CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

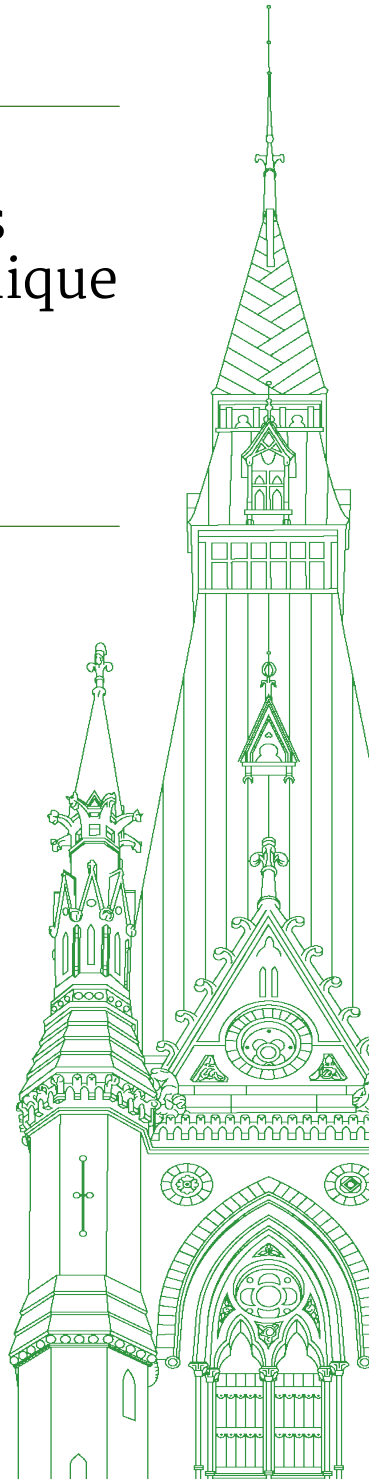
44e LÉGISLATURE, 1re SESSION

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

TÉMOIGNAGES

NUMÉRO 145

Le jeudi 12 décembre 2024



Président : M. John Brassard

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

Le jeudi 12 décembre 2024

● (1600)

[*Traduction*]

Le président (M. John Brassard (Barrie—Innisfil, PCC)): Je déclare la séance ouverte.

[*Français*]

Je vous souhaite la bienvenue à la 145e réunion du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique.

Conformément à l'article 108(3)h) du règlement et à la motion adoptée par le Comité le mardi 29 octobre 2024, le Comité reprend son étude de l'atteinte à la vie privée à l'Agence du revenu du Canada.

J'aimerais souhaiter la bienvenue à nos témoins de la première heure de cette réunion.

[*Traduction*]

Je suis heureux d'accueillir M. Peter Davis, vice-président associé, Relations gouvernementales et avec les intervenants.

Monsieur Davis, bienvenue au Comité. Vous avez jusqu'à cinq minutes pour présenter votre exposé au Comité, après quoi nous passerons aux questions.

Allez-y, monsieur.

M. Peter Davis (vice-président associé, Relations gouvernementales et avec les intervenants, H&R Block Canada Inc.): Merci beaucoup, monsieur le président.

Je remercie les membres du Comité de me donner cette occasion de témoigner aujourd'hui au nom de H&R Block Canada. Merci aussi pour la patience et la souplesse dont vous avez fait preuve envers moi en vous adaptant à mon horaire.

H&R Block Canada est fière de célébrer ses soixante années passées au service des Canadiens que nous aidons à payer leurs impôts et à recevoir leurs prestations. En 1964, le premier bureau fiscal de H&R Block Canada a été établi à Toronto, et notre siège social national trône aujourd'hui fièrement à Calgary. Au cours de ces 60 années au Canada, notre entreprise en est venue à compter près de 1 000 points de service et 10 000 associés qui servent les Canadiens de partout au pays pendant la période des impôts.

Je me propose de revenir sur certains aspects clés de notre déclaration du 15 novembre et du mémoire que nous avons remis au Comité le 6 décembre.

Durant ces plus de soixante années d'activité, H&R Block Canada a toujours accordé la priorité absolue à la protection et à la confidentialité des renseignements fiscaux de ses clients. H&R Block Canada est fière du cadre de protection des renseignements personnels de ses points de service, qui comptent parmi les meilleurs au Canada. Nous comprenons les responsabilités et les obligations importantes qui découlent de la protection des renseignements personnels des Canadiens, et nous avons mis en place des systèmes et des processus de sécurité solides pour les protéger.

Compte tenu de l'engagement pris par H&R Block Canada à l'égard de la confidentialité et de la sécurité des données, quand nous avons appris que nos clés d'accès électroniques avaient été compromises, nous avons immédiatement lancé une enquête interne exhaustive qui nous a permis de conclure que les données, les systèmes et les logiciels de H&R Block Canada n'avaient pas, quant à eux, été compromis. Nous n'avons eu vent d'aucune répercussion sur notre clientèle.

Je tiens également à assurer le Comité que H&R Block Canada n'a jamais envoyé de données personnelles de Canadiens ni d'images à des entreprises comme Google et Meta. Nous sommes au courant d'articles autrefois parus dans la presse américaine à propos de ce problème, mais nous sommes en mesure de confirmer que la description qu'en ont fait les médias ne s'applique pas aux clients de H&R Block Canada.

Permettez-moi de prendre un moment pour parler au nom de tout notre secteur.

En ma qualité de coprésident de l'Association canadienne des déclarants de revenus — l'association commerciale nationale de l'industrie canadienne des logiciels et de la préparation des déclarations de revenus — j'estime important d'expliquer le rôle essentiel de l'industrie des logiciels fiscaux en matière de protection des renseignements personnels des Canadiens. Les logiciels fiscaux mis au point par l'industrie, et qui sont destinés à être directement utilisés par les contribuables ou par des professionnels de la fiscalité au nom de leurs clients, sont annuellement soumis à un processus de certification très poussé appliqué par l'ARC afin que leur utilisation soit approuvée par le public et que la production électronique des déclarations de revenus à l'ARC soit autorisée. Les fournisseurs de logiciels fiscaux doivent également s'assurer que leurs produits et services sont conformes aux lois canadiennes sur la protection des renseignements personnels et la sécurité des données. Ces facteurs, conjugués à l'innovation au sein de l'industrie et aux investissements continus visant à améliorer et à faire évoluer continuellement la sécurité des données, donnent la possibilité aux Canadiens de se prévaloir de nombreuses options technologiques destinées à garantir l'acheminement de leurs renseignements personnels en toute sécurité.

La diversification des systèmes est une parade contre les risques liés à la cybersécurité, car les auteurs de menaces doivent tenter d'infiltrer plusieurs systèmes de TI sécurisés à la fois, plutôt qu'un seul système administré par l'ARC. Dans cette optique, outre que l'ARC est une cible de grande valeur pour les auteurs de menaces et qu'elle a déjà subi des failles de sécurité, la notion selon laquelle les renseignements des contribuables seront plus sûrs s'ils sont contrôlés et gérés uniquement par l'ARC au moyen d'une déclaration automatique ou de tout autre type de déclaration de revenus du gouvernement n'a pas de fondement crédible.

Avant de passer aux questions des membres du Comité, j'aimerais traiter d'un point. Ces procédures sont très probablement surveillées par des auteurs de menaces qui cherchent des occasions d'identifier et d'exploiter les renseignements potentiels sur la sécurité des données à des fins criminelles. En tant que plus grande entreprise de préparation de déclarations de revenus assistée au Canada, H&R Block Canada surveille de près ce qui se fait et se défend régulièrement contre les cybermenaces. Par conséquent, dans toutes nos déclarations au sujet de la cybersécurité, nous devons veiller à ne pas dévoiler d'informations sensibles qui pourraient aider les auteurs de menaces des renseignements à mener leurs activités criminelles. De plus, nous sommes tenus de respecter la législation canadienne sur la protection des renseignements personnels et les politiques de H&R Block Canada en matière de protection des renseignements personnels et de sécurité des données de nos clients, et de veiller à ce qu'aucun renseignement personnel de contribuables canadiens ne soit divulgué.

Merci encore, monsieur le président et distingués membres du Comité, de m'avoir invité à comparaître aujourd'hui au nom de H&R Block Canada. Je me ferai un plaisir de répondre à vos questions du mieux possible.

Le président: Merci, monsieur Davis.

Nous allons commencer par des tours de questions de six minutes.

M. Caputo va ouvrir le bal.

Allez-y, monsieur Caputo.

M. Frank Caputo (Kamloops—Thompson—Cariboo, PCC): Merci pour votre témoignage, monsieur Davis, et merci de votre déclaration liminaire.

J'en ai retenu que nous avons manifestement affaire à une atteinte massive à la vie privée. C'est ce qui nous amène au Parlement aujourd'hui.

Donc, d'après vous, cela ne semble pas concerner H&R Block, mais uniquement l'ARC?

M. Peter Davis: Je vous remercie de votre question.

Comme je l'ai dit dans ma déclaration et dans des mémoires précédemment remis au Comité, quand H&R Block Canada a été avisée par l'ARC que l'intégrité de nos clés d'accès électroniques avait été compromise, nous avons immédiatement déclenché une enquête exhaustive. Nous n'avons ménagé aucun effort. Tout au long de cette enquête et jusqu'à sa conclusion, rien ne nous a indiqué que les systèmes, logiciels ou appareils de sécurité de H&R Block Canada aient été compromis de quelque façon que ce soit.

Quant à savoir où ces failles de sécurité ont pu se produire, H&R Block Canada ne peut pas le dire avec certitude, mais nous savons que ce n'était pas au sein de notre organisation.

● (1605)

M. Frank Caputo: Merci.

Êtes-vous au courant de la façon dont les choses se passent aux États-Unis? Au Canada, si j'ai bien compris, il n'y a pas d'échanges de renseignements entre H&R Block et l'ARC à propos des questions cybernétiques, mais les États-Unis le font un peu différemment.

Êtes-vous au courant?

M. Peter Davis: Je ne suis au courant que de façon superficielle. Je suis ici à titre de représentant de H&R Block Canada qui parle de nos activités au Canada, mais je sais un peu ce qui se fait en matière de collaboration entre l'IRS et l'industrie de la préparation des déclarations de revenus aux États-Unis, comme le sommet sur la sécurité qui est un rassemblement annuel de l'industrie et de l'IRS pour échanger sur les pratiques exemplaires en matière de cybersécurité et discuter des menaces potentielles, dans la mesure où cela est possible et approprié.

M. Frank Caputo: Vous avez parlé de collaboration. Estimez-vous le genre de collaboration dont vous venez de parler existe au Canada?

M. Peter Davis: Cela ne se fait actuellement pas au Canada. C'est quelque chose que notre entreprise et l'industrie ont recommandé à l'ARC par le passé, et nous continuons de le faire. Dans la mesure du possible, nous aimerions qu'il y ait plus de collaboration entre l'agence et l'industrie pour lutter contre la fraude et tout autre type de menaces à la cybersécurité.

M. Frank Caputo: Depuis combien de temps recommandez-vous une plus grande collaboration avec l'ARC pour contrer ces cybermenaces croissantes?

M. Peter Davis: La question a été soulevée à maintes reprises dans les conversations de l'industrie avec l'ARC au cours des deux ou trois dernières années, je dirais.

M. Frank Caputo: Quelle a été la réponse de l'ARC?

M. Peter Davis: L'ARC a toujours été réceptive à l'idée. Je pense qu'un des défis dont l'ARC nous a fait part à propos de ce concept tient à la façon dont une telle mesure peut être mise en place dans le respect de la législation canadienne sur la protection des renseignements personnels.

Nous croyons savoir que l'ARC se penche sur la question et, une fois que nous aurons une idée plus claire de ce qui pourrait être possible, nous pourrons envisager d'avancer sur ce plan.

M. Frank Caputo: Est-ce que vous y voyez un obstacle à titre de patron de H&R Block?

M. Peter Davis: Est-ce que j'y vois un obstacle?

M. Frank Caputo: C'est ce que vous venez de décrire, non? Estimez-vous que la protection de la vie privée fait obstacle à une plus grande collaboration? Si le problème vient de l'ARC, êtes-vous d'accord avec l'Agence à cet égard?

M. Peter Davis: Dans la mesure où cela empêche l'ARC de collaborer avec l'industrie et avec notre organisation, alors oui, on peut parler d'obstacle.

M. Frank Caputo: D'accord. Quand on parle d'atteinte à la protection des données, de partage d'informations et des cybermenaces qui nous amènent ici aujourd'hui, avez-vous l'impression que l'ARC aurait dû agir plus rapidement sur certaines questions?

M. Peter Davis: Je ne suis pas en mesure de répondre à cette question, étant donné que nous n'étions pas au courant des enquêtes menées par l'ARC et de la plupart des mesures d'atténuation qu'elle entendait prendre. Je ne suis pas en mesure de vous répondre avec exactitude.

M. Frank Caputo: Estimez-vous que la communication avec H&R Block s'est faite en temps opportun?

M. Peter Davis: Oui, quand elle nous a avisés du moment où l'incident a peut-être commencé. Je dirais que cette communication s'est faite rapidement.

M. Frank Caputo: Bien.

Monsieur le président, combien de temps me reste-t-il?

Le président: Une minute et demie.

M. Frank Caputo: J'aimerais en parler un peu plus.

Savez-vous quand les atteintes ont été révélées? Quand H&R Block en a-t-il été avisé?

M. Peter Davis: Je ne suis pas en mesure de vous donner la date exacte, ne serait-ce que pour des raisons de sécurité, mais nous avons été avisés en avril dernier. Dès que nous avons eu la nouvelle, nous avons lancé notre enquête sur nos systèmes, logiciels et appareils de sécurité.

M. Frank Caputo: À votre connaissance, est-ce que certains de vos clients ont subi des pertes en raison de cela?

M. Peter Davis: Nous n'avons pas découvert de répercussions sur nos clients.

M. Frank Caputo: Savez-vous exactement combien de clients ont été touchés par cette mesure?

M. Peter Davis: Non, nous ne savons pas combien de Canadiens ont été touchés par cette mesure.

M. Frank Caputo: Vous n'en avez pas une petite idée?

M. Peter Davis: Non, je n'ai rien qui soit fondé sur des faits.

● (1610)

M. Frank Caputo: Avez-vous fait des recommandations de sécurité à l'ARC en fonction de ce qui s'est passé de votre côté?

M. Peter Davis: Oui, nous avons présenté une série de recommandations à l'ARC en août dernier. Nous croyons savoir que l'ARC continue de les examiner, et nous avons hâte de communiquer avec elle dès que possible.

M. Frank Caputo: L'ARC vous a-t-elle dit si elle les acceptera et comment les choses progressent?

Voici ce qui me préoccupe. Nous sommes en décembre. Cela remonte au mois d'août. Nous ne voulons pas nous retrouver dans la même situation. Je me demande simplement…

Le président: Monsieur Caputo, je suis désolé, mais votre temps est écoulé.

Monsieur Fisher, vous avez six minutes.

M. Darren Fisher (Dartmouth—Cole Harbour, Lib.): Merci beaucoup, monsieur le président.

Monsieur Davis, je suis heureux de vous rencontrer aujourd'hui. Merci de votre présence.

Certaines de mes questions ont peut-être été déjà posées de façon différente, mais toutes vont porter sur le même sujet.

Dans la lettre que H&R Block Canada a fait parvenir à notre comité, on peut lire en substance que les données, les systèmes et les logiciels de H&R Block Canada n'ont pas été compromis.

Je m'intéresse aux codes qui sont attribués à vos bureaux de spécialistes en déclarations de revenus. Parlez-nous un peu de vos stratégies et politiques internes pour assurer la sécurité de ces codes.

M. Peter Davis: Je vais essayer de répondre à cette question dans la mesure du possible, étant donné que je ne suis pas en mesure de vous donner beaucoup de détails à ce sujet en raison de nos politiques en matière de sécurité et de protection des renseignements personnels de nos clients.

Je peux dire que l'ARC attribue des numéros aux fins de la transmission électronique de déclarations aux préparateurs de déclarations de revenus et qu'on s'attend à ce que ces numéros soient traités dans la plus stricte confidentialité.

M. Darren Fisher: Avez-vous eu des problèmes avec ces codes?

M. Peter Davis: Non.

M. Darren Fisher: Il n'y a jamais eu de fuite de ces codes.

M. Peter Davis: Non.

M. Darren Fisher: Comment pouvez-vous garantir que votre personnel ne sera peut-être pas à l'origine de fuites dont nous parlons aujourd'hui?

M. Peter Davis: Cela faisait partie de l'enquête que nous avons menée et, comme je l'ai dit, nous n'avons ménagé aucun effort. Nous avons effectué un examen exhaustif de presque tout ce qui est lié aux justificatifs d'identité pour la TED et à la façon dont ils sont utilisés au sein de notre organisation. Rien ne laisse croire à une quelconque implication ou responsabilité de notre personnel dans ce qui s'est passé.

M. Darren Fisher: Lorsque vous recrutez de nouveaux employés, faites-vous des vérifications du casier judiciaire et ce genre de choses?

M. Peter Davis: Oui, nous vérifions les antécédents criminels de tous nos associés.

M. Darren Fisher: Est-ce que vous le faites pour tous vos nouveaux employés ou seulement pour ceux qui utilisent ces codes?

M. Peter Davis: Nous le faisons pour tous nos nouveaux employés.

M. Darren Fisher: Parlez-moi un peu de votre processus de recrutement, du moment où vous chercher de nouveaux collaborateurs et de votre processus de formation.

M. Peter Davis: Bien sûr.

M. Darren Fisher: Pourriez-vous nous parler un peu de la façon dont vous formeriez ces gens pour qu'ils comprennent l'importance d'être en possession de ces renseignements sur les contribuables?

M. Peter Davis: Avec plaisir.

Chaque année, nous tenons ce que nous appelons l'Académie fiscale de H&R Block Canada. Dès la fin de l'été, nous commençons à recevoir les demandes de Canadiens qui souhaitent suivre notre formation et devenir associés en fiscalité chez nous. Grâce à ce processus, nous leur enseignons tout ce qu'il faut savoir sur le Code des impôts et sur la manière de travailler avec les Canadiens pour préparer et transmettre leurs déclarations de revenus. Nous prenons aussi le temps de parler des mesures de sécurité et de la manière de garantir que les données des contribuables sont traitées avec la plus grande confidentialité à tout moment. Cela comprend également les renseignements nécessaires à la transmission électronique des déclarations à l'ARC. Il y a beaucoup de formation à ce sujet.

Nous offrons également de la formation supplémentaire aux participants à notre Académie fiscale que nous choisissons d'embaucher avant qu'elles ne commencent à préparer et à produire des déclarations de revenus dans nos bureaux.

Il y a beaucoup de formation sur la sécurité et la protection des renseignements personnels. Tous nos employés y participent chaque année.

M. Darren Fisher: Je suppose que ce serait la norme dans l'industrie pour les tierces parties et les organisations du secteur privé.

M. Peter Davis: Je ne peux pas parler au nom de toutes les organisations, mais c'est certainement une norme pour H&R Block Canada.

M. Darren Fisher: Très bien.

Lorsque H&R Block Canada transmet une déclaration de revenus à l'ARC au nom du contribuable canadien par voie électronique, comment vous assurez-vous, de votre côté, que les données sont sécurisées?

M. Peter Davis: Ces renseignements sont transmis au moyen d'un logiciel fiscal, qui est certifié par l'Agence du revenu du Canada. Chaque développeur de logiciels fiscaux, y compris H&R Block Canada, doit se soumettre à un processus de certification rigoureux avec l'ARC chaque année pour s'assurer que nos logiciels fiscaux répondent à un certain nombre d'exigences de l'ARC.

De plus, nous devons nous assurer que les logiciels fiscaux sont conformes à toutes les lois sur la protection des renseignements personnels et la sécurité des données. Un processus très détaillé permet de garantir que les logiciels fiscaux sont sûrs et sécuritaires pour les Canadiens.

● (1615)

M. Darren Fisher: Y a-t-il eu des atteintes de quelque nature que ce soit aux données de vos clients à H&R Block Canada?

M. Peter Davis: Je ne suis pas en mesure de vous donner des détails sur les atteintes à la vie privée en raison de nos politiques en matière de sécurité des données et de protection des renseignements personnels. En revanche, je peux dire que...

M. Matthew Green (Hamilton-Centre, NPD): J'invoque le Règlement, monsieur le président.

Le président: La parole est à vous pour votre rappel au Règlement.

M. Matthew Green: Monsieur le président, peut-être que M. Davis connaît mal les travaux parlementaires ou les pouvoirs des comités d'exiger des témoignages.

Malheureusement, il ne peut pas se retrancher derrière un quelconque pseudosecret professionnel. Il est ici devant le Parlement et il doit répondre aux questions des parlementaires.

J'aimerais que vous l'informiez de ses responsabilités devant le Comité.

Le président: Merci de ce rappel, monsieur Green.

Monsieur Davis, je comprends la nature délicate du système de sécurité et des mécanismes en place à H&R Block. Vous l'avez expliqué très clairement dans votre déclaration préliminaire.

Je vous demanderais de répondre aux questions du mieux que vous le pouvez. Nous sommes protégés par le privilège parlementaire, mais nous ne voulons certainement pas compromettre — et je suis d'accord avec vous sur ce point — tout secret commercial de H&R Block qui pourrait causer des problèmes. C'est l'instruction que je vais vous donner à cet égard.

Monsieur Green, j'espère que vous comprenez que lorsqu'on a demandé à H&R Block de comparaître devant nous, la convocation ne visait pas une personne en particulier. H&R Block a désigné M. Davis pour la représenter et je suis convaincu qu'il répond aux questions du mieux qu'il peut étant donné la nature du sujet qui nous occupe.

Monsieur Fisher, j'ai arrêté le chrono au moment du rappel au Règlement. Il vous reste donc une minute.

M. Darren Fisher: C'est très bien.

Vous l'avez peut-être déjà dit, mais pouvez-vous confirmer que toutes les données des clients de H&R Block Canada sont stockées uniquement sur des serveurs qui sont tous au Canada?

M. Peter Davis: Pour ce qui est du stockage de ces renseignements — tout cela est divulgué à nos clients et nous obtenons leur consentement —, dans certains cas, les données de clients peuvent être envoyées aux États-Unis à notre société mère, H&R Block. Cela pourrait être nécessaire pour fournir au client un produit ou un service précis. Dans certains cas, il peut s'agir de les informer de l'existence de certains produits et services dont ils souhaitent bénéficier. Ces données sont en grande partie stockées à cet endroit et ne sont pas incorporées dans les pixels ni dans tout autre élément susceptible d'être transmis à d'autres parties.

Le président: D'accord.

Merci, monsieur Fisher.

M. Darren Fisher: Je vous en prie.

Le président: M. Villemure est le suivant.

Monsieur Davis, pouvez-vous mettre votre écouteur, s'il vous plaît, et vous assurer qu'il est réglé sur l'interprétation en anglais? Assurez-vous de régler le volume pour pouvoir l'entendre.

[*Français*]

Monsieur Villemure, vous avez la parole pour six minutes.

M. René Villemure (Trois-Rivières, BQ): Je vous remercie beaucoup, monsieur Davis, d'être avec nous aujourd'hui.

Je ne répéterai pas les questions de mes collègues, qui étaient toutes pertinentes. J'aimerais plutôt parler de la protection de la vie privée. Pourriez-vous nous décrire la politique de H&R Block en matière de protection de la vie privée?

[*Traduction*]

M. Peter Davis: Puis-je demander de répéter la question? Le son a coupé un peu vers la fin.

[*Français*]

M. René Villemure: Pourriez-vous nous présenter la politique sur la protection de la vie privée de H&R Block?

[*Traduction*]

M. Peter Davis: Chez H&R Block Canada, nous avons mis en place plusieurs politiques de protection des renseignements personnels des clients. J'aimerais attirer votre attention sur ce que nous appelons notre formulaire d'assurance de la protection des renseignements personnels. C'est ce que nous considérons comme une norme d'excellence dans l'industrie ici au Canada. Nous prenons le temps de rencontrer nos clients dans nos bureaux et nous leur expliquons comment H&R Block Canada utilise leurs données et pourquoi. Nous prenons grand soin de limiter l'utilisation des données pour nous assurer qu'elles servent les besoins du client afin de lui fournir les produits et services auxquels il s'attend. Nous discutons de la façon dont ces données sont utilisées. Nous parlons d'un certain nombre de dispositions connexes et nous demandons le consentement du client pour procéder comme nous l'avons expliqué.

Ce qui distingue notre politique d'assurance de la protection des renseignements personnels, c'est que chaque année, quand nos clients reviennent nous voir au cours de la saison des impôts suivante, nous passons également en revue les changements apportés à ce formulaire. Il est très important pour nous que nos clients comprennent l'importance que nous accordons à la protection de leurs données. Nous voulons qu'ils soient informés et à l'aise avec les processus que nous avons mis en place pour protéger leurs renseignements personnels.

● (1620)

[*Français*]

M. René Villemure: Vous connaissez probablement le Règlement général sur la protection des données, ou RGPD, de l'Union européenne. La norme OR de H&R Block est-elle conforme au RGPD ou simplement à l'actuelle protection canadienne?

[*Traduction*]

M. Peter Davis: Il est certain que c'est ce que la loi canadienne exige. De mémoire, je ne sais pas s'il est également conforme au Règlement général sur la protection des données. Je ferai un suivi par écrit lorsque j'aurai obtenu une confirmation à ce sujet.

[*Français*]

M. René Villemure: C'est parfait. Merci beaucoup.

Vous parliez à l'instant du consentement. Croyez-vous que le client de H&R Block comprend ce à quoi il consent réellement?

[*Traduction*]

M. Peter Davis: Chez H&R Block Canada, nous nous donnons beaucoup de mal pour garantir que nos clients comprennent vraiment comment nous utilisons leurs renseignements afin de leur fournir les produits et services auxquels ils s'attendent. Nos fiscalistes, partout au Canada, sont formés pour vraiment prendre le temps d'expliquer nos mesures de protection des renseignements personnels et nos politiques en matière de données dans un langage simple. Je peux affirmer en toute confiance que nos clients comprennent bien comment leurs données sont utilisées.

[*Français*]

M. René Villemure: Les formulaires de consentement tiennent souvent sur une page et sont rédigés dans un jargon juridique. C'est la raison pour laquelle je vais poser ma prochaine question.

Combien de temps après la déclaration de revenus conservez-vous les données de vos clients?

[*Traduction*]

M. Peter Davis: Nous conserverons leurs renseignements conformément aux exigences de la loi, c'est-à-dire, je crois, l'année d'imposition et six ans de plus, donc sept ans. Je n'ai pas connaissance d'autres mesures de conservation que nous prenons, mais je vais le confirmer et faire un suivi par écrit auprès du Comité.

[*Français*]

M. René Villemure: À la fin de la période de rétention, comment disposez-vous des données relatives aux déclarations de revenus?

[*Traduction*]

M. Peter Davis: Nous suivons un processus très complet pour nous assurer que tous les renseignements personnels, une fois que nous ne sommes plus tenus de les conserver, sont complètement détruits. C'est un processus très complet.

[*Français*]

M. René Villemure: Pouvez-vous nous décrire concrètement votre manière de faire?

[*Traduction*]

M. Peter Davis: Je crains de ne pas pouvoir vous fournir beaucoup plus d'information à ce sujet, compte tenu de notre politique de sécurité des données et de protection des renseignements personnels. Je vais vérifier auprès de notre bureau si nous pourrions vous fournir d'autres détails et je ferai un suivi par écrit à ce sujet.

[*Français*]

M. René Villemure: D'accord.

Merci beaucoup.

Le président: Merci, monsieur Villemure.

[*Traduction*]

Pour que ce soit bien clair, monsieur Davis, la greffière a noté les suivis que vous allez faire par écrit. Elle vous relancera pour s'assurer que l'information nous est transmise. C'est un compromis raisonnable que nous pouvons envisager lorsqu'il s'agit de fournir des renseignements délicats à titre confidentiel au Comité.

C'est le tour de M. Green pour six minutes.

M. Matthew Green: Merci, monsieur le président.

Monsieur Davis, vous avez mentionné dans votre déclaration liminaire que H&R Block n'a jamais transmis de données personnelles de clients, y compris des pixels, à des entreprises comme Google et Meta. Vous avez dit, bien sûr, que cela vaut pour H&R Block Canada.

Pouvez-vous décrire, pour notre gouverne, qui possède effectivement les données exclusives de H&R Block — la filiale canadienne ou la société mère américaine?

● (1625)

M. Peter Davis: Quand vous parlez de « données exclusives », que voulez-vous dire exactement?

M. Matthew Green: Ce sont les renseignements personnels de vos clients, monsieur. Vous avez mentionné qu'une partie est envoyée aux États-Unis. Ne pourrions-nous pas dire, puisqu'il s'agit d'une filiale de H&R Block Incorporated, au Missouri, que tous les renseignements appartiendraient également à la société mère?

M. Peter Davis: Les renseignements que nous fournissent les Canadiens ne nous appartiennent pas. C'est entre H&R Block Canada et nos clients.

Je veux toutefois être prudent dans ma réponse à votre question, parce que je ne connais pas tous les tenants et aboutissants des aspects juridiques de la question de savoir qui serait l'ultime détenteur de ces renseignements. Si on ne...

M. Matthew Green: Monsieur Davis, mon temps est compté. Je vais reprendre mon temps de parole.

Vous avez mentionné que H&R Block Canada n'a jamais transmis de données personnelles de ses clients, y compris des pixels, à des entreprises comme Google et Meta. Pourtant, en juillet 2023, une enquête du Sénat des États-Unis a déterminé que H&R Block avait fort probablement divulgué des renseignements sur les déclarations de clients à Meta en violation des articles 6713 et 7216 en intégrant les pixels de Meta dans les outils mobiles et les sites Web de H&R Block que les consommateurs peuvent utiliser pour préparer leur déclaration de revenus.

Monsieur, êtes-vous au courant du recours collectif actuellement intenté contre H&R Block aux États-Unis?

M. Peter Davis: Nous prenons la sécurité des renseignements personnels de nos clients…

M. Matthew Green: Je vous ai simplement demandé si vous étiez au courant.

M. Peter Davis: Je suis au courant, oui.

M. Matthew Green: D'accord.

Vous savez que la poursuite tombe sous le coup de la loi RICO, la Racketeer Influenced and Corrupt Organizations Act, contre la société de préparation de déclarations d'impôts — votre société mère — et Meta. C'est une pratique qui a été établie par votre société mère. Pourtant, vous affirmez ici, avec assurance, que H&R Block Canada ne lui a jamais transmis de renseignements personnels sur ses clients.

Pouvez-vous garantir aujourd'hui, devant ce comité, qu'il en va de même pour votre société mère aux États-Unis?

M. Peter Davis: Je suis ici en tant que représentant de H&R Block Canada pour parler de nos clients et contribuables canadiens. Je peux affirmer avec certitude que leurs données ne sont pas partagées avec des entreprises telles que Google et Meta.

M. Matthew Green: Vous voulez dire par H&R Block Canada.

M. Peter Davis: C'est exact.

M. Matthew Green: Ce n'était pas ma question.

Ma question est la suivante: pouvez-vous nous donner la même assurance au nom de votre société mère, qui fait actuellement l'objet d'une enquête pour les mêmes pratiques que celles qui vous sont reprochées ici au Canada?

M. Peter Davis: En ce qui concerne les données de nos clients canadiens ni H&R Block Canada ni H&R Block ne divulguent ces données à des entreprises comme Google et Meta.

M. Matthew Green: Cela ne s'est produit qu'aux États-Unis.

M. Peter Davis: Je ne peux pas dire où cela s'est produit. Je suis ici en tant que représentant de H&R Block Canada.

Ce que je peux dire avec certitude, c'est que les données de nos clients canadiens n'ont pas été partagées avec des entreprises comme Google et Meta, que ce soit par l'intermédiaire de H&R Block Canada ou de H&R Block.

M. Matthew Green: Cependant, vous savez qu'une audience du Sénat a eu lieu aux États-Unis pour trancher cette question.

M. Peter Davis: Oui.

M. Matthew Green: Il n'est pas farfelu de penser que vous adoptez les mêmes pratiques, étant donné que vous êtes la filiale d'une société mère accusée de la même chose.

M. Peter Davis: Nous ne partageons pas les données des Canadiens avec des entreprises comme Google ou Meta chez H&R Block Canada ou H&R Block.

M. Matthew Green: J'ai une question relative aux consommateurs. Elle concerne l'action de la FTC qui a mis fin aux pratiques déloyales de déclassement et aux promesses trompeuses de production gratuite des déclarations de revenus de H&R Block.

Proposez-vous le même type de production gratuite au Canada?

M. Peter Davis: Je ne peux pas parler des produits et services de production propres à H&R Block.

Je peux vous parler un peu de ce que nous offrons ici, chez H&R Block Canada.

M. Matthew Green: Monsieur, voici ma question: Savez-vous que la FTC a exigé de votre société mère qu'elle verse 7 millions de dollars aux consommateurs?

M. Peter Davis: Je connais l'action de la FTC.

M. Matthew Green: Je vous demande si le produit qui vient de faire l'objet d'un règlement est également proposé au Canada.

M. Peter Davis: Non, il ne l'est pas.

M. Matthew Green: D'accord, cela suffira pour ma série de questions.

Merci.

● (1630)

Le président: D'accord. Merci, monsieur Green.

Voilà qui met fin au premier tour. Nous passons maintenant au deuxième tour de questions.

M. Chambers va donner le coup d'envoi pour cinq minutes.

M. Adam Chambers (Simcoe-Nord, PCC): Merci, monsieur le président.

Monsieur Davis, merci d'être ici. Je suis navré d'avoir manqué le tour précédent. Quelqu'un m'a joué un drôle de tour pendant les fêtes de fin d'année en envoyant la ministre de l'ARC en même temps au comité des finances, et c'est donc là que je me trouvais pendant les premières minutes.

Revenons-en à la question qui nous occupe. Est-ce que H&R Block Canada a des obligations en vertu du commissaire fédéral à la protection de la vie privée et de la Loi fédérale sur la protection de la vie privée?

M. Peter Davis: Oui, en ce qui concerne la question que le Comité…

M. Adam Chambers: Je veux dire en général.

M. Peter Davis: Oui, nous avons des obligations.

M. Adam Chambers: D'accord.

En vertu de cette loi, s'il y a une atteinte à la protection des données — puisque H&R Block serait régie par les dispositions de cette loi ou assujettie à celles-ci — H&R Block serait tenue de signaler cette atteinte, si elle en a eu connaissance, au commissaire à la protection de la vie privée. Il existe un régime de déclaration.

M. Peter Davis: C'est exact, oui.

M. Adam Chambers: À ma connaissance, H&R Block n'a pas fait de rapport au commissaire à la protection de la vie privée concernant d'éventuelles atteintes, y compris celles qui ont fait la une des journaux récemment. Est-ce juste?

M. Peter Davis: Étant donné que notre enquête, une fois que nous avons été informés par l'ARC de l'incident concernant nos authentifiants de dossiers électroniques… Nous avons commencé notre enquête dès que nous en avons eu connaissance. Nous avons mené une enquête approfondie qui a conclu que nos systèmes, nos logiciels et nos mesures de sécurité n'ont aucunement été compromis chez H&R Block Canada. Par conséquent, nous n'étions pas tenus de signaler quoi que ce soit au commissaire à la protection de la vie privée, et nous n'avions aucune raison de le faire.

M. Adam Chambers: Je présume qu'avec votre société mère, vous n'investissez pas seulement beaucoup de ressources monétaires dans la cybersécurité et les atteintes à la vie privée, mais que vous partagez également des renseignements sur les fraudes ou stratagèmes potentiels qui sont perpétrés contre diverses autorités fiscales, par exemple, au Canada et aux États-Unis. Est-ce juste?

M. Peter Davis: Nous sommes au courant de ce que nous voyons dans les médias que nous suivons. Dans bien des cas, l'ARC n'a pas encore l'habitude de communiquer ce genre d'information à l'industrie. Bien entendu, H&R Block et H&R Block Canada Inc. partagent également des renseignements en matière de cybersécurité.

M. Adam Chambers: En effet, je crois comprendre de votre témoignage que la protection de la vie privée et des renseignements personnels des personnes, soit leurs renseignements fiscaux, mais, plus important encore, leurs renseignements privés et personnels, est un principe fondamental de ce qui vous guide en tant qu'organisation. Vous avez beaucoup d'éléments en jeu pour protéger les renseignements personnels des gens et leur vie privée en général.

M. Peter Davis: Certainement. Nous nous occupons des impôts au Canada pour nos clients depuis plus de 60 ans. La protection des données et la confidentialité des renseignements de nos clients sont absolument primordiales dans notre travail.

M. Adam Chambers: Je ne vous demanderai pas de répondre à cette question, car ce serait potentiellement injuste, mais je dirai ceci. Il est de votre devoir de préserver la confidentialité et la sécurité des renseignements des personnes. Il y a eu un certain nombre d'autres exemples de fraude pure et simple perpétrée à l'ARC, avec un certain nombre de fraudes commises au détriment du contribuable, de schémas frauduleux et de choses qui ne sont pas contrôlées correctement à l'ARC. Le fait que vous n'ayez rien signalé au commissaire à la protection de la vie privée m'indique que ce problème n'émane probablement pas de H&R Block, mais qu'il pourrait provenir d'une source extérieure, qu'il s'agisse d'une tierce partie ou peut-être même de l'ARC. Je ne suis pas tout à fait certain.

Je ne vous demanderai pas de commenter, car je pense que cela pourrait vous mettre dans une position difficile, mais lorsque l'ARC dit que le problème ne vient pas d'eux, et que vous avez une liste d'exemples où ils ont eu des problèmes avec la fraude et la protection des renseignements privés, cela me semble logique. Je pense que votre témoignage est sincère et j'espère que, dans la mesure où vous trouverez d'autres informations, vous les communiquerez.

Pouvez-vous faire un suivi? Vous avez mentionné le fait que l'ARC ne collabore pas beaucoup avec l'industrie, mais cela se fait aux États-Unis. C'est exact?

● (1635)

M. Peter Davis: Je crois savoir qu'il existe des mécanismes de collaboration entre l'IRS et le secteur de la préparation des déclarations d'impôts aux États-Unis, à savoir le sommet sur la sécurité. Nous ne disposons pas d'un mécanisme similaire au Canada, et c'est une chose qu'il serait bon que l'ARC envisage.

M. Adam Chambers: Merci pour ce témoignage, monsieur Davis, et félicitations pour ces 60 années d'activité.

M. Peter Davis: Merci.

Le président: Merci, monsieur Davis.

Merci, monsieur Chambers.

Madame Shanahan, vous avez la parole pour cinq minutes.

Mme Brenda Shanahan (Châteauguay—Lacolle, Lib.): Merci, monsieur le président.

Je voudrais aborder quelques points. Je tiens à faire la distinction entre la raison pour laquelle nous sommes ici maintenant, qui est liée au rapport du *Fifth Estate* selon lequel il s'agit d'une utilisation frauduleuse des identifiants spéciaux de H&R Block pour accéder au site Web de l'ARC, quelque chose qui a été mis en place avec des sociétés privées et l'ARC au cours des deux dernières décennies pour l'utilisation de la déclaration en ligne… D'une manière ou d'une autre, quelqu'un a obtenu ces identifiants et les a utilisés pour modifier les informations et se faire passer pour un imposteur afin d'accéder au site Web de l'ARC. L'autre point concerne le partage des renseignements privés des clients.

Tout d'abord, je trouve intrigant votre manque de curiosité quant à la manière dont cela s'est produit, votre manque de coopération et le manque de coopération de votre entreprise. Historiquement, je pense qu'il y a eu une énorme coopération entre les sociétés privées de préparation des déclarations de revenus et l'ARC pour s'assurer que cela ne se produise pas.

M. Peter Davis: Je ne dirais pas qu'il n'y a pas eu de coopération. Nous avons certainement communiqué avec l'ARC tout au long de cet incident, dans la mesure du possible, et nous avons…

Mme Brenda Shanahan: Monsieur Davis, qu'est-ce qui ferait dire à l'ARC qu'il était question de H&R Block?

M. Peter Davis: Pardon. Qu'est-ce qui ferait dire à l'ARC qu'il était question de H&R Block pour...?

Mme Brenda Shanahan: Le rapport dont nous disposons affirme que des pirates informatiques ont obtenu des données confidentielles utilisées par H&R Block. Il s'agit des identifiants confidentiels que H&R Block utilise pour accéder à l'ARC. Quelqu'un, d'une manière ou d'une autre, à H&R Block… Il peut s'agir d'un employé. Il peut s'agir d'une personne qui a eu accès à l'information, ou d'un tiers, comme l'a indiqué M. Chambers. J'y reviendrai dans un instant.

M. Peter Davis: Pour être clair, comme je l'ai mentionné précédemment, nous prenons la protection des renseignements personnels de nos clients avec le plus grand sérieux. Je veux insister sur…

Mme Brenda Shanahan: Il ne s'agit pas de renseignements personnels. D'une manière ou d'une autre, quelqu'un s'est emparé de vos codes.

M. Peter Davis: Oui.

Mme Brenda Shanahan: Pourquoi l'ARC affirme-t-elle que ce sont les codes de H&R Block qui ont été utilisés?

M. Peter Davis: J'allais justement en parler.

Notre enquête n'a pas suggéré, de quelque manière que ce soit, que nos systèmes ont été compromis ni que nos dispositifs de sécurité ou nos logiciels…

Mme Brenda Shanahan: Vous soutenez que vos codes n'ont pas été utilisés lors de cette violation. C'est ce que vous affirmez?

M. Peter Davis: Non, j'affirme que H&R Block Canada, nos systèmes logiciels et nos dispositifs de sécurité n'ont pas été compromis, et que nous ne sommes donc pas responsables de…

Mme Brenda Shanahan: Vous le répétez, mais quelqu'un aurait pu utiliser vos codes et les laisser intacts pour que vous ne sachiez pas qu'ils avaient été utilisés. C'est l'ARC, de l'autre côté, qui a dit: « Hmm, ces codes sont utilisés ».

M. Peter Davis: Oui, et l'ARC ne nous a jamais dit qu'elle croyait que ces renseignements avaient été compromis par H&R Block Canada.

Mme Brenda Shanahan: Nous allons mettre cela de côté, mais je pense vraiment qu'il est important qu'il y ait une coopération entre toutes les parties à cet égard, aujourd'hui et à l'avenir.

En ce qui concerne la divulgation de renseignements personnels, vous indiquez ce qui suit sur votre site Web:

> Nous ne divulguons pas vos renseignements personnels à des tiers, sauf dans les cas décrits dans la présente politique de confidentialité, avec votre consentement, ou dans les cas où la loi le permet ou l'exige. Vos renseignements personnels peuvent être divulgués…

Je comprends l'argument de M. Villemure selon lequel les gens ne savent pas toujours à quoi ils consentent, mais voici ce à quoi ils consentent:

> À des fournisseurs externes employés ou retenus par nous ou par H&R Block US pour exécuter certains services ou fonctions… y compris… le traitement des transactions… le marketing, le traitement Remboursements instantanés[MD]…

C'est là pour ceux qui veulent le lire. J'ai un deuxième exemplaire si des gens veulent le lire.

Le site Web indique également que ces renseignements seront « utilisés ou stockés en toute sécurité aux États-Unis et seront, en plus des lois canadiennes, également soumis aux lois des États-Unis. »

Je pense que de nombreux Canadiens ne savent pas que leurs renseignements sont stockés aux États-Unis, ce qui peut poser problème à certaines personnes.

● (1640)

Le président: Votre temps est écoulé, madame Shanahan.

Monsieur Davis, je vais vous donner l'occasion de répondre rapidement. La parole est à vous.

M. Peter Davis: J'aimerais simplement souligner, comme je l'ai mentionné plus tôt, que nous sommes très fiers du cadre de protection de la vie privée des clients que nous avons mis en place à nos bureaux de détail chez H&R Block Canada. Une grande partie de cette démarche consiste à accompagner nos clients dans le processus du formulaire d'assurance de protection des renseignements personnels. Nous leur expliquons exactement comment leurs renseignements sont utilisés pour leur fournir les produits et services qu'ils attendent. Les éléments auxquels vous faites référence sont des éléments que nous examinons avec nos clients. Nous nous assurons qu'ils comprennent ce que cela signifie et nous veillons à obtenir leur consentement.

Le président: Merci, monsieur Davis.

[*Français*]

Monsieur Villemure, vous avez la parole pour deux minutes et demie.

M. René Villemure: Merci beaucoup, monsieur le président.

Monsieur Davis, chez H&R Block, des atteintes à la sécurité des données des clients ont-elles déjà eu lieu par le passé?

[*Traduction*]

M. Peter Davis: Je ne suis pas en mesure, en raison de notre politique sur la sécurité des données et la protection des renseignements personnels, d'entrer dans les détails de ce sujet particulier, mais ce que je peux dire au Comité…

M. Matthew Green: Monsieur le président, j'invoque le Règlement.

Le président: Allez-y, monsieur Green, pour votre rappel au Règlement.

M. Matthew Green: Monsieur le président, je ne pense pas que M. Davis comprenne bien le processus dans lequel il se trouve actuellement. Il ne peut pas fournir une réponse classique au Parlement sans devoir répondre à des questions de base.

S'il n'est pas à l'aise de répondre à ces questions devant un comité, je lui demanderais, par votre intermédiaire, monsieur le président, de le faire par écrit à notre comité, s'il ne veut pas le faire en direct devant l'auditoire, afin que notre comité puisse en tenir compte. Nous pourrions alors déterminer s'il y a lieu d'en faire état. Il ne peut pas simplement se présenter devant un comité parlementaire de la Chambre des communes et refuser de répondre à des questions de base.

Le président: Laissez-moi m'en occuper, monsieur Davis.

Monsieur Green, je suis tout à fait d'accord avec vous pour dire que ces réponses peuvent être fournies par écrit au Comité, si le Comité le souhaite. Si c'est ce que vous voulez faire, monsieur Green, si nous voulons que des renseignements soient fournis au Comité, nous pouvons certainement le faire.

Je crois que M. Davis est sincère dans ses tentatives de répondre aux questions du Comité. Encore une fois, comme je l'ai dit précédemment, je comprends qu'il s'agit d'une question délicate. Si la nature des questions est suffisamment délicate, nous pouvons demander à M. Davis une réponse écrite sur ces sujets, dans l'intérêt du Comité.

Monsieur Barrett, vous avez la parole pour ce rappel au Règlement.

[*Français*]

Monsieur Villemure, j'ai arrêté le chronomètre.

[*Traduction*]

M. Michael Barrett (Leeds—Grenville—Thousand Islands et Rideau Lakes, PCC): Cela s'est produit à plusieurs reprises. Je suis tout à fait d'accord avec l'intervention de M. Green. Il est évident que le témoin est tenu de fournir une réponse complète, au mieux de ses capacités, à toutes les questions posées par les membres du Comité.

Comme vous l'avez dit, monsieur le président, il appartient au Comité d'accepter ou non une réponse écrite. C'est la proposition de M. Green. Je n'ai pas d'objection à cela. Il convient toutefois de noter que le Comité a toujours la prérogative de décider si ces renseignements doivent rester confidentiels ou s'ils doivent être publiés — si leur publication est peut-être, pour dire les choses simplement, dans l'intérêt du public —, mais le témoin n'a pas le pouvoir discrétionnaire de répondre ou non à la question.

Bien que nous n'ayons pas d'objection à ce que la réponse à cette question de M. Villemure soit fournie par écrit, une réponse doit être fournie.

Le président: Compte tenu des deux rappels au Règlement, je pense que la position du Comité à ce sujet est assez claire, monsieur Davis.

Je ne veux pas parler au nom des autres membres du Comité, mais si vous estimez que ces renseignements peuvent être fournis au Comité, je vous recommande de le faire, et le Comité en disposera comme il l'entendra, en fonction des répercussions qu'ils auront sur cette étude pour nous aussi, car il s'agit d'une question très sérieuse pour les Canadiens. J'espère que vous comprenez.

Une autre option s'offre également au Comité. Il s'agit de passer à huis clos et de régler cette question, mais je ne veux pas vraiment que cela se fasse à moins que le Comité en décide ainsi.

Monsieur Green, cela vous convient-il?

● (1645)

M. Matthew Green: Oui. En ce qui concerne le rappel au Règlement — et il ne s'agit pas de M. Davis en particulier, car je sais qu'il est ici à titre personnel —, je veux juste que le Comité note que c'est une tendance de longue date que nous constatons maintenant quand les entreprises envoient leurs responsables des relations publiques ou des relations avec le gouvernement et non le président. À l'avenir, je pense que ce qu'il faut faire avec ce comité, pour obtenir des réponses complètes, c'est d'inviter ici à comparaître des gens qui ont le pouvoir et la discrétion de parler au nom de la société à laquelle nous parlons.

Je vous demanderais d'en tenir compte pour les prochaines invitations.

Le président: Oui, je pense que nous devrons être plus précis lorsque nous proposerons des motions sur les personnes que nous voulons voir comparaître devant le Comité, comme vous l'avez dit, monsieur Green. Est-ce juste?

[*Français*]

Monsieur Villemure, vous avez...

[*Traduction*]

M. Peter Davis: Monsieur le président, puis-je poursuivre sur le rappel au Règlement qui a été fait plus tôt? Je tiens à préciser très rapidement que si jamais il y avait une atteinte à la protection des renseignements personnels, notre entreprise serait tenue par la loi de signaler…

Le président: Attendez.

[*Français*]

Il n'y a pas d'interprétation.

M. René Villemure: Le son va et vient. Parfois, il y a de l'interprétation, parfois, il n'y en a pas.

Le président: Cela fonctionne-t-il, maintenant? Ce sont peut-être les écouteurs qui sont défectueux.

[*Traduction*]

Cela ne fonctionne-t-il pas du tout?

Je suis désolé, monsieur Davis. Nous allons nous assurer que M. Villemure entende votre point de vue.

Cela ne concerne pas vraiment le rappel au Règlement. Je vous ai donné un peu de latitude sur ce point, monsieur Davis, simplement parce que nous avons moins de temps que d'habitude.

[*Français*]

Cela fonctionne maintenant, monsieur Villemure.

[*Traduction*]

Monsieur Davis, vous pouvez peut-être exposer rapidement votre point de vue.

M. Peter Davis: Merci.

Très rapidement, s'il arrivait que des renseignements fassent partie d'une quelconque atteinte, notre organisation serait légalement tenue de communiquer cette atteinte au commissaire à la protection de la vie privée.

Nous n'essayons pas d'être évasifs devant le Comité, mais nous devons également respecter nos politiques en matière de protection des renseignements personnels.

Le président: Merci. C'est merveilleux.

[*Français*]

Monsieur Villemure, la parole est à vous pour deux minutes.

M. René Villemure: Merci beaucoup.

Tous ces points d'interrogation faisaient partie de ma question, également. Je vous remercie.

Je ne vous demandais pas quelles mesures avaient été prises. Je vous demandais plutôt s'il y avait eu de telles fuites ou non.

[*Traduction*]

M. Peter Davis: Je vous remercie de la question. Faites-vous référence à l'incident concernant les authentifiants de dossiers électroniques en particulier? D'accord.

Notre enquête a également porté sur ce point, et il n'y a jamais eu d'incident impliquant nos authentifiants de dossiers électroniques dans le passé.

[*Français*]

M. René Villemure: D'accord.

Je sais que vous en avez parlé brièvement plus tôt, mais les atteintes à la vie privée ont-elles toutes été rapportées au commissaire à la protection de la vie privée du Canada?

[*Traduction*]

M. Peter Davis: Je ne suis pas un expert en matière de signalement des atteintes à la vie privée, mais je peux dire que si nous devions signaler quelque chose au commissaire à la protection de la vie privée, nous le ferions absolument.

[*Français*]

M. René Villemure: Serait-il possible de demander à votre équipe de nous fournir cette réponse?

[*Traduction*]

M. Peter Davis: Oui. Merci.

[*Français*]

M. René Villemure: C'est très bien.

Merci beaucoup, monsieur le président.

Le président: Merci, monsieur Villemure.

[*Traduction*]

Monsieur Green, vous avez deux minutes et demie. Allez-y, s'il vous plaît.

M. Matthew Green: Merci beaucoup.

Je voudrais revenir sur les déclarations préliminaires concernant les atteintes à la sécurité dans le secteur privé.

Lors de sa comparution le 5 décembre 2024, le commissaire à la protection de la vie privée du Canada a déclaré: « Dans l'ensemble, les atteintes à la sécurité des données sont l'une des principales menaces qui pèsent sur les renseignements personnels. Durant l'exercice 2023-2024, qui s'est terminé le 31 mars 2024, le Commissariat a reçu plus de 350 rapports de cyberincidents dont la vaste majorité, soit plus de 90 %, provenait d'organisations du secteur privé. »

Monsieur Davis, selon vous, ces statistiques montrent-elles que les cyberincidents sont plus fréquents et plus susceptibles de se produire dans les organisations du secteur privé que dans les institutions du gouvernement fédéral?

● (1650)

M. Peter Davis: Je ne suis pas un expert en matière d'atteintes à la vie privée, et je ne suis donc pas en mesure de donner un avis sur les endroits où de telles atteintes auraient tendance à se produire le plus souvent.

M. Matthew Green: Monsieur Davis, vous êtes venu apporter un témoignage d'expert.

Dans votre lettre au Comité, vous avez déclaré: « Il n'existe aucune base crédible pour soutenir l'idée que la production automatisée de déclarations de revenus par l'ARC et les déclarations de revenus préremplies sécuriseront davantage les informations des contribuables ».

D'après les statistiques très générales que je viens de vous fournir, comment expliquez-vous la différence entre les atteintes à l'égard des institutions du gouvernement et celles du secteur privé?

M. Peter Davis: Je suis désolé, mais je ne vois pas le lien entre la production automatisée de déclarations de revenus par l'ARC et les atteintes potentielles à la vie privée dans le secteur privé. Pouvez-vous m'éclairer un peu à ce sujet?

M. Matthew Green: Oui, avec plaisir.

Sur l'ensemble des incidents, 90 % des signalements d'atteintes à la vie privée provenaient d'organisations du secteur privé et 10 % du gouvernement. Cette logique ne s'étend-elle pas aux organisations du secteur privé qui sont plus vulnérables aux atteintes à la vie privée?

M. Peter Davis: Comme je l'ai déjà dit, je ne peux pas me prononcer sur des statistiques que je ne connais que de seconde main. Je ne suis pas en mesure de porter un jugement éclairé sur ce point.

M. Matthew Green: Selon vous, qu'est-ce qui explique cette différence?

M. Peter Davis: Encore une fois, je ne peux pas me prononcer de façon éclairée sur les statistiques que j'entends de seconde main.

M. Matthew Green: D'accord.

Monsieur le président, par votre intermédiaire, M. Davis peut-il fournir au Comité, par écrit, une politique d'atteinte aux données des clients? En fait, ce que je demande, c'est la politique de H&R Block Canada en cas d'atteinte à l'intégrité des données des clients.

Le président: D'accord. Merci, monsieur Green. La greffière en a pris note. Nous ferons le suivi avec M. Davis et veillerons à ce que cette information soit fournie.

Monsieur Barrett, vous avez cinq minutes.

M. Michael Barrett: Monsieur le président, le 6 décembre, j'ai donné avis d'une motion que je vais maintenant proposer:

> Que le Comité entreprenne un examen des politiques de confidentialité des données et de passation de marchés employées par Exportation et développement Canada (EDC) pendant la mise en œuvre du programme du Compte d'urgence pour les entreprises canadiennes (CUEC), que le Comité fasse rapport de ses conclusions et recommandations à la Chambre, et que le Comité invite les personnes suivantes à témoigner:
>
> (a) Julie Sweet, PDG d'Accenture, et ses représentants;
>
> (b) Mairead Lavery, cheffe de la direction d'EDC, et ses représentants;
>
> (c) La vérificatrice générale du Canada, Karen Hogan.

Le président: Merci, monsieur Barrett. La motion est recevable.

Voulez-vous en parler?

M. Michael Barrett: Oui.

Le président: D'accord.

Monsieur Davis, je vais vous demander de partir, si vous le souhaitez. Je m'attends à ce que votre témoignage devant le Comité se termine avec la transition vers le prochain groupe de témoins et une discussion à ce sujet.

Comme je l'ai dit précédemment, la greffière a pris note de la demande du Comité. Elle vous communiquera ces informations, et le Comité s'attend à ce que vous nous les renvoyiez dans un délai raisonnable. La greffière indiquera la date à laquelle ces informations devront être fournies, et ce ne sera pas le jour de Noël. Je vous le garantis.

Merci, monsieur Davis, de votre témoignage.

Je donne maintenant la parole à M. Barrett.

Mme Brenda Shanahan: J'invoque le Règlement.

Le président: Allez-y.

Mme Brenda Shanahan: Monsieur le président, pouvons-nous avoir le texte de la motion? Habituellement, vous nous donnez une idée de ce qui s'en vient.

Le président: D'accord.

Madame la greffière, cette motion a-t-elle déjà été envoyée aux membres du Comité?

La greffière du Comité (Mme Nancy Vohl): Oui.

Le président: D'accord.

Nous l'enverrons, madame Shanahan, mais je vais donner la parole à M. Barrett pour qu'il puisse poursuivre.

Allez-y, monsieur Barrett.

M. Michael Barrett: Monsieur le président, le 2 décembre, la vérificatrice générale a publié un rapport qui est à l'origine de cette motion. Je parle du « Rapport 8: Compte d'urgence pour les entreprises canadiennes » en lien avec la pandémie de COVID-19. C'est un rapport indépendant. Le même jour, cet enjeu a fait l'objet d'une vaste couverture médiatique. Un avis de motion a été déposé et distribué dans les deux langues officielles à tous les membres du Comité le 6 décembre. Ceux-ci ont donc eu amplement le temps de se familiariser avec la motion et avec la situation dans la langue officielle de leur choix. Les rapports de la vérificatrice générale sont évidemment disponibles en anglais et en français dans leur version complète en ligne, et ils ont été mis à la disposition de tous les députés sous forme imprimée, soumis à embargo avant d'être déposés à la Chambre.

La vérificatrice générale du Canada a constaté qu'Exportation et développement Canada avait accordé 314 millions de dollars en contrats à fournisseur unique pour l'administration des prêts. Le gouvernement a confié à EDC le soin d'administrer ce programme de prêts d'urgence, mais EDC a par la suite fait volte-face et déclaré: « Nous n'avons pas la capacité nécessaire, et nous allons donc externaliser. » Le ministère a externalisé des contrats représentant des centaines de millions de dollars de l'argent des contribuables.

Certains détails de ces contrats sont extrêmement préoccupants. On a payait 14 heures par jour à Accenture pour les activités du centre d'appels, qui, pourtant, n'était ouvert que neuf heures par jour. Le tarif horaire par personne allait de 60 à 750 $. Tout aussi préoccupant, Accenture a confié une partie des tâches à une filiale brésilienne. Ces gens recevaient donc des salaires horaires de 750 $ pour administrer un programme qu'EDC était censé mettre en œuvre. Dire que c'était « généreux » est un euphémisme. Je suis tout à fait certain qu'aucun fonctionnaire ne gagne 750 $ l'heure. Il y a là un énorme conflit d'intérêts.

Pour conclure, je vais citer Karen Hogan, la vérificatrice générale. À son avis, il était impensable de ne pas régler ce conflit d'intérêts. Je ne saurais dire mieux. Il s'agit évidemment des renseignements personnels des Canadiens, des programmes du gouvernement du Canada et d'un conflit d'intérêts extrêmement préoccupant. Ce conflit d'intérêts a été jugé « inacceptable » par la vérificatrice générale.

Cette question s'inscrit effectivement dans le mandat du Comité. C'est important. Je ne pense pas que cette étude exigerait beaucoup de réunions. Le Comité a pour mandat de régler ces conflits d'intérêts. Alors que d'autres comités peuvent faire ce que font d'autres comités, le nôtre doit faire ce que lui seul peut faire. C'est la raison de cette motion.

● (1655)

Le président: Merci, monsieur Barrett.

J'ai vu d'abord M. Drouin. Je donnerai ensuite la parole à Mme Shanahan.

M. Matthew Green: Regardez-vous l'écran?

Le président: Je suis désolé, monsieur Green. Je n'étais pas sûr que vous ayez levé la main. La toile de fond est contrastée avec quelque chose de rouge qui rend les choses difficiles à distinguer.

Je vais donc donner la parole à M. Green, parce que je n'étais pas sûr qu'il ait levé la main, mais que c'était effectivement le cas.

Allez-y, monsieur.

M. Matthew Green: Merci beaucoup.

C'est une simple question sur la motion.

Elle ne précise pas d'échéance. Je tiens à ce qu'il soit bien clair pour le Comité que je n'ai pas l'intention d'être rappelé en raison d'une quelconque prérogative secrète du président ou en vertu de l'article 106(4) du Règlement. C'est une question importante, j'en conviens. J'estime qu'il faudra y accorder toute notre attention au retour de la Chambre. Je tiens à ce que ce soit clair.

Monsieur le président, puis-je demander si c'est l'intention de cette motion ou si c'est quelque chose qu'on cherchera à relancer au début de janvier en raison d'un cycle médiatique lent ou quelque chose de ce genre?

Le président: Posez-vous une question à ce sujet, monsieur Green?

M. Matthew Green: C'est une question honnête à l'auteur de la motion, parce qu'il n'y a pas de date, pas plus que d'indication comme « quand nous reprendrons les séances régulières de la Chambre ». Pour l'instant, c'est ouvert.

Je ne voudrais pas me trouver dans une situation où nous serions rappelés et devrions laisser nos électeurs et nos familles.

Le président: Il y a aussi que le nombre de réunions n'est pas précisé, monsieur Green. J'en ai également pris note.

Voulez-vous répondre rapidement, monsieur Barrett? Allez-y.

M. Michael Barrett: Nous accepterions aussi bien une entente au lieu d'un amendement — que le Comité donne suite à l'entente ou que la présidence assume l'entente selon laquelle cette motion sera examinée après la reprise des travaux de la Chambre au cours de la dernière semaine de janvier. Si la motion est adoptée, je pense que nous pourrons tous nous entendre sans que ce soit explicité.

Quant au nombre de réunions, je pense qu'il y en aurait probablement peu.

● (1700)

Le président: Oui. Compte tenu du nombre de témoins ici présents, il n'y en aurait probablement pas plus de deux.

M. Michael Barrett: Nous n'aurions pas d'objection.

Le président: D'accord.

Malheureusement, j'aurai besoin d'un amendement pour cela, à moins que le Comité ne consente unanimement à ce qu'on ne consacre pas plus de deux réunions à cette question. Les choses seraient plus claires ainsi.

Rien dans cette motion n'indique le nombre de réunions. Je vais demander qu'on précise qu'on ne consacrera pas plus deux réunions à cette motion.

M. Francis Drouin (Glengarry—Prescott—Russell, Lib.): Monsieur le président, nous devrions peut-être entendre tous les autres témoins avant de décider du nombre de réunions.

Le président: Oui, faisons cela.

M. Francis Drouin: Nous ne sommes pas encore sûrs d'être prêts.

Le président: Par souci de clarté, j'aurais besoin que quelqu'un me dise combien de réunions on veut consacrer à cette question. C'était ma suggestion avant de vous entendre, mais je vais m'en tenir à cela.

Allez-y, monsieur Drouin.

[*Français*]

M. Francis Drouin: Je salue les efforts de mon cher collègue M. Barrett. Au Comité permanent des comptes publics, nous sommes en train de faire une étude sur la question du Compte d'urgence pour les entreprises canadiennes. Il le sait puisqu'il a comparu devant ce comité. En fait, nous essayons de faire une étude sur les comptes publics. Depuis quelques jours, nous essayons de la programmer, mais les conservateurs font de l'obstruction systématique pour ne même pas entendre les témoins. La vérificatrice générale était devant nous hier, et nous recevions aussi d'autres témoins, mais les conservateurs ont fait de l'obstruction systématique.

Avant de voter sur cette motion, j'inviterais M. Barrett à parler avec MM. Perkins et Genuis, ainsi qu'avec M. Cooper, qui siège aussi parfois au Comité permanent des comptes publics. J'invite donc M. Barrett à discuter avec ses collègues. Je suis entièrement en faveur de l'efficacité des comités parlementaires. Si le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique décide de faire cette étude sur le programme du Compte d'urgence pour les entreprises canadiennes, vous pouvez être assurés que je ne serai pas d'accord pour gaspiller l'argent des contribuables en faisant la même étude au Comité permanent des comptes publics.

Je sais que c'est Noël et que nous sommes tous pressés d'adopter des motions et de retourner à la maison en disant que nous avons accompli des choses, mais j'invite mes collègues à avoir une discussion avec leurs autres collègues parlementaires.

[*Traduction*]

Dans cet esprit, monsieur le président, je veux m'assurer que nous ne dupliquons pas les services ou la responsabilité parlementaire. J'y crois sincèrement, mais la vérificatrice générale a déposé beaucoup de rapports le 2 décembre. Il y en a eu un sur les aînés. Et un autre sur les emplois d'été au Canada. Assurons-nous que nos comités parlementaires fonctionnent de façon efficace et qu'ils vont au fond des choses. Ne nous enfermons pas dans une situation comme celle que nous avons vécue avec TDDC, où le comité de l'industrie faisait la même étude en même temps et où les mêmes députés posaient les mêmes questions aux deux comités, avec les mêmes témoins.

J'aime bien cette idée, et je ne suis pas un membre régulier du comité de l'éthique, mais nous sommes en train de faire double emploi. Je suis certain que les conservateurs conviendront qu'on ne dépense pas efficacement l'argent des contribuables quand le comité des comptes publics... à moins qu'ils puissent convaincre leurs collègues du comité des comptes publics de laisser le comité de l'éthique se charger de cette étude pendant qu'ils se concentreront sur d'autres rapports de la vérificatrice générale. Cette solution me satisferait.

Je suis certain que les députés, puisqu'ils veulent former un gouvernement, en auraient déjà discuté avec leurs collègues pour que l'argent des contribuables soit dépensé plus efficacement. Nous aussi, nous dépensons de l'argent, et il est important de témoigner du respect aux contribuables.

Le président: Merci, monsieur Drouin.

Nous avons l'obligation d'examiner la motion dont nous sommes saisis. La motion est recevable. Elle porte sur la protection des renseignements personnels et le risque de... Eh bien, nous ne le savons pas. Si la motion est adoptée, nous le saurons sûrement en convoquant ces témoins.

Je considère que c'est distinct de ce que font d'autres comités en ce moment. Il s'agit d'une motion sur la confidentialité des données. C'est tout à fait conforme au mandat du Comité.

Allez-y, madame Shanahan.

● (1705)

Mme Brenda Shanahan: Merci, monsieur le président.

Je suis désolée de ne pas avoir eu la motion à portée de main. J'ai ici un dossier, comme vous pouvez le voir, contenant toutes les motions qui ont été présentées au Comité. J'essaie de suivre. Ce n'est pas facile. Je suppose que nous pouvons laisser celles-ci de côté pour l'instant ou les garder pour une date ultérieure. Elles seront peut-être relancées. Je ne sais pas si quelqu'un peut... parce que c'est de plus en plus lourd. Je peux vous dire que ce n'est pas bon pour mon dos.

Je suis désolée. Je suis de la vieille école. J'aime le papier. Cela me permet de lire, d'analyser, de prendre des notes et ainsi de suite.

J'ai écouté avec beaucoup d'intérêt mon collègue du comité des comptes publics. Je crois qu'il touche à quelque chose d'important. C'est un sujet qui a été soulevé très souvent, même ici, à savoir que nous ne devrions pas faire du travail en double.

Vous n'ignorez évidemment pas que les jours de notre mandat pour la 44e législature sont comptés. Nous devrions faire le meilleur usage du temps qu'il nous reste. Il y a de nombreuses questions à discuter. J'aimerais qu'on fasse le point sur les rapports qui ne sont pas terminés et sur le travail encore à faire au sujet de motions que d'autres députés semblent vouloir examiner.

Je comprends bien la proposition de limiter cette étude à deux réunions, mais pourquoi pas aucune? Laissons le comité des comptes publics faire son travail.

Parlant de laisser les autres faire leur travail, j'ai souvent remarqué que ce comité essaie de faire le travail de nos commissaires indépendants du Parlement, notamment du commissaire aux conflits d'intérêts et à l'éthique, sans parler d'autres commissaires de temps à autre. Mais c'est surtout du commissaire aux conflits d'intérêts et à l'éthique qu'il s'agit. Nous essayons de prendre de l'avance sur lui quand il y a un problème. Je suis certaine que les députés sont tout à fait capables d'alerter le commissaire s'ils estiment qu'il y a un conflit d'intérêts, comme n'importe qui dans la population. Quiconque s'inquiète de cette situation pourrait la signaler au commissaire.

Nous l'avons vu, dans certains cas à plusieurs reprises pour la même plainte — une, deux, trois ou quatre fois —, revenir avec la même conclusion. Apparemment, ce n'était pas suffisant pour les députés à l'époque, mais c'est tout de même conforme au rôle d'un agent indépendant, d'un haut fonctionnaire du Parlement. Ils font leur travail, ils font leur enquête et ils remettent un rapport. Je proposerais effectivement d'aller dans ce sens.

En l'état, je ne peux pas appuyer cette motion.

Merci.

Le président: Merci, madame Shanahan.

Pour l'information du Comité, le directeur et d'autres représentants du SCRS sont dans la salle pour discuter de TikTok avec notre prochain groupe de témoins.

Je vais donner la parole à M. Fisher, qui est le suivant sur la liste.

M. Darren Fisher: Merci, monsieur le président.

Par respect pour les témoins qui sont ici, je serai bref.

Cette question est étudiée par un autre comité. Elle pourrait effectivement relever de notre mandat. Le comité des comptes publics y a déjà consacré deux réunions. J'ai entendu des députés ici présents déclarer assez catégoriquement qu'ils ne sont pas d'accord avec le double emploi, c'est-à-dire que deux comités étudient la même chose. Voyons comment ils voteront.

Je ne vais pas appuyer la motion pour l'instant. Cela ne veut pas dire que je ne l'appuierai pas plus tard, peut-être après l'étude du comité des comptes publics. Mais, pour aujourd'hui, je voterai contre. Nous pourrions ensuite écouter les témoins.

Le président: Allez-y, monsieur Housefather. Vous avez la parole au sujet de la motion.

M. Anthony Housefather (Mont-Royal, Lib.): Merci, monsieur le président.

Je serai bref, moi aussi.

Je commencerai par dire que je ne suis pas tout à fait d'accord avec ma chère collègue, Mme Shanahan. La surveillance du travail de la vérificatrice générale et de tout le monde par les comités est à mes yeux tout à fait fondamentale. C'est le rôle des parlementaires. Je n'y vois aucun problème.

Ce qui me préoccupe, c'est que, après examen du rapport et de son résumé, je n'y ai rien trouvé au sujet de la protection des renseignements personnels, même pas dans le résumé. Ce rapport porte sur les contrôles financiers et les contrats, et cela n'est pas du ressort du comité de l'éthique. Cela relève du comité des comptes publics. Je ne comprends pas pourquoi le comité de l'éthique est saisi de cette question. J'ai lu le résumé. La protection des renseignements personnels n'y est même pas mentionnée. C'est vraiment là le problème pour moi.

Le comité des comptes publics s'en occupe déjà. S'il ne s'agit pas de protection des renseignements personnels, je ne vois vraiment pas en quoi que cela nous concerne. Il serait assurément fascinant d'examiner les modes de passation de marchés employés par EDC, dont il est question dans cette motion, mais je ne crois tout simplement pas que cela relève du comité de l'éthique.

Merci, monsieur le président.

● (1710)

Le président: Merci, monsieur Housefather.

Comme il n'y a personne d'autre sur ma liste, je vais demander — et je crois connaître la réponse — si nous avons un consentement unanime à l'égard de cette motion.

M. Michael Barrett: Je demande un vote par appel nominal.

Le président: Nous allons procéder à un vote par appel nominal.

Je vous écoute, madame la greffière.

Comme il y a égalité des voix, je vais voter oui.

(La motion est adoptée par 6 voix contre 5.)

Le président: Je vais suspendre la séance quelques minutes pour permettre au prochain groupe de témoins de s'installer.

● (1710)

_____(Pause)_____

● (1715)

Le président: Bon retour à tous.

Conformément à l'article 108(3)h) du Règlement et à la motion adoptée par le Comité le jeudi 21 novembre 2024, nous reprenons notre étude de la liquidation de TikTok Technology Canada, Inc.

Je souhaite la bienvenue aux témoins de la deuxième heure de notre séance d'aujourd'hui.

Du Service canadien du renseignement de sécurité, nous accueillons Daniel Rogers, directeur, et Paul Lynd, sous-ministre adjoint, Collecte de renseignements.

Je vous donne la parole, monsieur Rogers. Vous avez cinq minutes pour présenter votre exposé au Comité. Allez-y, monsieur.

M. Daniel Rogers (directeur, Service canadien du renseignement de sécurité): Merci, monsieur le président.

[*Français*]

Monsieur le président, mesdames et messieurs les membres du Comité, bonjour.

J'aimerais faire quelques remarques, et je vais essayer de les faire assez vite.

Je m'appelle Daniel Rogers et je suis directeur du Service canadien du renseignement de sécurité, ou SCRS. Je suis accompagné de mon collègue Paul Lynd, le sous-ministre adjoint chargé de la collecte de renseignements.

C'est un honneur pour nous d'être ici aujourd'hui et d'avoir la possibilité de contribuer à votre importante discussion sur la liquidation de TikTok Canada. J'espère être en mesure de vous éclairer sur le rôle que joue le SCRS en matière de sécurité nationale, ainsi qu'en matière de protection de la population et des intérêts relatifs à la prospérité du pays.

Administrée par Innovation, Sciences et Développement économique Canada, la Loi sur Investissement Canada, ou LIC, garantit que les investissements importants qu'effectuent des non-Canadiens au Canada sont avantageux pour l'économie canadienne. Elle permet ainsi au gouvernement d'examiner ces investissements, afin de s'assurer qu'ils ne portent pas atteinte à la sécurité nationale.

La LIC vise à établir un équilibre entre la prospérité économique et la protection du Canada contre les acteurs étrangers qui cherchent à acquérir des biens, des technologies, des infrastructures ou des renseignements personnels sensibles ou à en prendre le contrôle, et ce, à des fins qui pourraient être néfastes pour la sécurité nationale du Canada.

[*Traduction*]

Conformément à son mandat, le SCRS passe régulièrement en revue les avis d'investissement suscitant des préoccupations liées à la sécurité déposés au titre de la LIC, et collabore avec Innovation, Sciences et Développement économique Canada, avec Sécurité publique Canada et avec les organismes subventionnaires fédéraux pour alimenter le processus décisionnel du gouvernement. Il s'agit d'un travail essentiel, car le Canada constitue une cible pour nombre d'acteurs étatiques adverses qui, par leurs activités d'investissement, cherchent à favoriser leurs intérêts nationaux aux dépens de ceux du Canada.

Les auteurs de menaces s'intéressent particulièrement aux médias sociaux en raison des données qu'ils génèrent et recueillent: des sondages y sont effectués, des ensembles de données s'y constituent et, conformément aux conditions d'utilisation, les utilisateurs y donnent accès à leurs données personnelles, c'est-à-dire leurs albums photos, leurs messages et leurs listes de contacts, entre autres informations sensibles. Bien qu'elles soient plutôt anodines en elles-mêmes, certaines de ces informations, lorsqu'elles sont recueillies et réunies en quantité, peuvent permettre de cerner précisément des tendances et d'en apprendre davantage sur divers groupes, sur l'opinion publique, les communautés, et sur les réseaux sociaux et professionnels individuels.

Pour mener des activités d'ingérence étrangère, des États autoritaires comme la République populaire de Chine exploitent des mégadonnées provenant notamment du secteur privé. Au Canada, l'utilisation des données par le gouvernement est assujettie à des obligations sur le plan de l'éthique, de la loi et du respect de la vie privée; ce n'est pas le cas au sein des États autoritaires. La loi de 2017 sur le renseignement national adoptée par la RPC contraint les entités et les citoyens chinois à coopérer sur demande avec ses services de renseignement, ce qui implique de fournir toute information à l'État et à son appareil du renseignement. Cette politique appuie et reflète les tentatives d'ingérence de la RPC au Canada et dans les démocraties de même tendance. Par conséquent, le Canada et ses alliés doivent redoubler de prudence lorsqu'ils acceptent de communiquer leurs données à des plateformes liées à la RPC.

Le processus d'examen prévu par la LIC, auquel le SCRS a contribué, a permis d'établir que permettre à TikTok Canada de poursuivre ses activités porterait atteinte à la sécurité nationale. Bien que les dispositions de la LIC limitent ce que je peux communiquer sur un dossier en particulier, je souligne que l'évaluation faite par le SCRS et le gouvernement du Canada concorde avec l'Énoncé de politique sur l'examen des investissements étrangers dans le secteur des médias numériques interactifs formulé en mars 2024. En particulier, les facteurs suivants entrent en ligne de compte dans ces examens: la portée et le public cible, la nature et l'étendue des liens de l'investisseur avec un gouvernement étranger, ainsi que la propension de l'entreprise canadienne à être utilisée par l'État étranger afin de propager de la désinformation ou d'imposer une censure incompatible avec les droits et les valeurs des Canadiennes et des Canadiens.

● (1720)

[*Français*]

L'utilisation des médias sociaux soulève également des préoccupations relatives à la sécurité nationale lorsque ces derniers constituent un terreau fertile aux idéologies extrémistes et servent à radicaliser leurs utilisateurs. La quantité de propos violents qui se tiennent en ligne augmente, tout comme, en conséquence, la probabilité que les consommateurs de tels contenus se mobilisent à la violence. C'est une situation préoccupante. Principaux utilisateurs des médias sociaux, les jeunes peuvent être particulièrement vulnérables à la radicalisation en ligne.

Le Service canadien du renseignement de sécurité, ou SCRS s'affaire à enquêter sur les menaces pour la sécurité nationale et à formuler des conseils à cet égard en vue de les contrer. Il est en outre résolu à renforcer la résilience grâce au pouvoir modernisé découlant du projet de loi C-70qui lui a été conféré à cet effet.

Le nouveau pouvoir de renforcement de la résilience témoigne du fait qu'assurer la sécurité nationale du Canada est une tâche collective à laquelle doivent participer tous les ordres de gouvernement, les collectivités canadiennes, le milieu universitaire et le secteur privé, entre autres intervenants. Le SCRS entend collaborer avec ces groupes dans l'intérêt national, notamment par la communication accrue d'informations détaillées sur les menaces.

En conclusion, je profite de l'occasion qui m'est donnée pour répondre à vos questions. Gardez toutefois à l'esprit qu'il m'est impossible de fournir publiquement des détails sur certaines activités opérationnelles ou enquêtes du SCRS.

Merci.

Le président: Monsieur Rogers, je vous remercie pour votre allocution.

Nous allons commencer le premier tour de questions.

Monsieur Cooper, vous avez la parole pour six minutes.

[*Traduction*]

M. Michael Cooper (St. Albert—Edmonton, PCC): Merci, monsieur le président.

Merci, monsieur Rogers.

Concernant le partage de données personnelles avec le régime de Pékin, vous avez cité la loi chinoise sur le renseignement de 2017. En théorie, il semble vrai que les données des utilisateurs canadiens de TikTok risquent d'être partagées avec la RPC. Mais les représentants de TikTok qui ont comparu devant le Comité il y a quelques semaines nous ont dit que les données n'avaient pas été partagées et qu'un pare-feu avait effectivement été mis en place pour empêcher que ce soit possible.

Pourriez-vous nous en parler?

M. Daniel Rogers: Je peux parler du premier point, c'est-à-dire de l'inquiétude concernant le risque que ces données soient transmises à la Chine. Comme on l'a déjà dit au Comité, je crois, ces données ne sont pas entièrement hébergées au Canada. Des questions se posent quant à l'applicabilité de la loi chinoise aux entreprises chinoises, y compris à ByteDance, la société mère de TikTok. On peut très bien admettre que les données détenues par TikTok Canada puissent, comme vous l'avez laissé entendre, être communiquées à la République populaire de Chine.

M. Michael Cooper: À ce stade, cela me semble plus théorique qu'autre chose.

M. Daniel Rogers: Je ne peux pas parler publiquement d'un cas précis de données ainsi transmises et dont nous aurions eu connaissance grâce au renseignement, mais c'est un risque qui préoccupe beaucoup d'entre nous du point de vue de la sécurité nationale.

M. Michael Cooper: En quoi la fermeture de la filiale de TikTok a-t-elle une incidence quelconque sur ce risque? Il me semble que cela n'a rien à voir. Dans la mesure où il y a un risque, il persiste, n'est-ce pas?

● (1725)

M. Daniel Rogers: Effectivement. Vous avez raison, la fermeture de la filiale TikTok Canada n'élimine pas l'utilisation de l'application ici au Canada, ni les données qu'elle détient. Pour revenir à ce que j'ai dit dans mon exposé préliminaire au sujet de la cohérence de la décision avec les énoncés de politique précédents, je rappelle que le processus décisionnel dans ce contexte est un processus de la LIC. Certains événements déclenchent des décisions et des examens en vertu de la LIC, qui est administrée par ISDE. Le SCRS fournit des conseils en matière de sécurité nationale dans le contexte de ces examens.

M. Michael Cooper: Je vous remercie.

Le manque total de transparence de ce gouvernement concernant cette décision est troublant. D'un côté, il ferme la filiale de TikTok. De l'autre, les Canadiens sont libres d'utiliser l'application. Je ne vois pas nécessairement pourquoi il ne devrait pas en être ainsi, mais il ne semble pas y avoir de cohérence. Si l'on s'inquiète effectivement de l'utilisation de renseignements personnels ou du partage de données personnelles par et avec le régime communiste chinois, la mesure adoptée par le gouvernement ne semble pas du tout être une solution.

J'aimerais au moins comprendre, du point de vue théorique du partage de données personnelles avec la République populaire de Chine, puisque TikTok a mis sur pied le projet Texas, qui garantit que les données américaines restent aux États-Unis.

J'essaie de comprendre. Quand vous dites que certaines de ces données risquent d'être partagées et qu'elles ne sont pas entièrement hébergées au Canada ou ne restent pas au Canada, que voulez-vous dire? Sont-elles stockées aux États-Unis?

M. Daniel Rogers: Globalement, le problème est que la société mère de TikTok Canada est une entité chinoise assujettie aux lois de la RPC et que cela pourrait obliger l'entreprise à prendre des mesures comme obtenir des données ou utiliser la plateforme pour d'autres fins jugées utiles par le Parti communiste chinois. Ce risque existe toujours.

M. Michael Cooper: Est-il vrai que la société chinoise ByteDance exploite l'algorithme et en est propriétaire?

M. Daniel Rogers: À ce que je sache, oui.

M. Michael Cooper: D'accord.

Est-ce que l'algorithme est exploité en Chine, en RPC?

M. Daniel Rogers: Je ne suis pas bien placé pour parler des activités spécifiques de TikTok. Il faudrait poser la question à ses représentants. J'imagine que c'est plus décentralisé. Je ne pourrais pas en parler de façon crédible.

M. Michael Cooper: D'accord.

Eu égard au risque, au moins du point de vue théorique, ce serait certainement un problème dans la mesure où l'algorithme est exploité par la société chinoise ByteDance. Pour que l'algorithme fonctionne, les données doivent nécessairement être partagées avec ByteDance. Dans la mesure où l'algorithme est utilisé par ByteDance, alors, oui, en vertu de la loi chinoise sur le renseignement de 2017, l'entreprise pourrait être obligée de partager des données avec le régime de Pékin.

Je ne vois aucune preuve que cela se soit effectivement produit. Cela semble tout à fait théorique.

Le président: Merci, monsieur Cooper.

Nous avons dépassé le temps prévu.

Monsieur Rogers, pourriez-vous répondre rapidement à cette question? C'était davantage un commentaire qu'une question, à mon avis.

M. Daniel Rogers: Je pense avoir répondu à cette question. Je me ferais un plaisir de...

Le président: D'accord.

Pour l'information du Comité, j'ai bien demandé à la greffière de communiquer avec TikTok pour voir si des témoins seraient disponibles, parce que je pensais qu'ils pourraient être utiles à cette discussion. Comme vous le savez peut-être, l'entreprise a déposé une contestation juridique contre l'ordonnance de fermeture du gouvernement fédéral. Il n'est donc pas surprenant qu'elle n'ait pas de témoins à présenter aujourd'hui.

Monsieur Housefather, vous avez six minutes. Allez-y.

● (1730)

M. Anthony Housefather: Merci beaucoup.

Monsieur Rogers, bienvenue au Comité.

Je suis heureux de vous voir, monsieur Lynd.

Les questions de M. Cooper étaient très bonnes, mais je ne crois pas qu'elles portaient sur la décision découlant de la LIC. Cette décision n'avait rien à voir avec la protection des renseignements personnels des utilisateurs canadiens, mais portait sur d'autres enjeux liés à la sécurité nationale. Sinon, s'il s'agissait vraiment de protection des renseignements personnels, nous aurions complètement interdit l'application.

N'est-ce pas?

M. Daniel Rogers: J'espère que cela répondra à votre question.

Oui, vous avez raison de dire que la décision découlant de la LIC était propre à TikTok Canada, parce que c'est la transaction qui a déclenché l'examen.

M. Anthony Housefather: Dans le cadre de sa contestation judiciaire, TikTok Canada a invoqué des mesures procédurales injustes concernant l'examen de la sécurité nationale.

Je présume que vous n'êtes pas d'accord avec cette affirmation.

M. Daniel Rogers: Je tiens à préciser que le SCRS n'est qu'une partie de cet examen. Nous fournissons des conseils et des évaluations en matière de sécurité nationale qui s'inscrivent dans un contexte décisionnel plus large. La décision globale n'est pas prise par le SCRS, comme il se doit. Elle est prise par d'autres. Il y a des mesures de protection entourant cette décision, notamment le secret du Cabinet, la confidentialité en matière de sécurité nationale et l'information susceptible d'appartenir à l'entreprise. Il y a une limite aux détails que je peux fournir, et c'est vrai aussi parce qu'il y a une affaire devant les tribunaux, sur laquelle je ne peux pas me prononcer.

Je peux dire que le SCRS a participé à la décision. Nous avons fourni des conseils en matière de sécurité nationale. Comme je l'ai dit dans mon exposé préliminaire, la décision est conforme à la politique. C'est à peu près tout ce que je peux dire.

M. Anthony Housefather: Je comprends.

Sans vous demander si le SCRS a suggéré la décision dans ses conseils — à savoir obliger l'entreprise à fermer ses portes —, puis-je vous demander si, dans le cadre de son examen, le SCRS a constaté que les opérations de TikTok au Canada suscitaient des préoccupations importantes en matière de sécurité liées à l'influence étrangère?

M. Daniel Rogers: Je peux dire que le SCRS a fourni des conseils en matière de sécurité nationale et que nous avons constaté qu'il y avait des raisons d'être préoccupé par l'établissement de TikTok au Canada. La décision finale a été ce qu'elle est.

M. Anthony Housefather: A-t-on tenu compte de la décision du Congrès américain prévoyant que l'entreprise devrait, dans un certain délai, être vendue à un propriétaire national ou américain?

M. Daniel Rogers: Ce n'est pas une considération qui serait entrée en ligne de compte pour le SCRS.

M. Anthony Housefather: Vous n'avez rien examiné d'autre que la loi pour dire si, oui ou non, certaines préoccupations vous obligeraient à agir.

M. Daniel Rogers: C'est bien cela. Le SCRS a un rôle assez précis, qui consiste à fournir des évaluations concernant la sécurité nationale à l'appui du processus décisionnel.

M. Anthony Housefather: Permettez-moi de revenir aux questions sur la protection des renseignements personnels posées par M. Cooper.

David Vigneault, l'ancien directeur du SCRS, avait prévenu les Canadiens qu'ils devraient éviter l'application TikTok parce qu'elle pose un risque pour la sécurité des données.

Êtes-vous d'accord avec ce conseil? Est-ce aussi votre avis?

M. Daniel Rogers: M. Vigneault a fait une déclaration raisonnable.

Je dois m'en tenir à mon rôle au SCRS, qui n'est pas de prendre des décisions ou de faire des recommandations au nom du gouvernement.

Je peux certainement dire sans équivoque qu'il y a des risques pour la sécurité nationale que nous estimons inhérents à TikTok comme plateforme, du point de vue de ce que j'ai expliqué tout à l'heure au sujet de la possibilité que les données, les algorithmes et d'autres choses soient utilisés par la RPC contre les intérêts du Canada.

M. Anthony Housefather: Puisque vous êtes là, est-ce que le SCRS examine actuellement les algorithmes de TikTok ou l'a-t-il fait pour déterminer si des renseignements erronés circulent sur la plateforme dans différents domaines? Par exemple, les algorithmes de TikTok favorisent-ils l'antisémitisme au Canada en faisant circuler un narratif incitant des gens ou des utilisateurs à s'opposer à l'État d'Israël?

M. Daniel Rogers: Il est vrai que ce genre de rhétorique et de narratifs est omniprésent sur de nombreuses plateformes de médias sociaux, pas seulement sur TikTok Canada. Je n'ai rien de précis à dire au sujet de l'algorithme de TikTok Canada.

Comme je l'ai dit tout à l'heure, nous sommes très préoccupés par la quantité de contenu en ligne qui sert à radicaliser les gens, notamment les jeunes, contre un certain nombre de cibles, dont la communauté juive, la communauté LGBT et bien d'autres. C'est une tendance qui nous inquiète de plus en plus.

M. Anthony Housefather: Pouvez-vous au moins me dire si j'ai raison de supposer que le SCRS continue de surveiller les manifestations d'extrémisme sur la plateforme TikTok et d'autres plateformes semblables utilisées aujourd'hui au Canada?

M. Daniel Rogers: Oui, sur TikTok et sur d'autres plateformes. En fait, nous et nos alliés du Groupe des cinq, de même que nos alliés chargés de l'application de la loi, avons récemment publié un communiqué de presse et des lignes directrices sur la radicalisation des jeunes en ligne. Il est difficile d'enquêter, parce que les gens sont souvent radicalisés uniquement en ligne, notamment les jeunes. C'est une tendance inquiétante.

● (1735)

M. Anthony Housefather: Merci.

Est-ce qu'il me reste du temps, monsieur le président?

Le président: Il vous reste une minute et 10 secondes.

M. Anthony Housefather: D'accord.

Désolé. Vous êtes encore coincé avec moi.

Je vais revenir à l'algorithme dont vous avez parlé. Si j'ai bien compris, l'algorithme de TikTok Canada ne serait pas différent de l'algorithme que l'entreprise utilise aux États-Unis et dans d'autres pays, du moins d'après ce que l'entreprise déclare. Toujours si j'ai bien compris, l'un des problèmes associés à TikTok est qu'il s'y est répandu beaucoup de désinformation au sujet des élections américaines en 2016, en 2020 et peut-être en 2024.

Le SCRS a-t-il réfléchi à ce que nous devrions faire pour nous protéger au moment des élections canadiennes qui devraient avoir lieu l'an prochain, en 2025?

M. Daniel Rogers: Comme vous le savez sûrement, le SCRS est très préoccupé par les questions concernant l'ingérence étrangère dans les élections. Cela englobe la possibilité pour les auteurs de menaces d'utiliser des plateformes de médias sociaux pour répandre de la désinformation ou d'autres messages préjudiciables aux intérêts du Canada. Ce n'est pas une préoccupation propre à telle ou telle plateforme. Cela concerne davantage l'intention d'adversaires étrangers d'utiliser des plateformes, quelle que soit la façon dont ils pourraient obtenir leur...

M. Anthony Housefather: Je parle précisément du gouvernement chinois — nous avons un comité parlementaire spécial qui s'occupe de la Chine — qui est un adversaire étranger et qui utilise son algorithme sur TikTok, lequel, à ce que nous sachions, pourrait être contrôlé par le gouvernement chinois ou assurément par des sources chinoises dans le but d'aider un camp ou l'autre dans une élection canadienne.

Le président: Vous savez que votre temps de parole est écoulé.

Veuillez répondre très rapidement.

M. Anthony Housefather: Je suis désolé.

Oui. La réponse peut être très succincte.

Le président: Je vais vous laisser répondre brièvement, monsieur Rogers.

M. Daniel Rogers: Ma réponse succincte est que c'est l'une de nos préoccupations, compte tenu de la loi de la RPC et de l'utilisation de TikTok.

M. Anthony Housefather: Merci.

Le président: Merci, monsieur Housefather.

[*Français*]

Monsieur Villemure, vous avez la parole pour six minutes.

M. René Villemure: Merci beaucoup, monsieur le président.

Je vous remercie de votre présence aujourd'hui. Je trouve que vos propos sont clairs.

On a parlé d'un examen approfondi. Qu'est-ce qu'un examen approfondi?

M. Daniel Rogers: Qu'est-ce qu'un examen?

[*Traduction*]

Pour nous, cela dépend. Dans le cadre général d'une enquête, il pourrait s'agir d'une enquête sur un auteur de menaces précis. Dans le contexte de TikTok et de la LIC, il s'agirait d'un examen des activités d'une entreprise, de ses liens avec des gouvernements étrangers et des données dont le SCRS pourrait disposer dans ses réserves de renseignements susceptibles de révéler la possibilité qu'un adversaire étranger utilise une transaction contraire aux intérêts du Canada.

[*Français*]

M. René Villemure: Pourrait-on parler un peu plus en détail des risques pour la sécurité nationale qui ont mené à la liquidation de TikTok?

M. Daniel Rogers: Oui, un peu, mais comme je l'ai dit plus tôt, je ne peux pas donner de détails précis.

[*Traduction*]

En l'occurrence, il y a des préoccupations au sujet de l'utilisation de TikTok comme plateforme en général. TikTok Canada est évidemment affiliée à cette plateforme. Ces deux éléments ne sont pas sans lien.

Je ne peux pas parler des préoccupations précises que nous aurions au sujet de TikTok Canada, compte tenu des enjeux dont j'ai parlé tout à l'heure.

[*Français*]

M. René Villemure: La raison de ma question est simple. Par le passé, on a parfois vu la sécurité nationale être interprétée de façon très large et être utilisée comme prétexte.

Pouvez-vous nous parler de l'entreprise ByteDance et de son actionnariat? Elle possède TikTok, on le sait bien, mais a-t-elle aussi d'autres activités?

M. Daniel Rogers: Parlez-vous des activités de ByteDance en général?

M. René Villemure: Oui, et je parle aussi de son actionnariat.

M. Daniel Rogers: D'accord.

[*Traduction*]

Globalement, ByteDance est une entreprise chinoise. C'est notre principale préoccupation dans le contexte de cet examen. Elle exploite évidemment l'application TikTok, qui est une application mondiale accueillant des millions et des millions d'utilisateurs. Elle est assujettie à la réglementation chinoise de la sécurité nationale. Elle pourrait être utilisée par la Chine contre les intérêts du Canada.

[*Français*]

Je suis désolé, je ne sais pas si j'ai bien répondu à votre question.

M. René Villemure: Qui sont les propriétaires de ByteDance?

M. Daniel Rogers: Je ne le sais pas exactement.

M. René Villemure: On nous parle souvent du fait que le conseil d'administration de ByteDance est composé de Français, entre autres, mais je crois que le fondateur de TikTok est toujours très présent dans l'actionnariat.

M. Daniel Rogers: Je ne le sais pas. Je ne voudrais pas donner des informations inexactes.

M. René Villemure: Outre le partage de renseignements avec le Parti communiste chinois, y a-t-il d'autres formes de collaboration entre TikTok, ByteDance et le gouvernement chinois?

● (1740)

M. Daniel Rogers: Comme M. Cooper l'a dit, il y a quelques préoccupations théoriques sur ce plan. Nous savons que la loi chinoise sur la sécurité nationale s'applique à ByteDance et aux opérations de TikTok.

[*Traduction*]

Je ne peux pas parler de données de renseignement précises liées à quoi que ce soit de concret que nous saurions grâce aux canaux du renseignement.

[*Français*]

M. René Villemure: Dans le cadre de votre enquête au nom du ministère, avez-vous collaboré avec le commissaire à la protection de la vie privée du Canada?

[*Traduction*]

M. Daniel Rogers: Nous discutons régulièrement avec le commissaire à la protection de la vie privée. Dans le cadre de ces examens, l'évaluation est habituellement effectuée par le SCRS en fonction des données recueillies grâce au renseignement et de l'évaluation des menaces.

[*Français*]

M. René Villemure: Ce genre d'examen a-t-il lieu plus souvent que d'autres, par exemple?

M. Daniel Rogers: Oui, je pense que le SCRS en a fait plus de 1 000 l'année dernière.

M. René Villemure: D'accord, c'est quand même beaucoup.

Le rapport final est-il maintenant disponible?

M. Daniel Rogers: Notre avis au gouvernement?

M. René Villemure: Oui.

M. Daniel Rogers: Non, ce n'est pas disponible publiquement.

[*Traduction*]

Cela fait partie des conseils que nous donnons au gouvernement. Dans le cadre du processus décisionnel, ces conseils sont souvent assujettis à d'autres dispositions, comme le secret du Cabinet, et, comme je l'ai dit tout à l'heure, ils comportent des renseignements classifiés et parfois des renseignements privés de la société.

[*Français*]

M. René Villemure: Le souci que j'ai rejoint celui de M. Cooper. En effet, on nous dit à la fois qu'il faut bannir TikTok, et qu'on peut continuer de l'utiliser, c'est notre choix. C'est paradoxal, à mon avis.

Avez-vous contribué à la décision du gouvernement du Canada de bannir TikTok des appareils gouvernementaux?

[*Traduction*]

M. Daniel Rogers: L'interdiction de TikTok sur les appareils gouvernementaux a été une décision du Conseil du Trésor du Canada. De notre point de vue, la collecte de données par TikTok, notamment à partir d'appareils gouvernementaux, pourrait soulever des préoccupations en matière de sécurité nationale, et j'estime que cela diffère quelque peu de l'utilisation générale de la plateforme.

Je dois dire que le processus décisionnel, non seulement en ce qui concerne la Loi sur Investissement Canada, mais aussi l'interdiction de TikTok sur les appareils gouvernementaux, tient très souvent compte de nombreux facteurs différents, pas seulement de la sécurité nationale. Il peut s'agir de facteurs économiques, sociaux ou autres. S'agissant de décisions gouvernementales, on pense notamment aux données du gouvernement et aux préoccupations liées à la sécurité nationale qui y seraient intimement liées.

[*Français*]

M. René Villemure: Utilisez-vous TikTok?

M. Daniel Rogers: Non.

M. René Villemure: Monsieur Lynd, utilisez-vous TikTok?

M. Paul Lynd (sous-ministre adjoint, Collecte de renseignements, Service canadien du renseignement de sécurité): Non.

M. René Villemure: D'accord.

Merci, monsieur le président.

Le président: Je n'utilise pas TikTok non plus. Je n'en vois pas l'utilité.

[*Traduction*]

Monsieur Green, vous avez six minutes. Utilisez-vous TikTok?

M. Matthew Green: Oui, je l'utilisais assez régulièrement jusqu'au moment où j'ai cessé de le faire en raison des enquêtes Canada-Chine ont révélé le ciblage de députés. Les cas d'ingérence ou d'influence de médias sociaux dans le cadre de processus électoraux démocratiques sont bien connus et bien documentés. Rappelez-vous Cambridge Analytica en 2016, sans parler de toutes les fois où Elon Musk est intervenu dans les dernières élections aux États-Unis.

Monsieur Rogers, je vous souhaite la bienvenue au Comité. Je crois que c'est la première fois que j'ai l'occasion de discuter avec vous. D'après vous, en quoi TikTok diffère-t-elle sensiblement des autres plateformes de médias sociaux dans la façon dont les renseignements, les données, les algorithmes et les profils des utilisateurs sont utilisés?

M. Daniel Rogers: Si tant est que je puisse répondre à la question, je dirais que les Canadiens et d'autres s'inquiètent en général des plateformes de médias sociaux. Il y a, entre autres, la propagation de désinformation et la possibilité d'utiliser ces plateformes pour radicaliser des Canadiens ou pour nuire au Canada. Ce n'est pas propre à TikTok. C'est une constante des plateformes de médias sociaux.

Les préoccupations concernant plus particulièrement TikTok ont trait au régime en vertu duquel elle peut fonctionner, parce qu'elle est hébergée et contrôlée, en théorie du moins, par la Chine et assujettie aux lois chinoises sur la sécurité nationale. On sait que le type d'utilisation des données est un facteur important, et les protections garanties au Canada et dans d'autres pays ne sont pas les mêmes. Il existe des recours juridiques au Canada, et nous avons des protections en vertu de la Charte. Beaucoup de choses propres à notre pays n'ont pas d'équivalent en Chine.

M. Matthew Green: Votre examen a-t-il révélé des preuves ou des renseignements que vous êtes en mesure de communiquer publiquement et qui indiqueraient que TikTok a enfreint des lois canadiennes?

● (1745)

M. Daniel Rogers: Nous avons clairement indiqué dans le cadre du processus décisionnel que les préoccupations en matière de sécurité nationale liées à TikTok Canada avaient fait partie de notre réflexion. Je ne peux pas vous donner de détails à ce sujet, mais je peux vous dire que nous n'avons pas besoin que TikTok ait enfreint les lois canadiennes pour avoir des préoccupations en matière de sécurité nationale, et...

M. Matthew Green: Je suis désolé. Comme mon temps est limité, je dois reprendre la parole.

Avez-vous des préoccupations au sujet d'autres plateformes, comme Truth Social, X, Discord et WhatsApp? Nous avons cette discussion dans l'espoir d'envisager la situation de façon plus exhaustive et non pas limitée à une seule plateforme. Pourriez-vous nous parler des menaces de radicalisation, dont vous avez parlé plusieurs fois au Comité, mais cette fois dans le cadre d'autres plateformes?

M. Daniel Rogers: Nos préoccupations concernant la diffusion d'information et la radicalisation ne sont pas propres à telle ou telle plateforme, et nous n'avons pas non plus, du moins à ma connaissance — je suis directeur depuis seulement six semaines — effectué un examen semblable de l'une ou l'autre de ces plateformes pour l'instant, en tout cas pas dans le cadre du processus de la LIC. Nos préoccupations concernent davantage le contenu et la possibilité que des Canadiens soient radicalisés sur ces plateformes...

M. Matthew Green: Définissez le mot « radicalisation ». Vous l'utilisez, mais que signifie-t-il sur le plan juridique?

M. Daniel Rogers: Merci de cette question. Dans notre contexte, cela signifie habituellement... Je l'utilise comme abréviation de « radicalisation menant à la violence ».

Il y a un seuil. Les gens ont le droit de s'exprimer librement au Canada. Ils peuvent dire ce qu'ils veulent sur les médias sociaux et consommer l'information qu'ils souhaitent, mais, pour nous, la radicalisation est le processus par lequel une personne adhère à des croyances et les traduit en intention de commettre des actes de violence et de nuire à des personnes ici au Canada.

Monsieur Lynd, auriez-vous quelque chose à ajouter au sujet de la radicalisation?

M. Paul Lynd: C'est bien cela sur le fond, une mobilisation en vue de soutenir des actes de violence ou de commettre des actes de violence.

M. Matthew Green: Pourriez-vous nous en donner des exemples récents au Canada?

M. Daniel Rogers: Eh bien, vous avez probablement vu qu'on a arrêté un certain nombre de suspects ayant épousé des idéologies radicales et qui avaient peut-être planifié des attaques — des jeunes dans certains cas. Il y a aussi ceux qui vivent dans une chambre d'écho en ligne et qui ont peut-être moins de liens à l'extérieur pour tempérer ce qu'ils...

M. Matthew Green: Ce ne sont pas des exemples. Ce sont des généralités. Pour être plus précis, je veux parler du massacre de la mosquée de Québec, de l'attaque à la bombe incendiaire de la mosquée Ibrahim Jame, à Hamilton, et de la famille renversée par un camion-bélier à London. Est-ce que ce sont des cas de radicalisation?

M. Daniel Rogers: Je ne voudrais pas faire erreur. Je n'utiliserai pas le nom, mais je sais effectivement que certaines des arrestations de cette année sont principalement liées à la radicalisation en ligne. Je ne veux pas vous induire en erreur et vous fournir un nom qui ne serait pas le bon, mais je me ferai un plaisir de vous revenir à ce sujet si cela vous est utile.

M. Matthew Green: Vous est-il possible d'énumérer, dans le cas de TikTok, les principaux risques en matière de sécurité nationale que vous avez circonscrits et qui ont mené à la décision du gouvernement du Canada d'ordonner sa liquidation?

M. Daniel Rogers: Je ne peux pas me prononcer sur les détails, si ce n'est pour dire que nous avons fourni une évaluation de la sécurité nationale soulignant certains risques à cet égard.

M. Matthew Green: D'accord. Quel risque y a-t-il à communiquer publiquement au Comité certains de ces renseignements?

M. Daniel Rogers: Eh bien, pour commencer, il y a dans les documents confidentiels du Cabinet des privilèges que nous devons respecter dans le cadre du processus décisionnel du gouvernement. De plus, les tribunaux sont saisis d'une affaire qui devra faire l'objet d'une procédure équitable, et je dois tenir compte du fait que cette procédure n'a pas encore commencé. Il y a peut-être des renseignements classifiés susceptibles de révéler des sources ou des techniques ou qui auraient pu nous être communiqués par nos alliés et que ceux-ci ne nous autoriseraient pas à divulguer publiquement.

M. Matthew Green: En vertu de la Loi sur le SCRS, vous êtes évidemment dans l'obligation de dire la vérité devant les tribunaux. Si, dans le cadre de la procédure civile, on vous pose ces questions, vous serez obligé de divulguer ces renseignements. N'est-ce pas?

M. Daniel Rogers: Je ne peux pas vous donner d'avis juridique précis. Je sais qu'il existe des moyens de protéger l'information dans le cadre de diverses procédures judiciaires au Canada et qu'ils pourraient être applicables en l'occurrence. Je n'ai pas examiné en détail la façon dont cette affaire pourrait se dérouler et les renseignements qui pourraient y être révélés.

Le président: Merci, monsieur Green.

Merci, monsieur Rogers.

Cela met fin à notre première série de questions. Je suis sûr que cette affaire judiciaire sera suivie très attentivement par beaucoup de gens.

Monsieur Barrett, vous avez cinq minutes. Allez-y, monsieur.

M. Michael Barrett: Concernant la décision découlant de la Loi sur Investissement Canada, quelles sont les solutions de rechange ou les alternatives à la fermeture complète d'une entité ici au Canada?

● (1750)

M. Daniel Rogers: Il vaudrait peut-être mieux poser certaines de ces questions à ISDE, qui applique la plupart des dispositions de la loi. Notre contribution se limite à fournir une évaluation de la sécurité nationale.

Cela dit, je crois savoir qu'il existe d'autres solutions, par exemple des mécanismes d'atténuation, mais je ne voudrais pas parler en son nom.

M. Michael Barrett: Pourriez-vous nous donner un exemple de mécanisme d'atténuation?

M. Daniel Rogers: Je n'en ai pas à l'esprit pour l'instant. Excusez-moi, mais ce n'est pas le domaine d'expertise du SCRS à l'égard de la loi.

M. Michael Barrett: Le risque pour la sécurité nationale est si grand que, en vertu de la Loi sur Investissement Canada, le siège social de cette entité a reçu l'ordre de cesser ses activités au Canada, mais les Canadiens peuvent l'utiliser sans restriction. Que doivent en penser les Canadiens? Le risque est tellement grand que le gouvernement a ordonné la fermeture de cette entité, mais il leur dit de ne pas hésiter à continuer d'utiliser l'application. Quelle conclusion les Canadiens sont-ils censés en tirer?

M. Daniel Rogers: Le SCRS a été clair, comme je le suis maintenant, au sujet des risques liés à l'application elle-même.

M. Michael Barrett: Pourriez-vous être clair? Les Canadiens devraient-ils continuer d'utiliser TikTok?

M. Daniel Rogers: Nous avons dit, et je le répète ici, que l'utilisation de TikTok en général soulève des préoccupations en matière de sécurité nationale, notamment au regard de la quantité globale de données et de la possibilité que le gouvernement chinois utilise la plateforme contre les intérêts du Canada.

M. Michael Barrett: Êtes-vous en train de dire que les Canadiens devraient l'utiliser ou non?

M. Daniel Rogers: Je dis que ce n'est pas au SCRS de faire ce genre de recommandation aux Canadiens ou de prendre ce genre de décision à leur place.

Le SCRS peut fournir une évaluation de la sécurité nationale, mais il est très important que d'autres facteurs entrent en ligne de compte dans ces décisions. La décision concernant TikTok Canada est très différente de la décision concernant TikTok en général, parce qu'il y a des facteurs très différents en jeu.

M. Michael Barrett: Quant à la question distincte de savoir si les Canadiens... Je ne parle pas d'une interdiction. Je ne parle que de conseils. Vous êtes le directeur du principal organisme de renseignement au Canada. Vous êtes à l'avant-garde et, bien que ce soit un nouveau poste, vous avez été nommé en raison de vos compétences et de votre vaste expérience dans le milieu du renseignement au Canada.

Les Canadiens devraient-ils continuer d'utiliser TikTok? Je ne demande pas si le gouvernement devrait l'interdire pour les Canadiens. Je vous demande si, à titre de dirigeant du SCRS, vous croyez qu'il est sage pour les Canadiens de l'utiliser.

M. Daniel Rogers: Il y a une très grande différence entre le choix individuel d'utiliser quelque chose et l'effet global sur la sécurité nationale canadienne.

Je peux vous donner un exemple personnel. Quand j'étais jeune, je n'imaginais pas être un jour le directeur du SCRS. À l'époque, j'ai peut-être examiné l'information disponible et j'ai décidé de continuer d'utiliser TikTok parce que je ne voyais pas alors en quoi cela pourrait être un souci, quand bien même la Chine aurait accès à mes renseignements. Je m'en soucie aujourd'hui parce que je suis le directeur du SCRS.

À mon avis, les gens doivent tenir compte de leurs propres risques. C'est un facteur important pour prendre une décision. À ce stade, je ne peux pas parler au nom du gouvernement, mais je peux dire qu'il y a des risques dont j'espère que les Canadiens tiendront compte lorsqu'ils décideront personnellement d'utiliser TikTok.

M. Michael Barrett: Vous avez parlé d'agrégation des données — qu'il s'agisse de renseignements, d'images, de géolocalisation, et des tendances et habitudes des Canadiens. Ces renseignements sont recueillis, peut-être utilisés par la dictature communiste de Pékin, et agrégés.

Il me reste environ une minute.

À l'échelle individuelle, quels sont les risques pour les jeunes utilisateurs canadiens — les jeunes M. Rogers et futurs directeurs du SCRS —, en 50 secondes s'il vous plaît, monsieur?

M. Daniel Rogers: Si le souci est que le gouvernement chinois puisse avoir accès aux données, ces jeunes sont informés des activités d'ingérence étrangère, des actes de répression transnationale et d'autres activités contraires aux intérêts individuels et collectifs du Canada. Toute personne qui utilise TikTok aujourd'hui devrait savoir que ses données peuvent être assujetties à ce régime.

Si vous vous opposez ouvertement au gouvernement de la Chine ou au Parti communiste chinois, vous pourriez avoir des soucis immédiats. Sinon, il se peut que vous en ayez un jour, et vous devez vous demander si vous voulez prendre ce risque.

M. Michael Barrett: Des entreprises locales de ma collectivité s'interrogent sur le fait qu'elles vendent leurs produits au Canada en utilisant TikTok. Que dois-je leur dire? Devraient-elles s'inquiéter?

M. Daniel Rogers: Le même conseil s'applique à elles. Les données et l'utilisation de TikTok seront accessibles au régime que nous avons décrit. Ces entreprises doivent prendre une décision.

● (1755)

M. Michael Barrett: Merci.

Le président: C'était une discussion intéressante, monsieur Rogers.

Que tout le monde sache que je vais donner la parole à M. Bains pour cinq minutes.

[*Français*]

M. Villemure et M. Green vont disposer de deux minutes et demie chacun.

C'est ainsi que va se terminer notre réunion.

[*Traduction*]

Je vois que M. Green lève le pouce.

Monsieur Bains, vous avez cinq minutes. Allez-y.

M. Parm Bains (Steveston—Richmond-Est, Lib.): Merci, monsieur le président.

Merci aux représentants du renseignement de sécurité d'être parmi nous aujourd'hui.

Je vous remercie de votre travail, de vos mesures proactives en matière d'engagement communautaire et de votre travail concernant le projet de loi C-70, notamment au sujet du renforcement de la Loi sur l'ingérence étrangère et la protection de l'information, ce qui n'avait pas été fait depuis plus de 20 ans. Je tiens à vous remercier, vous et le ministère, de votre travail à cet égard.

Je vais commencer par dire que la prolongation des activités de TikTok pourrait permettre à des acteurs étrangers d'exploiter les données des utilisateurs canadiens ou de répandre de la désinformation. Est-ce un énoncé exact pour vous, monsieur Rogers?

M. Daniel Rogers: Je crois que le début de votre question m'a échappé.

Je crois que vous avez demandé si TikTok pouvait permettre la propagation de désinformation. C'est vrai, et c'est aussi vrai pour d'autres plateformes de médias sociaux.

M. Parm Bains: Plus précisément, j'ai dit que les activités de TikTok pourraient permettre à des acteurs étrangers d'exploiter les données des utilisateurs canadiens et de répandre de la désinformation. Est-ce exact?

M. Daniel Rogers: Oui, c'est exact.

M. Parm Bains: Quelles directives le SCRS a-t-il données concernant le calendrier de liquidation de TikTok pour réduire au minimum les risques potentiels pour la sécurité publique et notre intégrité démocratique?

M. Daniel Rogers: Notre rôle est de conseiller le gouvernement à cet égard. Nous lui avons fourni des conseils sur un certain nombre d'éléments décisionnels, dont le plus récent, à savoir la liquidation de TikTok Canada.

Nous recueillons aussi des renseignements de sécurité, évidemment. Quand nous pouvons en recueillir pour informer le gouvernement des moyens par lesquels des adversaires étrangers ou d'autres utilisent les plateformes de médias sociaux pour compromettre la sécurité du Canada, nous le faisons, et ces renseignements classifiés entreront en ligne en compte dans les décisions à venir du gouvernement.

M. Parm Bains: Pour revenir à ce que mon collègue M. Barrett a dit au sujet de la présence physique de TikTok en sol canadien par opposition à l'application proprement dite, pourriez-vous expliquer la distinction?

M. Daniel Rogers: Oui. L'application elle-même peut continuer de fonctionner indépendamment de la présence de TikTok Canada sur notre sol.

M. Parm Bains: Est-ce que le risque est différent si l'entreprise est installée ici? Est-ce qu'il est important pour nous qu'elle ne soit pas installée sur notre sol indépendamment de l'application proprement dite? Je crois savoir qu'elle peut continuer à produire de l'information, à recueillir des données et à utiliser des algorithmes pour saisir de l'information sur ce que font les gens, mais n'est-ce pas là la question?

M. Daniel Rogers: L'examen de TikTok Canada a soulevé des préoccupations en matière de sécurité nationale qui étaient propres à ces activités. Dans le contexte de la Loi sur Investissement Canada, nous examinons les activités elles-mêmes, et c'est ce dont le gouvernement a tenu compte pour prendre sa décision à ce moment-là.

M. Parm Bains: Vous avez parlé de nos alliés du Groupe des cinq. Le gouvernement s'est aligné sur ses alliés eu égard aux risques associés à TikTok.

Comment le SCRS évalue-t-il la réponse du Canada à ces risques comparativement à celle de ses alliés? Que font ces derniers? Échangez-vous de l'information entre vous pour savoir ce qui est efficace et ce qui ne l'est pas?

M. Daniel Rogers: Très bonne question. Nos alliés ont des systèmes différents d'examen des investissements et de contrôle des applications, ainsi que d'autres types de cadres législatifs. On ne peut pas comparer terme à terme.

La principale activité du SCRS est de veiller à partager et à comparer les renseignements de sécurité et les évaluations avec nos alliés du Groupe des cinq. Nous nous intéressons, par exemple, aux activités de la Chine et d'autres pays en lien avec les plateformes de médias sociaux comme TikTok et, probablement quand c'est possible, aux mesures d'atténuation qui se sont révélées efficaces grâce à la collecte de renseignement.

M. Parm Bains: TikTok a son siège social en Chine. C'est une entreprise chinoise, mais elle est utilisée par des milliards de personnes. Êtes-vous en mesure d'identifier certains pays hostiles qui l'utilisent plus que d'autres?

● (1800)

M. Daniel Rogers: J'invite mon collègue à intervenir s'il en sait plus que moi.

Nous avons effectivement constaté que des acteurs étrangers utilisent de nombreuses plateformes de médias sociaux, dont TikTok. Nous avons exprimé publiquement nos préoccupations au sujet de la désinformation répandue et de l'influence exercée par la Russie, la Chine et d'autres pays.

Monsieur Lynd, voulez-vous ajouter quelque chose?

M. Paul Lynd: Certainement.

Ce qui inquiète au sujet de TikTok est son association avec la Chine. Comme nous l'avons dit ici, TikTok recueille beaucoup de données personnelles et a accès à beaucoup de données personnelles sur nos appareils. Le SCRS a très publiquement signalé les risques liés à l'utilisation de TikTok. Il est tout à fait évident que la Chine a pour stratégie de recueillir des données massives et des données personnelles partout dans le monde.

La Chine est également la principale source de menace en matière d'ingérence étrangère au Canada. Quand on recueille une grande quantité de données personnelles et que, en plus, on dispose de l'intelligence artificielle et de l'apprentissage machine pour trier ces données et les utiliser contre des gens, on peut les utiliser pour s'ingérer dans les affaires de pays étrangers, pour cibler des personnes, pour organiser des cyberattaques, pour intimider, pour influencer et pour compromettre l'avenir.

Ce qui nous préoccupe, en fait, c'est le vaste accès que TikTok permet aux données personnelles et le fait que les lois sur la sécurité nationale de la Chine obligeraient l'entreprise à partager ces données.

M. Parm Bains: Merci beaucoup.

Le président: Merci, monsieur Bains. Je trouvais important que M. Lynd réponde à cette question, et c'est pourquoi vous avez eu beaucoup plus de temps que d'habitude. C'était une réponse importante.

Merci, monsieur Lynd.

[*Français*]

Monsieur Villemure, vous avez la parole pour deux minutes et demie.

M. René Villemure: Deux minutes et demie, ce n'est pas très long.

A-t-on constaté un accroissement des activités du gouvernement chinois en matière d'ingérence, ici au Canada?

[*Traduction*]

M. Daniel Rogers: Il est évident que la Chine continue d'intervenir au Canada. On en a eu une preuve spectaculaire dernièrement, et cela concerne le SCRS. Nous nous inquiétons particulièrement de cette situation dans le contexte de l'utilisation potentielle des médias sociaux pour fournir à la Chine des narratifs susceptibles de constituer de la désinformation ou pour nuire à des intérêts canadiens.

[*Français*]

M. René Villemure: Vous parliez de radicalisation un peu plus tôt. J'ai souvent lu que le but du gouvernement chinois était de créer le chaos par de fausses histoires.

Voyez-vous la recrudescence de certains thèmes, comme la religion, par exemple? Quels thèmes trouve-t-on actuellement?

M. Daniel Rogers: Vous voudrez peut-être ajouter quelque chose à propos des thèmes, monsieur Lynd.

[*Traduction*]

Je pense que la Chine cherche particulièrement à faire valoir des narratifs qui lui soient favorables dans la collectivité. On le constate assez régulièrement. Il ne s'agit pas nécessairement de semer le chaos, mais plutôt de promouvoir un narratif servant ses propres intérêts, en rendant la perspective chinoise séduisante pour les Canadiens, ce qui pourrait être contraire à leurs intérêts, ou en essayant d'influencer la diaspora chinoise ici, au Canada.

Monsieur Lynd, avez-vous quelque chose à ajouter?

M. Paul Lynd: Je rappellerais simplement que le principal objectif de la Chine est de protéger le Parti communiste chinois. Ce qui inquiète le plus le SCRS, c'est l'ingérence étrangère au Canada et le fait que la Chine poursuit des objectifs liés à sa propre politique étrangère au Canada.

Je n'ai pas de détails à portée de la main sur les différents sujets abordés, mais ce qui nous préoccupe vraiment, c'est l'ingérence chinoise au Canada.

[*Français*]

M. René Villemure: Voyez-vous une différence dans l'utilisation de l'anglais, du chinois ou du français, par exemple?

M. Daniel Rogers: C'est une bonne question. Je ne sais pas si les Chinois utilisent plus le français ou l'anglais au Canada. Je sais qu'ils utilisent n'importe quelle technique pour atteindre efficacement la majorité des Canadiens.

[*Traduction*]

Globalement, il y a un écosystème anglophone beaucoup plus important aux États-Unis, par exemple, et cela tend à avoir un effet sur les Canadiens anglophones ou sur les francophones qui consomment des médias en anglais.

[*Français*]

M. René Villemure: Merci beaucoup.

Le président: Merci, monsieur Villemure.

[*Traduction*]

Monsieur Green, vous avez deux minutes et demie. Allez-y, monsieur.

M. Matthew Green: Merci beaucoup.

Peut-être que le directeur pourrait répondre à une question à laquelle TikTok elle-même ne pourrait pas répondre, ou du moins qu'elle n'envisagerait même pas. Selon vous, pourquoi, comme député, ne devrais-je pas être sur TikTok?

M. Daniel Rogers: Excellente question.

Les risques dont j'ai parlé dans l'une de mes réponses s'appliquent particulièrement aux députés, qui peuvent intéresser le gouvernement chinois en raison de leur influence. Si vos données se trouvent sur TikTok et que la Chine les utilise, elle pourrait chercher à en savoir plus sur vous, sur vos réseaux personnels et sur l'écosystème dans lequel vous travaillez, pour orienter l'ingérence étrangère, l'espionnage, les cyberattaques ou d'autres choses dans votre direction.

Comme députés, vous avez évidemment tous un accès particulier au gouvernement et une influence sur lui que la plupart des gens n'ont pas, et je peux imaginer pourquoi vous seriez une cible particulièrement intéressante pour le gouvernement chinois.

● (1805)

M. Matthew Green: En quoi est-ce différent des autres plateformes? On dit que nous vivons dans un capitalisme de surveillance, hors la Chine et son capitalisme d'État. Qui nous dit que les gouvernements chinois, indien, russe, israélien ou américain ne pourraient tout simplement pas acheter cette information directement à Meta, X ou à n'importe quelle autre partie fournissant ces types de plateformes?

M. Daniel Rogers: C'est une autre bonne question.

Je ne dirais évidemment pas que la plateforme TikTok est notre seule préoccupation du point de vue de l'accès des Chinois aux données et de leurs activités d'influence. C'en est une parmi d'autres, mais c'est surtout en raison de la possibilité que sa loi sur la sécurité nationale s'applique directement à une entreprise dont le siège social se trouve en Chine.

L'une des principales différences entre TikTok et les autres, ainsi qu'entre la Chine et d'autres pays, c'est que la Chine s'adonne depuis longtemps à des activités d'ingérence étrangère au Canada. Elle dispose d'un programme cybernétique très sophistiqué et très efficace pour la collecte de renseignement et pour l'espionnage. C'est généralement la principale source de cyberactivité au Canada. Quant à savoir quel gouvernement, la Chine s'est distinguée de plusieurs façons.

M. Matthew Green: Votre évaluation de la menace change-t-elle lorsque les mêmes types d'activités ont pour origine un « allié »?

M. Daniel Rogers: La Loi et le mandat du SCRS ne se limitent pas à un pays. Nous examinons tout ce qui atteint un certain seuil à l'égard de notre sécurité nationale et tout ce qui est contraire aux intérêts du Canada à cet égard. À l'heure actuelle, cela concerne effectivement la République populaire de Chine et non pas nos alliés.

M. Matthew Green: Ne serait-il pas logique de penser que nous sommes plus influencés par les médias américains et l'information américaine que par d'autres sources étrangères?

M. Daniel Rogers: Comme je l'ai dit tout à l'heure, le ciblage de la désinformation par certains acteurs étrangers vers un écosystème américain a des répercussions sur les Canadiens qui consomment également de l'information dans cet écosystème.

M. Matthew Green: Intéressant. Ce n'est pas exactement ce que j'ai demandé, mais c'est une réponse intéressante. Merci beaucoup.

Je sais que mon temps est écoulé, mais j'ajouterai simplement, monsieur le président, que j'ai encore plus de questions à poser qu'il n'y a de réponses à ce sujet. J'aimerais vraiment obtenir d'autres éléments d'information de la part de M. Rogers, même si c'est sur ordre d'une séance à huis clos. Comme membre de l'opposition, j'estime — et je ne dis pas cela dans le cadre d'une question de privilège, mais je vais simplement le dire — que nous n'avons toujours pas toute l'information dont nous aurions besoin pour procéder à une véritable analyse.

Merci beaucoup.

Le président: Merci, monsieur Green.

À ce sujet, je vous laisse le soin, ainsi qu'aux autres membres du Comité, de décider comment vous voulez procéder. La motion adoptée par le Comité visait à traiter cette question comme nous le faisons. On nous a demandé de convoquer certains témoins, et nous faisons tout, par l'entremise de la greffière, pour les faire venir. Je vous laisse décider de la façon dont vous voulez procéder.

Nous essayons toujours de communiquer avec M. Vigneault, l'ancien directeur du SCRS. J'ai aussi invité des représentants de TikTok. La motion n'en parlait pas, mais j'ai estimé qu'ils seraient utiles pour notre étude. Ils ont respectueusement refusé, et je suppose que cela est attribuable aux circonstances de la procédure actuelle au civil.

On me rappelle qu'il y a aussi le ministre. Il nous a fait savoir qu'il serait disponible à la fin de janvier. Je crois que ce sera une réunion intéressante. Nous verrons ce que nous pouvons faire pour que tout le monde soit présent.

Je n'ai pas d'autres questions à aborder. Je vous écoute, madame Shanahan.

Mme Brenda Shanahan: Prévoyez-vous une réunion le 17?

Le président: Je laisse tout ouvert pour l'instant. Je le ferai savoir au Comité. Il m'est très difficile de dire non à ce stade. Je ne sais pas ce qui va se passer. Vous serez informés à l'avance. Je crois que vous avez quelque chose ce soir-là.

● (1810)

Mme Brenda Shanahan: J'ai une fête à organiser.

Des députés: Oh, oh!

Le président: Monsieur Lynd et monsieur Rogers, au nom du Comité, je vous félicite de vos nominations respectives. Je ne peux même pas imaginer le travail qui vous attend. Le Comité s'est intéressé à la question de l'ingérence étrangère et de la désinformation, et je suis assez vieux pour me rappeler qu'on appelait cela du mensonge. Vous avez tout un défi à relever.

Je vous remercie au nom du Comité et des Canadiens. Félicitations encore une fois pour vos nominations. Merci d'être venus nous voir aujourd'hui pour répondre aux questions des membres du Comité.

M. Daniel Rogers: Merci beaucoup. Ce fut un plaisir.

Le président: C'est tout. Je vous souhaite à tous une excellente fin de semaine, et soyez prudents sur la route.

La séance est levée.