des mégadonnées, dans le document. Pourriez-vous nous en parler davantage?

● (1235)

M. Anthony Durocher: Certainement. C'est une très bonne question, et ce sont d'excellentes observations; je peux vous dire que, lorsque M. Maurice Stucke a témoigné devant le Comité, nous avons examiné la transcription avec beaucoup d'intérêt parce que nous suivons ce qu'ont à dire des chefs de file comme lui sur la question.

Je conviens tout à fait que, dans l'économie numérique, nous sommes passés d'une concurrence statique à une concurrence dynamique. La concurrence statique, c'est la concurrence de l'ancien monde sur les prix et les extrants, laquelle occupe encore une place importante dans nombre d'industries partout au Canada. Dans le domaine numérique, ce que nous voyons, c'est que les entreprises se livrent une grande concurrence pour les utilisateurs en fonction de la façon dont elles innovent au chapitre de l'offre de leurs produits aux consommateurs. Nous appelons cela les effets non liés aux prix. Lorsque je parle de la modernisation des outils que nous utilisons dans le cadre de la Loi sur la concurrence, c'est exactement dans le but de régler ces problèmes d'effets non liés aux prix.

Le vice-président (M. Nathaniel Erskine-Smith): Excellent.

Une autre chose dont vous avez parlé dans votre livre blanc, c'était l'obstacle au changement de services. Il n'est pas facile pour moi d'imprimer tout de mon profil Facebook et de le transférer dans un autre réseau social. Il me semble qu'un autre obstacle est les effets de réseau, mais comme votre livre blanc l'indique, il y a de grands avantages positifs qui découlent de ces effets.

Je ne sais pas quel est l'avantage positif d'un obstacle au changement de services. Je sais que, lorsqu'on prend le Règlement général sur la protection des données et qu'on voit qu'il comporte une règle sur le droit à la portabilité, et d'autres ont parlé non seulement de ce droit, mais également du droit à l'interopérabilité, cela n'augmenterait-il pas la concurrence?

M. Anthony Durocher: Oui. C'est également une excellente question.

La portabilité des données visée par le Règlement général sur la protection des données est l'aspect le plus notable, à mon avis, du point de vue de la concurrence. En théorie, elle peut favoriser la concurrence. Elle peut permettre aux consommateurs de transférer leurs données d'une plateforme à une autre. Évidemment, les difficultés surgissent des menus détails pour ce qui est de la façon dont cela est rendu opérationnel, mais c'est certainement quelque chose que nous prenons en note.

Nous le constatons dans le secteur bancaire canadien. Par exemple, le principe sous-jacent de l'initiative visant les services bancaires ouverts est de permettre aux gens de transférer leurs données d'un fournisseur de services à un autre. Au chapitre de la concurrence, c'est certainement très intéressant. C'est quelque chose que nous surveillons de très près.

En même temps, nous devons surveiller la façon dont cela est rendu opérationnel. Sur le plan de la concurrence, lorsque nous regardons les règlements sur la protection de la vie privée, une autre considération liée à la concurrence concerne le coût de la conformité. Il ne doit pas être élevé au point d'isoler les grands joueurs et de faire en sorte qu'il est plus difficile pour les plus petits joueurs d'affronter la concurrence.

Le vice-président (M. Nathaniel Erskine-Smith): Ne pensez-vous pas que, lorsque vous examinez les autres facteurs au-delà du prix et de la protection de la vie privée, qui sont des aspects dont s'inquiète évidemment le Comité, la notion de protection de la vie privée par défaut uniformiserait les règles du jeu? N'éliminerait-elle pas le pouvoir de négociation inégal entre les monopoles, pour ainsi dire, et chaque consommateur? Une personne n'aurait pas à abandonner immédiatement tous ses droits à la vie privée dès le départ. Nous pourrions nous pencher sur d'autres facteurs liés à la substituabilité au-delà du prix.

Croyez-vous qu'il serait utile pour nous de mener cette discussion?

M. Anthony Durocher: Certainement. Nous croyons que les forces du marché devraient favoriser les améliorations à tous les égards, y compris la protection de la vie privée.

Le vice-président (M. Nathaniel Erskine-Smith): C'est juste.

Monsieur Santor, j'ai une dernière question.

Mme Wilkins, sous-gouverneure, a fait remarquer en février passé que les données étaient devenues une autre source de pouvoir monopolistique. Elle avait deux préoccupations. Premièrement, cela pourrait avoir une incidence négative sur l'innovation; et, deuxièmement, certaines entreprises pourraient se remettre à fixer les prix de manière monopolistique à long terme.

Il y a peut-être d'autres inquiétudes. D'autres témoins nous ont fait part d'autres préoccupations potentielles à l'égard des politiques antitrust.

Mme Wilkins a rejeté certaines solutions possibles dont parlent d'autres personnes concernant la façon dont nous réglementons la propriété et la communication d'informations et le fait que nous traitons peut-être les plateformes technologiques comme des services.

Lorsque les représentants du CRTC ont témoigné à propos de la neutralité du Net, ils ont parlé d'un article qui indique que les entreprises n'ont pas le droit d'établir une discrimination injuste, ou —y compris envers elles-mêmes — une préférence indue ou déraisonnable, ou encore de faire subir un désavantage de même nature. Voilà ce qui en est pour le traitement équitable.

Devrions-nous réglementer Facebook, Google, Apple, Amazon et Microsoft? Ne devrions-nous pas les traiter comme Rogers et Bell?

● (1240)

M. Eric Santor: C'est une question qui va au-delà du mandat de...

Le vice-président (M. Nathaniel Erskine-Smith): Pourtant, Mme Wilkins a proposé de les traiter comme des services.

M. Eric Santor: Pour répondre à cette question, il faudrait demander à des personnes qui possèdent l'expertise pour décider si la concurrence... Pour comprendre pleinement les avantages de la numérisation, nous devons nous assurer que la concurrence est efficace.

Nous devons nous poser ces questions, mais il s'agit d'une question ouverte, à savoir quelle est la meilleure façon d'y arriver. Je m'en remettrais à mes collègues à cet égard.

Le vice-président (M. Nathaniel Erskine-Smith): Merci beaucoup.

La seule chose que je dirais, c'est que je suis très heureux que Mme Wilkins ait parlé de ses préoccupations et défini le problème. Si elle a des solutions à proposer, elle est invitée à le faire.

Est-ce que quelqu'un d'autre a des questions?

M. Picard a une question, et ce sera ensuite M. Baylis suivi de Mme Mathyssen.

[*Français*]

M. Michel Picard: Madame Gendron-O'Donnell, en réponse à une question, vous avez été claire au sujet de votre capacité d'agir quant à la transparence de ce qui est prévu dans les contrats.

Pour améliorer vos enquêtes, y a-t-il des modifications ou des choses que vous aimeriez recommander au Comité? On parle d'utilisation abusive ou d'indication trompeuse. L'omission en fait-elle partie? Y a-t-il des aspects de votre réglementation qui devraient être modifiés pour améliorer votre capacité d'enquête?

Mme Alexa Gendron-O'Donnell: Je vous remercie de votre question.

Comme mon collègue vous l'a indiqué, les questions de politique ou qui concernent la Loi sur la concurrence ne relèvent pas du mandat du Bureau de la concurrence. Nous sommes satisfaits des dispositions actuelles de la Loi sur la concurrence, et c'est le ministère qui s'occupe de ces aspects. De notre côté, nous faisons le maximum avec les ressources dont nous disposons. Nous concentrons nos efforts sur les domaines où nous pouvons avoir le plus d'incidence possible, et nous ciblons les enquêtes qui auront le plus d'effets positifs pour les Canadiens.

M. Michel Picard: Ma prochaine question s'adresse aux représentants du CST.

Dans votre compréhension de la menace, faites-vous la distinction entre la quantité industrielle d'informations qu'on jette sur les réseaux sociaux et qui confond les gens, et l'attaque directe ou le piratage? La plupart des lecteurs ne savent plus quoi penser, comment penser et quoi regarder. En fait, il s'agit simplement de propagande à outrance.

Y a-t-il un autre élément qui serait assimilable à du piratage, mais qui relève de votre responsabilité et qui constitue une menace? Il faut connaître la différence entre les choses. Le gouvernement doit pouvoir agir sur la bonne chose. Il ne peut pas agir sur le droit de quelqu'un de dire ce qu'il veut, même si ce sont des niaiseries. Si, par contre, on publie des choses à un endroit où on ne peut pas le faire, le gouvernement a le droit d'agir.

À votre niveau, faites-vous la différence entre les deux?

[*Traduction*]

M. Dan Rogers: Je peux répondre en ce qui concerne l'aspect du renseignement étranger. Peu importe la méthode, que ce soit par piratage ou par envoi de désinformation, peu importe la technique utilisée par un gouvernement étranger, par exemple, ou une organisation qui chercherait à causer du tort au Canada, nous nous intéressons à cela aussi longtemps qu'il s'agit d'une priorité du gouvernement en matière de renseignement. Du point de vue du renseignement étranger, ces deux aspects peuvent être distincts, mais nous nous intéressons aux deux.

Du point de vue de l'intervention, André, voulez-vous faire un commentaire là-dessus?

[*Français*]

M. André Boucher: Oui.

Monsieur Picard, comme vous l'avez mentionné, nous examinons la menace et la méthode utilisée normalement. Nous nous concentrons sur la confidentialité, l'intégrité et la disponibilité des systèmes et des réseaux. L'information véhiculée sur ces réseaux ne relève pas de la responsabilité du CST. Nous nous assurons que, quelle qu'elle soit, l'information est sauvegardée, protégée ou transmise de façon sécuritaire.

M. Michel Picard: D'accord, je vous remercie.

[*Traduction*]

Le vice-président (M. Nathaniel Erskine-Smith): Merci beaucoup.

Monsieur Baylis, vous avez quelques minutes. Nous voulons terminer la séance d'ici 12 h 50 afin que nous puissions passer à huis clos et discuter de certaines affaires du Comité.

M. Frank Baylis: Monsieur Rogers, dans votre exposé, vous avez parlé des cybermenaces qui visent le processus démocratique canadien. Nous venons de recevoir les représentants d'Aggregate IQ, une entreprise située au Canada qui s'est ingérée activement dans le vote sur le Brexit du Royaume-Uni et également, nous croyons, dans les élections présidentielles américaines que le président Trump a gagnées.

L'entreprise utilisait des données volées. Il s'agissait des données volées à Facebook. Cette entreprise est-elle visée par votre enquête? Ou vous concentrez-vous seulement sur l'extérieur? Si l'entreprise mène ses activités ici au Canada et qu'elle s'immisce dans les affaires d'autres personnes, il serait stupide de notre part de croire que, demain, elle ne va pas se retourner contre nous. Y a-t-il des limites à vos pouvoirs d'enquête? Le fait qu'une entité canadienne s'ingère activement dans des processus électoraux et se moque de notre comité comme elle le fait me dérange beaucoup.

● (1245)

M. Dan Rogers: Notre mandat légal se limite aux menaces étrangères à l'extérieur du Canada. Une entreprise canadienne qui s'adonne à tout type de comportement ne serait pas visée par notre mandat d'enquête visant le renseignement étranger, mais il y a peut-être d'autres entités au Canada qui ont ce mandat. Je ne peux pas m'avancer à cet égard, mais le SCRS, la GRC et d'autres se concentrent davantage que nous sur ce qui se passe au pays.

M. Frank Baylis: Si je vous comprends bien, vous êtes le chef du renseignement électromagnétique étranger. Est-ce le mot-repère pour cybersécurité?

M. Dan Rogers: C'est notre appareil de collecte de renseignements étrangers au sein du CST. André est sous-ministre adjoint des Opérations du côté de la cybersécurité. C'est le Centre qui réagira aux cybermenaces et donnera des avis à cet égard. Nous faisons une collecte de renseignements qui peut guider les activités du Centre et d'autres activités au gouvernement.

M. Frank Baylis: Interagissez-vous avec d'autres entités étrangères qui craignent de faire l'objet de piratage elles-mêmes? Est-ce que les Américains ou les Anglais ont communiqué avec vous pour assurer une coordination précisément en ce qui concerne les activités d'AIQ?

M. André Boucher: Le Centre canadien pour la cybersécurité est en fait un de ces nombreux centres nationaux. Nous travaillons en étroite collaboration avec des centres similaires et le Groupe des cinq, mais également avec des centres de partout dans le monde. Une partie du Centre constitue également l'équipe nationale d'intervention en cas d'urgence informatique, l'élément national qui comporte des équipes d'intervention d'urgence et qui s'inscrit dans un réseau mondial. Il y a des paliers de praticiens de cybersécurité qui travaillent ensemble et qui communiquent — lorsqu'ils le peuvent — de l'information qui est pertinente à leurs mandats.

M. Frank Baylis: Qui au Canada devrait s'occuper d'AIQ et de ses activités?

M. André Boucher: Selon ce que vous avez dit, pour ce qui est de l'information volée, cela relèverait du mandat de la GRC.

M. Frank Baylis: Ce qu'ont affirmé les représentants d'AIQ, c'est qu'ils ont construit le logiciel et qu'ils n'ont jamais touché aux données. C'est un véritable argument. Ils ont dit qu'ils n'ont jamais eu accès aux données. Ils n'ont jamais été en contact avec les données, selon leurs dires, ou ils avaient de petits ensembles de données. Ils ont été très prudents sur cette question, mais ils ont clairement construit les programmes ou le logiciel. Ils ont utilisé les données pour s'immiscer de manière active dans un processus démocratique. Ils ont également enfreint d'autres règles du Royaume-Uni. Nous savons cela.

La GRC possède-t-elle les outils de cybersécurité pour examiner la question des données volées? Qu'en est-il de l'ingérence dans un processus démocratique? Voilà deux choses distinctes. D'un côté, ils ont volé quelque chose, et de l'autre, c'est ce qu'ils font avec.

Le vice-président (M. Nathaniel Erskine-Smith): Veuillez répondre brièvement, et nous allons également laisser deux ou trois minutes à Mme Mathyssen.

M. André Boucher: Très brièvement, lorsque le centre de cybersécurité reçoit un appel d'une victime à propos d'un vol d'identité ou de renseignements, nous renvoyons l'appel à la GRC, et celle-ci a le pouvoir et le mandat d'intervenir.

Le vice-président (M. Nathaniel Erskine-Smith): Merci beaucoup.

Madame Mathyssen, vous avez deux ou trois minutes.

Mme Irene Mathyssen: Merci beaucoup, monsieur le président.

Encore une fois, merci à tous de toutes ces informations.

J'avais une question concernant les géants technologiques. La plupart d'entre eux sont américains, et ils exercent beaucoup d'influence au-delà de la frontière américaine. Nous savons cela. Le pouvoir monopolistique de ces géants technologiques devrait-il être visé par des accords commerciaux internationaux auxquels prennent part les États-Unis ou tout pays du siège social, et si oui, comment procéderiez-vous?

M. Anthony Durocher: Je suis heureux de répondre à cette question.

En droit de la concurrence, nous finissons par à traiter en permanence avec des entreprises transfrontalières. Nous examinons les fusions sous forme de conglomérat. Certainement, dans le secteur technologique, beaucoup de décisions sont prises à l'extérieur des frontières canadiennes et une très grande partie de l'information pertinente se trouve hors du Canada. Il est essentiel pour nous d'y avoir accès à cette information et d'avoir compétence en la matière.

Quant aux accords commerciaux, je crois qu'ils dépassent la portée de notre mandat. Je ne suis pas bien placé pour me prononcer là-dessus. Ce que je peux vous dire, c'est que nous entretenons d'excellentes relations avec nos homologues étrangers qui appliquent leurs lois antitrust respectives et communiquons en permanence les uns avec les autres.

Mme Irene Mathyssen: Vous ne serez peut-être pas en mesure de répondre à cette question, mais je me demande s'il faudrait intégrer quoi que ce soit à ces accords commerciaux. La réalité, c'est que les parlementaires, et, par extension, les citoyens qu'ils servent, n'ont pas accès aux textes des accords commerciaux avant que le gouvernement les ratifie. Devrait-il y avoir plus de transparence? Devons-nous en savoir plus?

● (1250)

M. Anthony Durocher: Le Bureau de la concurrence possède un groupe international qui participe aux accords commerciaux, et nombre de ces accords comportent des chapitres sur la concurrence. Le nouvel Accord États-Unis–Mexique–Canada a un chapitre sur la concurrence qui vise principalement à garantir une bonne communication d'information entre les organismes afin de leur permettre de travailler en collaboration et de faire leur travail parce que, comme je l'ai dit, la plupart des politiques antitrust comprennent une portée internationale. Il y a des cartels internationaux et des fusions sous forme de conglomérat qui font l'objet d'avis dans des dizaines de pays, et des attitudes commerciales qui peuvent avoir également une portée internationale.

Notre rôle est de vraiment nous assurer de maintenir ces relations et de communiquer les uns avec les autres étant donné la portée internationale des activités.

Le vice-président (M. Nathaniel Erskine-Smith): Malheureusement, nous n'avons plus de temps, mais je remercie tous nos témoins dans la salle. Si vous avez d'autres idées que vous voulez communiquer au Comité sur ce sujet, veuillez les soumettre par écrit.

Sur ce, nous allons suspendre la séance deux ou trois minutes, le temps que les gens quittent la salle, et nous allons revenir à huis clos pour nous pencher sur certaines affaires du Comité.

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