CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

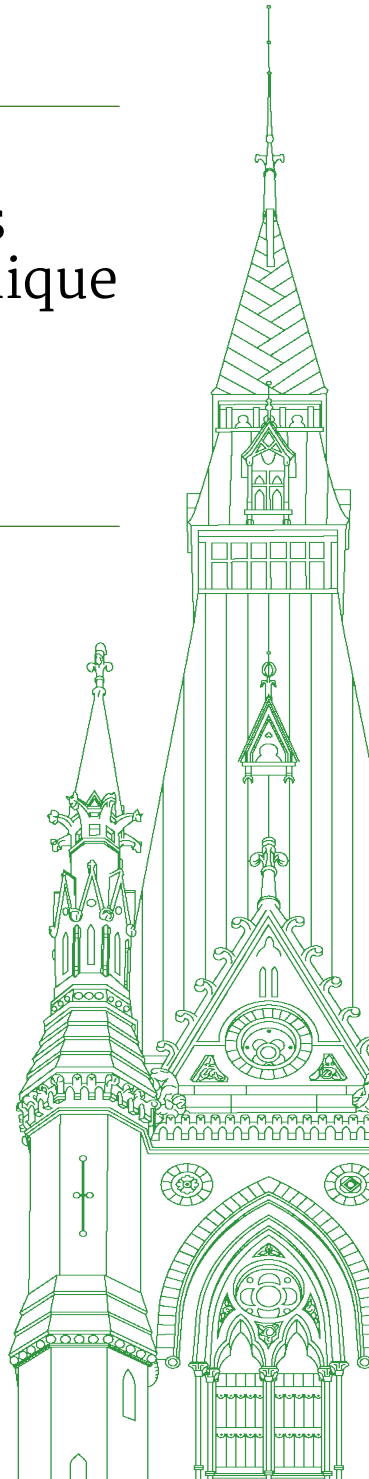
44e LÉGISLATURE, 1re SESSION

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

TÉMOIGNAGES

NUMÉRO 032

Le mardi 9 août 2022



Président : M. Pat Kelly

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

Le mardi 9 août 2022

● (1105)

[*Traduction*]

Le président (M. Pat Kelly (Calgary Rocky Ridge, PCC)): La séance est maintenant ouverte.

Bienvenue à tous à la réunion numéro 32 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 26 juillet 2022, le Comité se réunit pour étudier les outils d'enquête sur appareil utilisés par la Gendarmerie royale du Canada.

La réunion d'aujourd'hui se déroule sous forme hybride, conformément à l'ordre de la Chambre adopté le jeudi 23 juin 2022.

Je viens tout juste de réaliser en lisant l'avis que nous accueillons deux témoins pour la réunion de ce matin. Je vais séparer la réunion en deux parties, pour chaque témoin. Il s'agit des témoins qui étaient prévus dans la motion que nous avons adoptée. Pour la réunion de cet après-midi, nous allons accueillir, dans une partie de la réunion, les trois témoins que nous présentent les partis.

Nous allons commencer par M. Therrien, pour la première heure, puis pour la deuxième heure, nous allons accueillir Mme Polsky.

Sur ce, je souhaite la bienvenue à l'ancien commissaire, M. Therrien, qui n'en est pas à son premier témoignage devant le Comité. Nous avons tenu de nombreuses réunions du Comité avec lui. Je veux donc lui dire que nous sommes heureux de le revoir, et je l'invite à amorcer la première partie de la séance en nous présentant sa déclaration préliminaire.

Monsieur Therrien, vous avez un maximum de cinq minutes.

[*Français*]

M. Daniel Therrien (avocat, à titre personnel): Je vous remercie beaucoup, monsieur le président.

Cela me fait plaisir d'être ici.

Je vous remercie de m'avoir invité à témoigner dans le cadre de votre importante étude, qui fait suite à la publication du 22 juin de la réponse du gouvernement à une question posée par le député Van Popta. Celle-ci portait sur la surveillance d'appareils mobiles.

Dans cette réponse, la Gendarmerie royale du Canada, ou GRC, révélait avoir colligé secrètement, à l'aide d'outils d'enquête sur appareil, des renseignements se trouvant sur le téléphone mobile ou d'autres appareils électroniques de Canadiens, toujours avec une autorisation judiciaire et en vertu du Code criminel.

[*Traduction*]

Je ne connais rien des faits, mis à part ce qui a été rapporté par la GRC en réponse à la question de M. Van Popta. Mes commentaires seront donc surtout axés sur le contenu du droit applicable. Je sais que la GRC a réitéré, hier, qu'elle n'utilise pas d'outils d'enquête sur appareil sans autorisation judiciaire, car cela constituerait une infraction au Code criminel.

Il va sans dire que la collecte secrète par l'État de renseignements personnels ou d'autres informations qui se trouvent dans les appareils numériques des Canadiens est une pratique des plus indiscrètes. Malgré tout, même un tel niveau d'indiscrétion peut être légal et conforme aux principes de protection des renseignements personnels si la collecte de l'information est autorisée par la Loi et pourvu qu'elle soit nécessaire et proportionnelle à l'atteinte des objectifs impérieux de l'État.

La GRC soutient que son utilisation d'outils d'enquête sur appareil dépend toujours d'une autorisation judiciaire, conformément aux dispositions du Code criminel, lesquelles comprennent plusieurs mécanismes de protection des renseignements personnels. Ces outils peuvent seulement être utilisés lorsqu'il s'agit d'un crime grave. Une autorisation judiciaire est exigée, et la norme applicable est souvent élevée: celle des motifs raisonnables de croire qu'un crime a été ou sera commis et que des éléments de preuve concernant ce crime seront trouvés sur l'appareil qui sera fouillé. Les juges peuvent imposer des modalités à la collecte d'informations, y compris des conditions pour limiter l'atteinte à la vie privée.

[*Français*]

Ces dispositions me semblent raisonnables, ou, du moins, elles constituent un bon point de départ pour la protection de la vie privée dans le contexte d'enquêtes criminelles où l'État a des motifs impérieux d'agir et où ses actions sont contrôlées par le pouvoir judiciaire.

Est-ce que ces dispositions sont perfectibles? C'est possible, et le gouvernement y semble ouvert. Pour arriver à la conclusion que des changements législatifs s'imposent, il serait important, selon moi, de savoir comment les dispositions actuelles ont été appliquées et, le cas échéant, y trouver des motifs de préoccupation. Vous avez posé certaines questions à la GRC en ce sens, entre autres sur la teneur des mandats obtenus.

Votre étude porte ultimement sur les conditions préalables afin de donner aux Canadiens la confiance que leurs droits sont protégés lorsque des méthodes intrusives sont utilisées par les forces de l'ordre. L'existence d'un cadre juridique rigoureux et d'une surveillance indépendante est au cœur de cette question de confiance. L'équilibre entre la transparence et la protection des méthodes policières sont aussi en cause. Cela me fera plaisir de parler plus longuement de ces thèmes en répondant à vos questions.

Finalement, la GRC justifie l'utilisation d'outils d'enquête sur appareil et d'autres méthodes intrusives, entre autres pour contrer les difficultés que lui pose le chiffrement des données. Dans la mesure où le recours à ces méthodes reçoit l'autorisation judiciaire, au cas par cas, et que la protection offerte à la population générale par le chiffrement n'est pas autrement compromise, cela me semble acceptable. Je vous renvoie à ce sujet au mémoire publié par le Commissariat à la protection de la vie privée le 5 décembre 2016 lors d'une consultation gouvernementale sur le cadre de sécurité nationale du Canada.

Cela me fera plaisir de tenter de répondre à vos questions.

[*Traduction*]

Le président: Merci, monsieur Therrien.

Avant de donner la parole au premier intervenant, j'ai un peu d'information administrative à partager avec les membres du Comité. Non seulement nous devrons peut-être nous occuper des motions qui pourraient être proposées, mais nous devons aussi donner des instructions à nos analystes. Je propose de le faire à la fin de la deuxième partie de la réunion. Selon le greffier, nous aurons quelques minutes à la fin de la deuxième partie pour régler les points concernant les travaux du Comité, alors c'est ce que j'ai l'intention de faire.

Sur ce, nous commençons le premier tour de questions par M. Bezan.

Vous avez un maximum de six minutes.

● (1110)

M. James Bezan (Selkirk—Interlake—Eastman, PCC): Merci, monsieur le président.

Je veux vous remercier, monsieur Therrien, d'être avec nous aujourd'hui.

Durant quelle période avez-vous été le commissaire à la protection de la vie privée du Canada?

M. Daniel Therrien: J'ai été en fonction de 2014 à 2022.

M. James Bezan: Avez-vous été surpris d'apprendre, lors du témoignage d'hier de la GRC et du ministre Mendicino, qu'on utilisait déjà des outils d'enquête sur appareil pour pirater nos téléphones cellulaires avant que vous ne soyez commissaire à la protection de la vie privée et qu'on ne vous a jamais consulté, pas même une seule fois, ou demandé quelles sont les répercussions sur la protection de la vie privée lorsque ce genre d'outils sont utilisés sur nos appareils?

M. Daniel Therrien: C'est l'outil lui-même qui m'a surpris, à quel point il est indiscret, et le fait qu'il était utilisé depuis si longtemps. Bien sûr, il y a eu de nombreuses discussions au fil des ans — comme la GRC l'a dit hier, cela remonte probablement au début des années 2000 — sur la question de l'accès légal. Autant pendant mon mandat comme commissaire que lorsque j'étais au ministère de la Justice, j'ai suivi ces discussions, et j'y ai aussi participé. Mais l'utilisation de cet outil en particulier pour déjouer le chiffrement, cela a effectivement été une surprise.

M. James Bezan: Si on considère leur, si je peux dire, non-divulgation délibérée de l'utilisation de cette technologie, si vous en aviez été au courant plus tôt, le Commissariat à la protection de la vie privée aurait-il formulé des recommandations sur la façon dont cela aurait dû être utilisé pour protéger le droit à la vie privée des Canadiens et des Canadiennes? Si vous aviez été au fait de la situation, auriez-vous, si je peux dire, dénoncé davantage la GRC pour son utilisation de cette technologie, ou même la Sécurité publique pour ne pas avoir fourni d'outils réglementaires en vue de veiller à ce que le droit à la vie privée des Canadiens et des Canadiennes soit protégé?

M. Daniel Therrien: C'est une question complexe. Je dirais, comme le commissaire Dufresne l'a dit hier, que j'aurais examiné — comme il le fera —, les conditions détaillées dans lesquelles cet outil peut être utilisé pour voir s'il y a des recommandations qui pourraient être formulées quant à son utilisation au-delà des limites du droit; encore une fois, ce serait un bon début.

La partie VI du Code criminel, c'est un bon début. On y énonce les mécanismes de protection de la vie privée. On y prévoit des seuils élevés pour les autorisations judiciaires. Il faut une autorisation judiciaire, alors ce n'est pas comme si la GRC pouvait utiliser cet outil sans que cela soit surveillé par un organisme indépendant. Mais même compte tenu de tous ces bons mécanismes, j'aurais examiné — comme le fera M. Dufresne, si je ne me trompe — la totalité des conditions dans lesquelles cet outil est utilisé, pour voir si d'autres recommandations pourraient être formulées sur la façon dont ils pourraient être utilisés d'une manière qui protège le droit à la vie privée.

M. James Bezan: Comme vous le savez — puisque vous avez énormément d'expérience en ce qui concerne les questions juridiques, le fonctionnement du gouvernement et aussi pour ce qui est de fournir des conseils en lien avec la justice, la protection des droits des personnes et d'autres choses— , il y a différents types de mandats qui sont prévus à la partie VI du Code criminel, selon qu'il s'agit d'un dispositif d'écoute ou de surveillance vidéo. Il y a des mandats de nature générale qui ont une portée plus large. Faudrait-il recommander un nouveau type de mandat pour l'utilisation de la technologie d'enquête sur appareil?

M. Daniel Therrien: Vous avez demandé, hier, si les juges qui reçoivent les demandes d'autorisation judiciaire ont l'expertise technique... Ils ont bien sûr l'expertise juridique, ou ils ont l'expertise technique pour prendre les meilleures décisions, du moins je le crois. J'ai entendu hier, dans le témoignage du gouvernement — du ministre, je crois, mais certainement dans celui de la GRC — que les juges des cours supérieures ont cette expertise, alors il doit y avoir une formation que les juges doivent suivre.

Devrait-il y avoir des types de mandats spéciaux? Je crois que cela dépendrait du fait de savoir si le régime actuel, tel qu'il est appliqué par les juges qui possèdent cette expertise juridique et technique, suffit à protéger la vie privée. C'est peut-être le cas, mais je ne sais pas.

● (1115)

M. James Bezan: Hier, nous discutions de la question au *Feuilleton*. De fait, il a été dit, par rapport à la question au *Feuilleton*, que la GRC vous avait consulté, lorsque vous étiez commissaire à la protection de la vie privée, ou avait consulté le Commissariat à la protection de la vie privée, au sujet de l'utilisation des outils d'enquête sur appareil, mais nous savons maintenant que cela n'est jamais arrivé. Quelle est votre interprétation de la réponse à la question au *Feuilleton*, par rapport au témoignage proprement dit?

M. Daniel Therrien: Le commentaire voulant que nous ayons été consultés concernait très probablement une autre initiative connexe, et pas l'utilisation de cette technologie en particulier.

M. James Bezan: Nous savons qu'il existe des logiciels espions sans clic, comme Pegasus, et maintenant nous découvrons que d'autres entreprises dans le monde...

Le président: Monsieur Bezan, vous avez largement dépassé votre temps.

M. James Bezan: D'accord.

Le président: Terminez rapidement.

M. James Bezan: Merci. Êtes-vous sûr que c'était vraiment six minutes?

Le président: Oui. Vous avez commencé à poser une question à cinq minutes et 55 secondes.

C'est au tour de Mme Hepfner, pour un maximum de six minutes.

Mme Lisa Hepfner (Hamilton Mountain, Lib.): Merci, monsieur le président.

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

Vous avez dit, dans votre déclaration, que selon ce que vous savez, même une technologie aussi indiscrète que les outils d'enquête sur appareil peut être utilisée légalement dans certaines circonstances. Il peut être nécessaire pour les organismes d'application de la loi de pouvoir utiliser des outils aussi indiscrets.

Pourriez-vous nous fournir plus de détails sur le genre de situations où la police pourrait devoir utiliser un tel outil?

M. Daniel Therrien: Je crois que l'important, c'est de trouver un équilibre entre la protection de la vie privée et les autres intérêts publics. Il ne fait aucun doute que cet outil en particulier est extrêmement indiscret, bien plus que les outils d'écoute électronique habituels. Il ne fait pas qu'enregistrer les communications téléphoniques entre une personne A et une personne B. Lorsque c'est installé sur le téléphone, sur l'appareil numérique de la personne, l'État — la police — a accès à tout ce qui se trouve sur le téléphone. C'est extrêmement indiscret.

Pour trouver un équilibre, donc, il doit y avoir des raisons d'intérêt public extrêmement fortes pour justifier que l'État ait accès à ce genre d'information et puisse utiliser ces outils. Un nombre limité d'infractions sont énumérées dans le Code criminel, des infractions graves pour lesquelles la police, munie d'une autorisation judiciaire, est autorisée à utiliser la technologie en question; il s'agit d'infractions comme le meurtre, le terrorisme, le trafic de drogues et d'autres choses du genre.

Je crois que, en général, les infractions énumérées correspondent bien à la définition des « motifs impérieux de l'État ».

Mme Lisa Hepfner: Compte tenu des grandes avancées technologiques et du fait que les organisations criminelles savent très facilement déjouer les techniques habituelles d'écoute électronique, je me demande pourquoi vous étiez surpris d'apprendre que la police s'était aussi dotée de nouvelles capacités d'enquête, adaptées à notre ère numérique.

M. Daniel Therrien: Ce n'est pas le fait que la police avait la technologie pour intercepter des communications dans le contexte de ses enquêtes qui m'a surpris. Dans le passé, ces outils étaient plus ou moins limités. Comme je l'ai dit plus tôt, l'écoute électronique sert à intercepter une communication précise. Ce qui m'a surpris, c'est à quel point cet outil est indiscret, pas le fait que l'État pourrait utiliser cette technologie dans le cadre de ses enquêtes.

Mme Lisa Hepfner: Selon ce que nous a dit la police hier, les communications de nos jours sont chiffrées soit avant qu'elles ne quittent l'appareil, soit quand l'appareil les reçoit. C'est donc une technologie qu'elle peut utiliser pour déjouer le chiffrement.

M. Daniel Therrien: Je l'admets. J'admets que le chiffrement, même s'il peut avoir de nombreux avantages sociétaux pour protéger le droit à la vie privée des Canadiens et des Canadiennes ordinaires par rapport à leurs communications, à leurs transactions commerciales, etc., peut être un obstacle très difficile pour les organismes d'application de la loi. Je l'admets.

Comme je l'ai dit dans ma déclaration, je crois que le fait de posséder une technologie adaptée aux difficultés que pose le chiffrement, moyennant une autorisation judiciaire décidée au cas par cas, n'empêche pas d'autres personnes de bénéficier du chiffrement. Je crois que c'est acceptable.

Je dirais qu'une partie de ce qui m'a surpris, c'est le débat public qui se poursuit sur l'accès légal dans ce cas précis et sur la mesure dans laquelle la police peut utiliser des moyens pour surmonter les obstacles que pose le chiffrement, même s'il n'est jamais ressorti du débat public que les outils d'enquête sur appareil étaient utilisés pour cela.

Je ne dis pas que c'est inacceptable d'utiliser des outils d'enquête sur appareil, mais ce qui m'a surpris, dans les nombreux débats publics sur les difficultés que pose le chiffrement, à l'époque où j'étais commissaire à la protection de la vie privée, c'est qu'on ne m'a jamais dit qu'il existait un outil pour déjouer le chiffrement.

● (1120)

Mme Lisa Hepfner: Y a-t-il quoi que ce soit qui montre ou qui donne à penser que la GRC a utilisé cet outil au-delà de ce qui est autorisé dans le Code criminel? Y a-t-il quoi que ce soit qui donne à penser qu'il y a eu de la surveillance de masse ou quelque chose du genre?

M. Daniel Therrien: Je n'ai rien en ce sens. Je sais que la GRC a dit, hier, qu'il ne s'agit pas simplement de la prendre au mot. On nous a dit, hier, que ce serait un crime si la GRC utilisait cet outil sans autorisation judiciaire, et que ce n'est pas ce qu'elle fait. J'accepte sa réponse.

Mme Lisa Hepfner: Merci beaucoup.

Il ne me reste que très peu de temps, monsieur le président, alors je vais céder la parole.

Le président: La parole va à M. Villemure.

[*Français*]

M. René Villemure (Trois-Rivières, BQ): Je vous remercie, monsieur le président.

Monsieur Therrien, je vous remercie de venir témoigner devant nous une fois de plus.

Nous vous sommes toujours reconnaissants de vos commentaires éclairés.

Hier, le commissaire Dufresne a déclaré avoir été surpris en apprenant les faits. Je crois que vous avez également été surpris, à moins que je ne me trompe.

Notre débat vise à préserver la confiance du public envers les institutions. Je crois que le Bureau du Commissariat à la protection de la vie privée du Canada est l'une des institutions de choix, l'une des institutions privilégiées, pour accomplir cette tâche.

Des représentants de la GRC nous ont dit qu'ils vous avaient consulté. Dans le cas d'autres mandats, nous avons également appris que vous aviez été consulté sans pouvoir regarder sous le capot. Il me semble que la GRC vous consulte sur des sujets banals afin de dire qu'elle vous a consulté, alors qu'elle s'abstient pour d'autres sujets.

Suis-je dans l'erreur en affirmant cela?

M. Daniel Therrien: Je pense que cette question est au cœur de votre étude. C'est peut-être plus compliqué qu'il n'y paraît.

Hier, il a été question de la possibilité de modifier la loi pour faire des évaluations des facteurs relatifs à la vie privée, ou EFVP. Il s'agit d'une obligation juridique, et je pense que c'est une très bonne idée. Présentement, cette obligation relève d'une norme, ou politique, du Conseil du Trésor. Il y a un certain flou pour ce qui est de savoir quand les évaluations en question doivent être faites et à quel moment le commissaire doit être consulté.

Je reviens un peu sur ce que j'ai dit tantôt. Je répète que les conditions préalables à la confiance sont des règles juridiques claires, des normes juridiques élevées et une surveillance indépendante.

La partie VI du Code criminel donne tout cela. Ce n'est pas comme s'il y avait une absence de règles; il y a des règles. Les règles peuvent-elles être bonifiées? Cela est probable.

Hier, il a été question d'une possible bonification qui préciserait que la GRC ou d'autres institutions fédérales doivent consulter le Commissariat à la protection de la vie privée, et cela serait une obligation juridique. C'est une bonne idée, mais, si vous recommandez d'en faire une obligation juridique, je vous encourage à préciser les circonstances dans lesquelles ces évaluations doivent être faites. Selon la norme du Conseil du Trésor, il doit y avoir une évaluation lorsqu'un programme ou une activité, nouvelle ou modifiée de façon considérable, a des répercussions sur la vie privée. La GRC vous a dit, hier, qu'il n'y avait rien de nouveau quant au fait qu'elle utilise cette technologie en particulier. Il ne faut pas se concentrer sur la technologie, il faut se concentrer sur l'atteinte à la vie privée. Selon la GRC, des arguments justificatifs soutiennent cette question. Personnellement, je ne suis pas d'accord sur cela, mais je ne trouve pas qu'il s'agit d'une position déraisonnable.

Je pense que, en plus de dire que le fait de mener une évaluation est une obligation juridique, vous avez la responsabilité de préciser, en termes généraux, le moment où ces évaluations doivent être faites et dans quel but elles doivent l'être. Ainsi, on pourrait s'assurer, de façon proactive, que la loi est respectée. Il n'y aurait pas seulement un examen *ex post facto*, mais aussi un examen préalable pour s'assurer que la loi est respectée. Idéalement, il vous faudrait également reconnaître la vie privée comme un doit fondamental, comme M. Dufresne l'a suggéré hier.

● (1125)

M. René Villemure: Absolument.

De quelle année date la partie VI de la loi?

M. Daniel Therrien: Parlez-vous des dispositions législatives sur la protection de la vie privée?

M. René Villemure: Oui.

M. Daniel Therrien: La législation date des années 1980.

M. René Villemure: Il est donc raisonnable de croire qu'un nouveau regard sur cette législation pourrait être à l'ordre du jour. N'est-ce pas?

M. Daniel Therrien: Oui, c'est le moins que l'on puisse dire.

M. René Villemure: Hier, nous avons beaucoup entendu parler de la partie VI du Code criminel. Vous savez comme moi qu'une situation peut être légale tout en étant non éthique pour de nombreuses raisons. Je crois que le fait d'évoquer seulement la partie VI est incomplet. Il est nécessaire d'être en mesure de scruter la situation de manière impartiale. L'impression que j'avais hier, c'est que j'étais obligé de croire la GRC. Il fallait la croire.

Devons-nous demeurer sur cette position, c'est-à-dire l'obligation de croire la GRC? Si c'est le cas, cela maintient-il ou augmente-t-il la confiance de la population?

M. Daniel Therrien: Je pense que ce n'est pas la même situation que celle liée à l'affaire Clearview AI. Dans cette affaire, sur la question de la reconnaissance faciale, le cadre juridique était très imparfait et presque inexistant. De plus, il n'y avait pas de surveillance par une autorité indépendante.

La partie VI fournit un cadre juridique qui comprend des normes exigeantes et une surveillance indépendante par des tribunaux. Ce régime est-il parfait et impossible à bonifier? La réponse est non. Nous avons un bon point de départ.

M. Daniel Therrien: À cause de ce point de départ, je pense que le public devrait avoir confiance quant au fait que la GRC ne commettra pas un crime en utilisant l'outil sans autorisation judiciaire, comme ses représentants l'ont affirmé hier. Toutefois, il est sans doute possible de bonifier ce cadre juridique de façon proactive, notamment en ce qui touche les évaluations des facteurs relatifs à la vie privée.

M. René Villemure: Il faut continuer.

M. René Villemure: Je vous remercie beaucoup.

[*Traduction*]

Le président: Merci.

C'est maintenant au tour de M. Green.

Vous avez un maximum de six minutes.

M. Matthew Green (Hamilton-Centre, NPD): Merci.

J'aimerais poursuivre et entrer dans ce qui est, pour moi, le vif du sujet, c'est-à-dire le renforcement des cadres juridiques.

Nous avons entendu le commissaire à la protection de la vie privée, plus tôt, dans son témoignage dire que des évaluations des facteurs relatifs à la vie privée devraient faire partie du processus. Selon le sous-commissaire, du moins, d'après les documents que nous avons reçus, il y aurait un processus pour l'intégration des nouvelles technologies.

Compte tenu de votre expérience dans ce domaine et puisqu'une grande partie de notre travail, en tant que comité de l'éthique, consiste à suivre les situations après coup d'une façon très réactive, quels seraient les éléments d'un cadre juridique que vous recommanderiez au Comité pour aider à combler l'écart qui existe manifestement entre ce qui est légalement, éthiquement et technologiquement faisable, compte tenu du rythme auquel la technologie avance par rapport aux lois existantes?

M. Daniel Therrien: Si on pouvait commencer en proposant un amendement potentiel qui ferait que ce soit une exigence juridique, au lieu que cela fasse simplement partie des politiques des ministères et des institutions, y compris la GRC, de réaliser des évaluations des facteurs relatifs à la vie privée, ce serait un bon début.

À ce sujet — et le commissaire Dufresne a aussi parlé du rôle du Commissariat à cet égard —, je viens de laisser entendre à M. Villemure que vous voudriez peut-être formuler des recommandations, pas seulement pour établir une exigence juridique, mais aussi pour définir d'une certaine façon les objectifs visés par les EFVP. Je vous encouragerais à examiner le rôle du CPVP et le rôle des tribunaux.

Je ne crois pas que le CPVP devrait remplir le même rôle que jouent les tribunaux en vertu de la partie VI du Code criminel. Je crois que la valeur que le CPVP ajoute aux tribunaux est qu'il peut examiner de façon proactive, au niveau des programmes au lieu du niveau de chaque cas individuellement, les conditions dans lesquelles l'outil peut être utilisé et formuler des recommandations en ce sens.

● (1130)

M. Matthew Green: Je crois que je suis d'accord.

Il a aussi été question, vu que la Loi sur la protection des renseignements personnels s'en vient, de la distinction entre ce qui est formulé dans le préambule en comparaison du cadre juridique proprement dit, pour ce qui est de créer les garde-fous.

D'après votre expérience, autant au ministère de la Justice qu'au CPVP, quelles seraient vos recommandations pour la prochaine Loi sur la protection des renseignements personnels, afin qu'il y ait un cadre juridique qui non seulement s'appliquerait aux organismes d'application de la loi, mais aussi qui protégerait de façon plus générale les citoyens ici au Canada contre ce genre d'utilisation?

M. Daniel Therrien: Je crois qu'un préambule serait une bonne idée.

Vous avez dit, hier, que vous voudriez qu'il y ait des normes juridiques claires, comme l'exigence de réaliser une EFVP, et je suis d'accord, mais un préambule aide à définir pour tout le monde, y compris les organisations du gouvernement, notre approche en matière de protection de la vie privée, quand on fait une évaluation des facteurs relatifs à la vie privée. Si le préambule énonce que la protection de la vie privée est un droit fondamental essentiel pour protéger la dignité des personnes, alors quand la GRC, le ministère de la Santé ou n'importe quelle autre organisation va effectuer une EFVP, les gens vont garder ce message important en tête. Ce n'est pas simplement un exercice où il faut cocher une case...

M. Matthew Green: Il a aussi été conclu que cela n'était pas juridiquement contraignant. Comment pourrions-nous faire en sorte que la consécration des droits soit juridiquement contraignante, en tant que droits fondamentaux dans le cadre juridique de la Loi sur la protection des renseignements personnels?

M. Daniel Therrien: Le préambule peut toujours être utilisé comme outil d'interprétation. C'est important d'avoir une norme juridique claire. L'EFVP est obligatoire... c'est une norme juridique claire, mais un préambule, même s'il n'a pas force exécutoire en soi, est un outil très précieux pour l'interprétation, et il donne vie à la norme juridique en question.

M. Matthew Green: Je vais passer à un autre sujet maintenant. Nous avons parlé de directives stratégiques et, espérons-le, des recommandations pour la Loi, et nous sommes passés à ce que je crois être une lacune actuellement dans la surveillance; mes collègues en ont parlé: le fait que c'est la police qui surveille la police.

Dans le spécimen de mandat que vous avez fourni, il y avait une section sur les interceptions au moyen d'outils d'enquête sur appareil, et il était question des communications de vive voix interceptées au moyen d'un tel outil. La personne chargée de la surveillance qui examine ensuite la communication « doit cesser de l'examiner dès qu'il détermine qu'aucune personne visée au paragraphe 3a n'est partie à la communication ».

Essentiellement, cela donne une situation où l'outil est installé sur un appareil, l'appareil est surveillé, et nous sommes censés faire confiance à la GRC aveuglément, même si, comme l'a décrit la GRC, il n'y a aucun processus en place pour des audits ou une évaluation du rendement par rapport à cela. Ce qui me préoccupe, c'est que, si on laisse cela ainsi, sans qu'il y ait explicitement des garde-fous quant au moment et à la façon dont l'outil peut être utilisé, la façon dont les données sont recueillies de façon globale fait que cela est susceptible d'entraîner des perquisitions ou des saisies illégales de personnes et de documents qui ne sont pas visés par le mandat.

Avez-vous des commentaires à faire à ce sujet et sur des façons dont nous pourrions mettre en place une surveillance?

M. Daniel Therrien: Peut-être que ma réponse va vous surprendre un peu.

Je ne crois pas que la GRC est une organisation rebelle. Actuellement, comme elle l'affirme — et je la crois —, elle utilise les outils d'enquête sur appareil seulement avec une autorisation judiciaire, et les autorisations judiciaires s'assortissent de conditions. Ma prémisse de base n'est pas que la GRC veut manquer à ces conditions. De fait, cela pourrait être un crime de ne pas respecter les conditions en question, parce que l'utilisation de cet outil est seulement légale si les conditions imposées par la cour sont respectées.

Cela dit, ce serait peut-être une bonne idée d'avoir des processus d'audit pour s'assurer que l'agent de police qui effectue la tâche en question le fait en respectant les exigences de la cour.

● (1135)

Le président: Je dois hélas vous interrompre, parce que nous avons largement dépassé le temps imparti avec cette réponse. Si vous n'avez pas terminé ce que vous aviez à dire, peut-être que vous pourriez l'intégrer dans une autre réponse.

M. Daniel Therrien: Non, j'avais terminé.

Le président: C'est maintenant au tour de M. Williams, pour un maximum de cinq minutes.

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

Monsieur Therrien, merci beaucoup d'être avec nous aujourd'hui.

Vous avez été commissaire à la protection de la vie privée pendant huit ans, est-ce exact?

M. Daniel Therrien: Oui, effectivement.

M. Ryan Williams: Dans vos mots, pourquoi est-ce que le Commissariat à la protection de la vie privée est une partie importante du gouvernement canadien?

M. Daniel Therrien: Le CPVP joue un certain nombre de rôles, dont celui d'enquêter sur les plaintes et d'agir, comme je l'ai dit il y a quelques minutes, à titre d'organisme de surveillance indépendant pour le gouvernement. Le gouvernement doit obéir aux lois. Il est aidé par le ministère de la Justice, qui a comme devoir de veiller à ce que le gouvernement agisse dans le respect de la Loi, mais tous ces processus sont concentrés dans l'appareil exécutif.

L'un des rôles du CPVP est de s'assurer de la confiance du public en portant un regard indépendant, qui va au-delà des mécanismes de l'appareil exécutif, pour veiller à ce que les lois, et en particulier les lois en matière de protection de la vie privée, sont effectivement respectées. Il doit aussi jouer un rôle proactif.

M. Ryan Williams: Voilà où je veux en venir, comme je crois que vous l'avez mentionné, c'est que c'est une question de confiance.

M. Daniel Therrien: Oui.

M. Ryan Williams: Il faut donner confiance aux Canadiens pour qu'ils soient convaincus que, quand le gouvernement et ses organisations agissent d'une façon ou d'une autre, de nombreuses façons, ils peuvent avoir foi en ces organisations. Est-ce exact?

M. Daniel Therrien: Oui.

M. Ryan Williams: Hier, je crois que vous l'avez entendu également, la GRC et le ministre ont dit que les juges délivraient seulement des mandats lorsque c'est nécessaire, que cette technologie est sécuritaire et que nous pouvons leur faire confiance. Ils ont déclaré que, à leur avis, il n'était pas nécessaire pour eux de faire des EFVP, des évaluations des facteurs relatifs à la vie privée, et c'est ce que nous avons constaté.

À votre avis, dans quelle mesure cela est-il vrai? Pouvons-nous faire intrinsèquement confiance au gouvernement? Pourrions-nous simplement nous débarrasser du Commissariat à la protection de la vie privée? Dans quelle mesure est-ce que ce qu'ils ont dit est vrai?

M. Daniel Therrien: Respectueusement, je ne pense pas que ce soit un exemple de « faites-nous confiance », quand on dit que les cours donnent seulement les autorisations après examen et que c'est donc légal. Vous dites, « faites-nous confiance ». La confiance dépend de deux choses: un cadre juridique clair et rigoureux et une surveillance indépendante. Les cours fournissent cette surveillance indépendante.

Nous avons un bon point de départ avec la partie VI du Code criminel. Est-ce qu'on peut l'améliorer? Probablement.

Le CPVP a certainement une expertise particulière qu'il peut mobiliser, et réaliser des évaluations des facteurs relatifs à la vie privée est très probablement une bonne idée, dans les circonstances. Il y a aussi l'Office de surveillance des activités en matière de sécurité nationale et de renseignement, l'OSSNR, qui joue un rôle et qui est aussi un organisme de surveillance indépendant.

Il y a au moins trois organisations en tout qui fournissent un certain niveau de confiance: les cours, le CPVP et l'OSSNR, qui sont indépendants de l'organe exécutif.

Votre étude vise à établir, compte tenu du caractère indiscret de cette technologie, si les mécanismes de protection pourraient être améliorés. Il se pourrait bien que la réponse soit oui.

M. Ryan Williams: À propos de ce rôle... la GRC a dit hier que cette technologie était parfois utilisée dans le cadre d'enquêtes en cours.

Pouvez-vous expliquer, puisque vous avez occupé ce poste pendant si longtemps, comment une EFVP protège la technologie qui pourrait être utilisée pour permettre au gouvernement de l'utiliser de cette façon, quand vous menez une enquête ou faites une EFVP? Comment protégez-vous cette technologie qui est utilisée dans le cadre d'enquêtes en cours? Quelles mesures recommanderiez-vous de mettre en œuvre pour cela?

● (1140)

M. Daniel Therrien: Je pense qu'il y a de nombreux acteurs, et que chacun devrait jouer un rôle sans qu'il y ait double emploi avec les rôles des autres. Les cours ont un rôle important, mais elles sont liées par les dispositions de la partie VI du Code criminel. Le Commissariat à la protection de la vie privée examine de façon plus générale la protection de la vie privée en vertu de sa loi; il peut donc fournir une assurance supplémentaire au public que la vie privée, au-delà de ce qui est prévu dans le Code criminel, sera respectée quand ces outils seront utilisés.

Chacun de ces mécanismes apporte un certain niveau de confiance. Pour exprimer les choses différemment, le fait que la partie VI existe ne veut pas dire que le CPVP n'a aucun rôle à jouer. Il a effectivement un rôle à jouer.

Le président: Merci.

Maintenant, pour un maximum de cinq minutes, c'est à M. Hardie.

M. Ken Hardie (Fleetwood—Port Kells, Lib.): Merci beaucoup, monsieur le président.

Monsieur Therrien, c'est vraiment un sujet fascinant. J'ai le plaisir de remplacer mon collègue, Greg Fergus, aujourd'hui.

Il faut une autorisation judiciaire. Est-ce que c'est exigé pour plus que les incidents et l'utilisation de la technologie dont nous discutons aujourd'hui? Est-ce qu'il y a d'autres domaines d'enquête où des autorisations judiciaires sont exigées?

M. Daniel Therrien: De façon générale, en vertu du Code criminel, si l'utilisation de techniques d'enquête entraîne une atteinte à la vie privée — un moyen traditionnel serait l'écoute électronique —, alors une autorisation judiciaire est exigée. Les fouilles, évidemment, parce qu'elles constituent une atteinte à la vie privée, exigent une autorisation judiciaire. Il y a un certain nombre d'atteintes à la vie privée qui exigent une autorisation judiciaire.

M. Ken Hardie: Êtes-vous avisé quand des autorisations judiciaires sont délivrées? Est-ce qu'on vous avertit à l'avance de ce genre d'activité?

M. Daniel Therrien: Non, parce que les cours assurent une surveillance indépendante, et ce mécanisme fonctionne indépendamment.

M. Ken Hardie: Croyez-vous que les évaluations des facteurs relatifs à la vie privée que font les cours avant de délivrer ces autorisations sont raisonnablement alignées sur les conditions que vous surveillez?

M. Daniel Therrien: Je suis convaincu que les cours appliquent la Loi correctement. S'il y a une erreur, il existe des mécanismes d'appel pour veiller à ce que la Loi soit appliquée correctement. Cela nous ramène à la partie VI du Code criminel, qui énonce les normes pour les cours, précisant une certaine définition de la vie privée, alors que la Loi sur la protection des renseignements personnels a une définition plus large de la vie privée. Le fait que je sois convaincu que les cours font leur travail correctement ne veut pas dire que le CPVP, qui applique une définition légèrement différente, n'a pas aussi son propre rôle.

M. Ken Hardie: Malgré la confiance que vous éprouvez envers les cours, y a-t-il un mécanisme d'audit auquel vous participez pour examiner les autorisations que les tribunaux ont délivrées afin de voir si tout est effectivement parfaitement synchronisé?

M. Daniel Therrien: Ma réponse à votre question serait que le rôle du CPVP consiste à examiner comment le processus d'autorisation fonctionne dans les cas spécifiques, non pas pour passer en revue ce que les cours ont fait — ce ne serait pas approprié —, mais plutôt afin d'établir si les lois sont suffisantes pour protéger le droit à la vie privée des Canadiens.

M. Ken Hardie: Nous avons surtout parlé des activités de la GRC. Existe-t-il des dispositions similaires pour le SCRS?

M. Daniel Therrien: Il y a des dispositions différentes pour le SCRS et pour le CST, le Centre de la sécurité des télécommunications, en ce qui concerne l'interception des communications. Est-ce que ces organisations utilisent une technologie similaire aux outils d'enquête sur appareil? Je ne sais pas, c'est bien possible, mais il y a certainement des lois qui régissent l'utilisation de la technologie par le SCRS et le CST pour intercepter des communications.

● (1145)

M. Ken Hardie: Dans le cas de Jeffrey Delisle, l'officier de la Marine qui a fini par être condamné pour espionnage, nous avons reçu énormément d'information par l'intermédiaire du FBI. Je ne sais pas si nous pouvons être certains que le FBI suit les mêmes règles que nous par rapport à l'utilisation de cette technologie. Peut-être que si, mais est-ce qu'il pourrait y avoir des problèmes, surtout devant les cours, par rapport à l'admissibilité de l'information recueillie, puis transmise par une autre organisation de sécurité à l'extérieur du Canada?

M. Daniel Therrien: C'est difficile à répondre à cette question dans l'abstrait.

Je crois que M. Delisle a été condamné, ce qui veut donc dire que la cour compétente était certainement convaincue de la recevabilité des éléments de preuve à charge. Encore une fois, il y a une surveillance judiciaire importante. Je vais m'arrêter là.

M. Ken Hardie: Si vous étiez en possession de plus d'informations à propos de ce qui se passe quand les autorisations judiciaires sont délivrées et de ce qui se fait réellement — les motifs, etc. —, surtout dans le cadre d'une enquête en cours, est-ce que cela vous compromettrait, par rapport à vos obligations envers le Parlement de faire rapport et surtout de rendre des comptes en ce qui concerne l'application de la loi?

Le président: Je suis vraiment désolé, mais j'ai été lent sur la détente.

Monsieur Hardie, vous avez commencé à poser votre question alors que votre temps était déjà écoulé.

Monsieur Therrien, je ne sais pas si vous pouvez répondre rapidement, sinon, comme je l'ai dit plus tôt, nous allons devoir y revenir.

M. Daniel Therrien: Je ne pense pas que ce soit le rôle du CPVP de remettre en question les décisions des cours par rapport à des cas spécifiques, en particulier s'il s'agit d'enquêtes en cours. Encore une fois, le CPVP devrait examiner les choses au niveau des programmes, pas au niveau des cas individuellement, et certainement pas pendant qu'une enquête est en cours.

Le président: Merci.

La parole va maintenant à M. Villemure pour deux minutes et demie.

[*Français*]

M. René Villemure: Je vous remercie, monsieur le président.

Je profiterai des deux minutes et demie qui me sont imparties pour poser deux questions et tenter de faire le tour du sujet.

Hier, un officier de la GRC a soulevé une question que nous n'avons pas eu le temps de creuser tout à fait. Elle portait sur la surveillance potentielle de citoyens canadiens par des puissances ou des entreprises étrangères. À titre de commissaire à la protection de la vie privée, à l'époque, étiez-vous au courant de ces pratiques?

M. Daniel Therrien: Je n'avais pas de preuves, mais disons que j'avais certains doutes.

M. René Villemure: Vous aviez un doute raisonnable.

Est-ce cela?

M. Daniel Therrien: Oui, j'avais un doute raisonnable.

M. René Villemure: Actuellement, y a-t-il une disposition qui empêcherait une puissance étrangère de surveiller des Canadiens?

M. Daniel Therrien: Il s'agit ici de sécurité nationale et de mesures prises par les agences de sécurité nationale pour empêcher la violation du droit canadien. C'est à cet égard que cela se passe.

M. René Villemure: On a dit que les technologies étaient intrusives. Selon un représentant de la GRC, il y a toujours eu de l'intrusion dans la vie privée, mais l'outil a changé.

Ne recueille-t-on pas trop de renseignements?

Cette information, est-elle conservée de manière sécuritaire afin de s'assurer qu'une fuite de données comme celle qui est survenue chez Desjardins ne peut pas arriver? Il s'agit de beaucoup de renseignements.

M. Daniel Therrien: Il est vrai qu'il y a toujours eu des méthodes de collecte d'information et d'interception de communications. Cependant, avec cet outil, nous sommes dans un autre monde en ce qui a trait au caractère intrusif de la collecte de renseignements en question.

Ce que la GRC dit est peut-être justifiable, mais je ne suis pas d'accord que l'utilisation de cet outil n'aurait pas dû donner lieu à l'évaluation des facteurs relatifs à la vie privée, étant donné son caractère extrêmement intrusif. Il aurait dû y avoir une consultation auprès du Commissariat.

M. René Villemure: Je vous remercie.

M. Daniel Therrien: Ai-je bien répondu à votre question?

M. René Villemure: Oui, vous y avez bien répondu.

Nous n'avons pas entendu parler hier d'outils moins intrusifs qui pourraient permettre d'atteindre la même fin.

Avez-vous une opinion à ce sujet?

M. Daniel Therrien: Encore une fois, il est question du rôle du Commissariat à la protection de la vie privée et des tribunaux. Suivant l'un des critères énoncés dans la partie VI du Code criminel, la cour doit être convaincue qu'il n'y a pas d'autres moyens pour arriver à la fin désirée, soit de colliger la preuve. Sur le plan des programmes, le Commissariat peut avoir un rôle à jouer, mais il y a déjà des dispositions qui obligent les tribunaux à se pencher sur cette question.

M. René Villemure: Puis-je avoir cinq secondes de plus, monsieur le président?

[*Traduction*]

Le président: Non, vous avez dépassé votre temps. Je suis désolé.

● (1150)

[*Français*]

M. René Villemure: Je vous remercie beaucoup.

[*Traduction*]

Le président: La parole va à M. Green, pour deux minutes et demie.

M. Matthew Green: Merci.

Compte tenu des commentaires sur la nature indiscrète de la technologie et du fait qu'elle soit répandue, croyez-vous que l'utilisation de cette technologie par les organismes d'application de la loi pourrait potentiellement, violer les droits et libertés d'autrui prévus par la Charte?

M. Daniel Therrien: Oui.

M. Matthew Green: Connaissez-vous quelques-uns des travaux qui ont été faits en Europe, par rapport à l'enquête sur Pegasus et le groupe NSO? Plus particulièrement, en 2018, le Conseil de l'Europe a adopté un protocole modifiant la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Essentiellement, les principes appuient les droits garantis par la Convention européenne des droits de l'homme et établissent de nouveaux principes intrinsèquement, y compris le concept de la protection de la vie privée dès la conception.

Selon vous, le principe de la protection de la vie privée dès la conception devrait-il être une norme de pratique pour toutes les nouvelles technologies que les organismes d'application de la loi voudraient utiliser?

M. Daniel Therrien: Assurément.

M. Matthew Green: Pourriez-vous prendre quelques instants afin de définir, pour les gens qui ne savent peut-être pas ce qu'est la protection de la vie privée dès la conception, comment cela pourrait être appliqué en contexte?

M. Daniel Therrien: J'ai mentionné plus d'une fois, au cours des dernières minutes, la surveillance judiciaire. La surveillance judiciaire, c'est-à-dire la surveillance *ex post facto*, que ce soit par les cours ou par le CPVP, est nécessaire, mais c'est beaucoup mieux que la prise en compte de la protection de la vie privée soit intégrée aux processus qui mènent à l'utilisation d'une technologie particulièrement indiscrète. L'avantage de la protection de la vie privée dès la conception ou des évaluations des facteurs relatifs à la vie privée est essentiellement que cela permet de veiller à ce que la population soit assurée que les violations ne seront pas seulement découvertes après coup, mais que le nombre de violations sera grandement réduit, parce que les bons processus sont en place.

M. Matthew Green: Seriez-vous d'accord pour dire que cela englobe aussi les principes de la transparence et de la reddition de comptes?

M. Daniel Therrien: Oui.

M. Matthew Green: Nous savons, en vérité, que dans le passé, la GRC, en particulier lorsqu'elle utilisait la technologie Stingray, une technologie utilisant l'identité internationale d'abonnement mobile pour la surveillance de masse, n'était pas particulièrement communicative à propos de son utilisation. De fait, cela a eu pour conséquence que certaines affaires ont été rejetées par les tribunaux. J'aimerais seulement prendre un moment pour souligner le fait que ces principes — nous avons parlé de la comparaison entre ce qu'il y a dans le préambule et les cadres juridiques — de la transparence, de la reddition de comptes et de la protection de la vie privée dès la conception devraient être intégrés dans tous les processus des organismes d'application de la loi.

M. Daniel Therrien: Oui, et je...

Le président: Merci.

Je ne pense pas que c'était une question. Quoi qu'il en soit, il ne reste pas suffisamment de temps pour une réponse.

M. Matthew Green: S'il est d'accord, alors ce sera inscrit au compte rendu et fera partie du hansard du Comité.

Le président: D'accord, il peut signifier son accord.

M. Daniel Therrien: Je suis d'accord, mais encore une fois, je vous encourage à ne pas donner de définitions trop prescriptives pour ces concepts, mais de privilégier plutôt des définitions générales.

Le président: Merci.

La parole va maintenant à M. Kurek, puis les dernières questions pour ce témoin seront posées par Mme Khalid, qui aura cinq minutes.

Allez-y, monsieur Kurek.

M. Damien Kurek (Battle River—Crowfoot, PCC): Merci beaucoup, monsieur le président.

Monsieur Therrien, nous sommes heureux de vous accueillir à nouveau au comité de l'éthique.

Mon but sera d'obtenir un peu plus de détails dans le cadre de cette discussion qui a été très intéressante. En particulier, il y a les réponses que le ministre a fournies hier. Il a refusé de divulguer si... D'une façon détournée, il a bel et bien reconnu que quand d'autres organisations utilisent effectivement des outils d'enquête sur appareil... D'une certaine façon, il a indirectement reconnu que ce type de technologie était utilisé par d'autres organisations qui relèvent du ministre de la Sécurité publique.

Je ne sais pas si vous avez eu l'occasion d'écouter son témoignage d'hier, mais êtes-vous préoccupé par le manque de franchise de la part du ministre, lorsqu'il a témoigné devant le Comité hier?

M. Daniel Therrien: Je vous encouragerais à nouveau à clarifier la Loi. Si vous voulez plus de transparence, faites-en une exigence juridique, en plus d'en définir le concept. En ce qui concerne la GRC, par exemple, son principe de base, et peut-être aussi celui du ministre, quand il a répondu hier, est d'essayer d'être transparent, mais de protéger ses méthodes d'opération, afin que les criminels ne puissent pas savoir comment la GRC fonctionne parce que cela nuirait bien sûr aux enquêtes. Quand la police et les fonctionnaires du gouvernement répondent à ce genre de questions, ils ont toujours en tête la nécessité de protéger les méthodes d'opération.

Hier, j'ai entendu quelque chose qui m'a fait penser à une norme, que vous devriez peut-être prendre en considération. Ce serait que le gouvernement et la police aient l'obligation d'être transparents, excluant seulement ce qui est nécessaire pour protéger les méthodes de la police et l'intégrité des enquêtes. En d'autres mots, la norme serait la transparence.

L'exception s'appliquerait uniquement à ce qui est nécessaire. Peut-être que si cela était plus clair... non, pas peut-être. C'est clair, pour moi, parce qu'à de nombreuses occasions... et ce que je dis ne s'applique pas au ministre; je parle des discussions que j'ai eues au cours des années avec les organismes d'application de la loi et de la sécurité nationale, parce que leur principe de base n'est pas de divulguer les choses qui pourraient nuire à leurs enquêtes. Parfois, elles sont excessivement prudentes pour ce qui est de trouver l'équilibre entre la transparence et la protection de leurs méthodes.

Si la Loi était plus claire quant au fait que la transparence est la règle, et qu'il est seulement acceptable de ne pas être transparent quand cela est nécessaire pour protéger les méthodes de la police, alors peut-être que les choses progresseraient.

● (1155)

M. Damien Kurek: J'ai posé une question à votre successeur, hier, et je crois que cela pourrait nous être utile d'entendre votre réponse également.

À l'époque où vous étiez commissaire, quand on consultait le Commissariat à la protection de la vie privée et que des questions sur l'intégrité des opérations ou l'état des enquêtes étaient soulevées dans les discussions pour savoir si la vie privée des Canadiens allait être protégée, est-ce que le Commissariat à la protection de la vie privée prenait des mesures pour s'assurer que ces choses soient protégées?

M. Daniel Therrien: Le CPVP a des employés qui ont une cote de sécurité. Cela a été clairement expliqué aux organisations de la sécurité nationale et de l'application de loi, et elles le comprennent. Oui, on prenait de telles mesures.

M. Damien Kurek: Merci.

Dans ce cas...

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

M. Damien Kurek: D'accord.

Le président: C'est maintenant au tour de Mme Khalid, pour les cinq prochaines minutes.

Mme Iqra Khalid (Mississauga—Erin Mills, Lib.): Merci beaucoup, monsieur le président, et par votre intermédiaire, je remercie M. Therrien de sa présence ici aujourd'hui.

Je vais poursuivre sur le même sujet que mon collègue, M. Kurek, a abordé au début. Cela concerne le rôle de surveillance des ministres et la mesure dans laquelle ils ont un mot à dire.

Hier, nous avons entendu les témoignages selon lesquels l'utilisation de cette technologie remonte à 2012. Cela veut dire que soit Vic Toews, soit Steven Blaney, était le ministre à l'époque. Selon vous, la GRC a-t-elle consulté soit le ministre Toews, soit le ministre Blaney, avant de commencer à utiliser cette technologie?

M. Daniel Therrien: Avant de commencer à utiliser les outils d'enquête sur appareil?

Mme Iqra Khalid: Oui.

M. Daniel Therrien: Je ne sais pas. J'ai entendu le ministre Mendicino dire que ce serait une question opérationnelle, et non une question de politique ou législative. Peut-être bien que la GRC a décidé de commencer à utiliser cet outil pour des raisons opérationnelles, sans en informer le ministre de l'époque ou demander son autorisation. Je ne sais pas.

Mme Iqra Khalid: Merci.

Vous étiez le précédent commissaire à la vie privée du Canada; la GRC vous a-t-elle jamais consulté avant de commencer à utiliser cette technologie, à la demande de certains ministres, comme le ministre Toews ou le ministre Blaney? L'un ou l'autre de ces ministres a-t-il demandé ou approuvé une EFVP, une évaluation des facteurs relatifs à la vie privée? Avez-vous jamais reçu une telle EFVP à cette époque?

M. Daniel Therrien: Ni moi ni le CPVP ne savions que la police utilisait cet outil, alors non, nous n'avons jamais été consultés à ce sujet dans le passé.

Mme Iqra Khalid: Saviez-vous si la GRC utilisait n'importe quel autre logiciel développé par le groupe Awz, qui avait des liens étroits avec l'ancien premier ministre Harper. Par exemple, Corsight, leur logiciel de reconnaissance faciale, ou viisights, leur logiciel de reconnaissance comportementale?

● (1200)

M. Daniel Therrien: Je ne sais rien à ce sujet.

Mme Iqra Khalid: Nous venons d'ouvrir une nouvelle porte ici aux complotistes chez eux qui écoutent cela et qui commencent à croire que la GRC fait de la surveillance de masse. Selon vous, est-ce vrai? Est-ce que la GRC fait une surveillance de masse qui vise les Canadiens?

M. Daniel Therrien: Je ne crois pas. La GRC a dit qu'elle utilisait seulement les outils d'enquête sur appareil avec une autorisation judiciaire. C'est ce que je crois. En ce qui concerne le déroulement de notre enquête sur la reconnaissance faciale, est-ce que la GRC utilise la surveillance de masse? Probablement pas, mais elle utilise certainement certains outils indiscrets sans qu'il y ait nécessairement des mesures de protection juridiques claires ou une surveillance indépendante.

La surveillance de masse peut prendre de nombreuses formes, mais apparemment pas celle d'outils d'enquête sur appareil... probablement pas, mais je ne sais pas.

Mme Iqra Khalid: Nous avons eu des conversations avec d'autres membres qui spéculent sur le rôle des préambules et leur intégration dans la législation. À votre avis, dans quelle mesure est-il important de préserver le pouvoir discrétionnaire des agents de la GRC dans le cadre de leur travail de sécurité et de protection des Canadiens? Où se trouve l'équilibre entre la protection de la vie privée et la surveillance, qui est très importante?

Croyez-vous que la création de règles et de règlements rigides concernant la vie privée, qui, dans les 32 cas dont nous parlons, n'a fait que porter atteinte à la vie privée de ceux qui faisaient l'objet d'une enquête pour des infractions très graves comme le terrorisme, le meurtre, le trafic...? Pensez-vous que les tribunaux et les agents de la GRC devraient disposer d'un pouvoir discrétionnaire dans le cadre de leur rôle? Où se situe cet équilibre?

M. Daniel Therrien: Vous avez commencé votre question en faisant référence aux préambules, puis êtes passée à la question de savoir s'il devrait y avoir des règles normatives. Ma réponse, c'est que, bien sûr, les fonctionnaires, y compris la police, ont en fin de compte un rôle à jouer dans le cadre de la Loi. La Loi ne devrait pas être trop normative, mais en même temps, je pense que c'est votre rôle en tant que parlementaires de fournir une bonne orientation — peut-être pas une orientation trop normative, mais une bonne orientation de fond — aux fonctionnaires sur la façon d'exercer leurs responsabilités.

Je ne pense pas que le fait d'inclure dans le préambule de la Loi sur la protection des renseignements personnels l'idée que la vie privée est un droit fondamental soit normatif, et je pense que ce serait une bonne orientation générale à donner à la GRC.

Le président: Merci.

Mme Iqra Khalid: Monsieur le président, si vous le permettez, je me demande s'il serait possible que M. Therrien reste un peu plus longtemps pour la deuxième heure également. Je sais que mes collègues ont aussi des questions à poser.

Le président: Eh bien, j'avais prévu de diviser la séance en deux groupes avec les deux personnes, mais je ne...

Je pense que c'est à M. Therrien de décider s'il souhaite rester.

M. Daniel Therrien: Je suis heureux de rester.

Le président: Ce n'est pas ainsi que j'avais prévu de procéder, mais d'accord.

Mme Iqra Khalid: Merci beaucoup. Je vous en suis reconnaissante.

Le président: M. Green invoque le Règlement.

M. Matthew Green: Je veux simplement m'assurer que nous comprenons bien que la prolongation accordée à M. Therrien permet toujours de remettre le chronomètre à zéro. Nous ne les combinons pas. Nous avons deux séances distinctes.

Le président: Oui. J'avais prévu de faire en sorte que ces deux témoins distincts de notre motion constituent chacun leur propre groupe à cette fin. M. Therrien est le bienvenu, et les membres peuvent lui poser des questions, mais je crois savoir que Mme Polsky a déjà commencé et qu'elle s'est soumise à un test audio. Nous allons y aller directement sans...

M. Villemure a un rappel au Règlement.

[*Français*]

M. René Villemure: Monsieur le président, je veux simplement m'assurer que nous pourrons entendre suffisamment Mme Polsky, parce que je crains que la partie opposée tente de ne pas l'entendre. J'aimerais m'assurer que nous pouvons lui poser toutes les questions que nous désirons. J'adore écouter M. Therrien, mais quand même…

[*Traduction*]

Le président: Tous les députés pourront poser des questions à qui ils veulent.

M. René Villemure: C'est bien.

Le président: Comme je l'ai dit, nous allons recommencer les tours.

Sur ce, j'aimerais commencer, car j'aimerais terminer la séance le plus près possible de 13 heures, afin que nous puissions régler quelques points.

Je souhaite la bienvenue à Mme Polsky au sein du Comité et je l'invite à présenter sa déclaration liminaire, pour un maximum de cinq minutes.

● (1205)

Mme Sharon Polsky (présidente, Conseil du Canada de l'accès et la vie privée): Merci, monsieur le président.

Bonjour de Calgary.

Je vous remercie, vous et les membres du Comité, de m'avoir invitée à comparaître devant vous aujourd'hui.

En 1964, Ronald Reagan a dit: « La liberté n'est jamais à plus d'une génération de l'extinction. »

En 1992, notre Cour suprême a déclaré: « La surveillance électronique est à ce point efficace qu'elle rend impossible, en l'absence de réglementation, l'anéantissement de tout espoir que nos communications restent privées. » La Cour suprême a aussi dit que nous avons le droit de savoir lorsque l'État porte atteinte à notre vie privée.

La nécessité de cette étude nous indique que la déclaration de la Cour est restée lettre morte.

Comme nous l'avons vu avec Clearview AI, la police a parfois échantillonné des outils policiers axés sur les données sans trace écrite de l'approvisionnement, des outils dont elle dit avoir besoin pour assurer la sécurité publique afin de se protéger contre les menaces perçues ou, comme le prévoit le projet de loi C-27, d'apporter des avantages à la société. Autrement dit, la technologie elle-même est moralement neutre. La façon dont son utilisation est justifiée change tout, et c'est pourquoi il est si important que cette étude ne soit pas cachée derrière des portes closes, à l'abri du regard du public.

Nous savons que la Stasi espionnait secrètement ses citoyens, mais nous ne nous attendons pas à ce que les gouvernements démocratiques espionnent les leurs. Pourtant, cela se produit maintenant au Canada et dans le monde entier, où des journalistes, des cadres, des militants sociaux et des représentants élus dont les opinions diffèrent de celles du parti au pouvoir sont espionnés.

Or, jusqu'à récemment, lorsque les gens pensaient à la GRC, c'était pour évoquer Dudley Do-Right et le sergent Preston, des défenseurs de la justice et du franc jeu dans leur poursuite incessante des contrevenants, qui respectaient l'intention dans la lettre de la loi, la Charte et la vie privée des Canadiens, plutôt que d'utiliser un programme de surveillance non signalé pour espionner les comptes de médias sociaux des Canadiens.

Il est vrai que les logiciels espions peuvent aider la police à faire son travail. Mais le plus souvent, ils sont téléchargés par centaines de milliers et utilisés par les trafiquants d'êtres humains pour contrôler les esclaves sexuels et, dans les conflits familiaux, terroriser les partenaires.

Ils font aussi partie d'un nouveau secteur lucratif qui fait que notre vie privée, notre liberté et notre démocratie ne sont pas à plus d'une crise ou d'une élection de l'extinction. Comment un député ou un bureaucrate peut-il être certain que les documents confidentiels du Cabinet, les stratégies militaires, les plans électoraux ou quoi que ce soit d'autre peuvent être discutés en privé alors qu'il existe une chance bien réelle qu'une application cachée permette à quelqu'un, quelque part dans le monde, d'écouter, de regarder et d'enregistrer chacun de vos messages textes, de vos courriels et chacune de vos photos, de siphonner vos contacts et vos mots de passe et d'activer silencieusement le microphone et la caméra pour vous observer et vous écouter, vous et votre environnement, sans être détecté?

Pour ce qui est de la question de savoir si les logiciels espions présentent des avantages sociaux, la réponse est un oui retentissant, même si cela peut paraître contradictoire. C'est la Ford Pinto de la technologie, un danger caché du public en général et de certaines personnes en particulier, avec de nombreuses retombées socialement bénéfiques sur le plan de l'emploi, du commerce et des taxes.

L'industrie mondiale de la cybercriminalité génère plus de 1,5 billion de dollars américains par an. L'industrie mondiale de la cybersécurité se chiffre à 1,7 billion de dollars et, au Canada, elle représente actuellement 3,5 milliards de dollars américains.

Pegasus n'est que le dernier logiciel espion à faire les manchettes. Il nous rappelle que les logiciels d'espionnage sont une entreprise non partisane, qui offre des chances égales à tous, et que les outils de lutte contre le terrorisme mis en place après le 11 septembre ont fait de nous tous des proies faciles pour les attaques et l'utilisation de nos propos contre nous. Peut-être qu'ils l'ont déjà fait.

Pour perturber l'industrie de la surveillance mercenaire, il faudra une volonté politique multipartite, un effort coordonné à l'échelle nationale et internationale et un changement d'approche afin de prévenir d'emblée les dommages en réglementant l'exploitation de la vie privée. Il faut tenir pour responsable qui il se doit.

Les développeurs, les producteurs et les distributeurs de logiciels espions, les investisseurs et la technologie intrinsèquement défectueuse font que le risque est plus grand que la récompense, car la réglementation du contenu d'Internet n'arrêtera pas les logiciels espions ou les prédateurs d'enfants, et les lois interdisant les sociétés de piratage informatique et permettant d'attraper occasionnellement un criminel n'ont rien changé.

L'utilisation de logiciels espions doit être rendue illégale, sauf dans des situations exceptionnelles particulières et pour la durée la plus courte possible nécessaire à l'atteinte d'un objectif d'enquête particulier, et leur utilisation doit être approuvée à l'avance par une tierce partie indépendante, bien informée et apolitique, afin que les Canadiens puissent retrouver la confiance dans le gouvernement et le secteur public et avoir une raison de voir les agents de la Police montée comme Dudley Do-Right, et non pas comme Snidely Whiplash.

● (1210)

Le président: Merci de votre déclaration liminaire.

Nous passons maintenant à M. Bezan, pour un maximum de six minutes.

M. James Bezan: Merci, monsieur le président.

Je tiens à remercier Mme Polsky de se joindre à nous aujourd'hui.

À quel point avez-vous été choquée, en tant que présidente du Conseil du Canada de l'accès et de la vie privée, d'apprendre hier, lors d'un témoignage, que la GRC déploie des outils d'enquête sur appareil depuis avant 2012?

Mme Sharon Polsky: Malheureusement, pas du tout.

M. James Bezan: Comme vous le savez, ce système de piratage mobile qui a été utilisé sur nos appareils a été interdit — en particulier Pegasus — aux États-Unis. Préconisez-vous que ce type de technologie soit interdit ou que les services de police et d'autres organisations l'utilisent selon des directives plus strictes?

Mme Sharon Polsky: Je pense que le problème est plus grand que cela, car il ne s'agit pas seulement d'interdire l'utilisation par la police d'un outil qui peut être utilisé à des fins légitimes, que ce soit par la police ou par d'autres organismes d'application de la loi. Le problème, c'est que ces outils, si avancés soient-ils techniquement, sont tous disponibles sur le marché pour quiconque dispose d'une connexion Internet et veut les télécharger. C'est là que réside le problème, car sinon, nous ne faisons que travailler après coup pour essayer d'attraper celui qui les utilise.

Notre Code criminel, pour autant que je sache, ne parle pas de quelqu'un qui met un logiciel espion sur mon téléphone ou le vôtre, comme un conjoint, un partenaire intime ou un étranger. S'il prend des photos intimes et les distribue sans mon consentement, le Code criminel en parle, mais pas du logiciel espion lui-même. Personne ne parle d'empêcher les logiciels espions d'être utilisés en premier lieu. Personne ne parle de la façon dont le logiciel espion est capable de tirer parti des lacunes et des déficiences de tant de programmes logiciels.

La semaine dernière, en une seule journée, Google a apporté 37 correctifs, y compris des correctifs critiques. Cette société et d'autres continuent de poser des rustines sur des logiciels défectueux. Il faut exiger que les logiciels soient testés correctement afin de réduire au minimum les possibilités pour les logiciels espions de tirer parti dès maintenant des déficiences intégrées.

M. James Bezan: Sachant que certains de ces logiciels sont offerts sur le marché, ce que j'ai appris au cours des 24 dernières heures... Nous avons parlé de Pegasus, mais maintenant, il y a aussi Paragon, Candiru, le logiciel Cognyte. Il est possible que ces logiciels aient été intégrés à des drones.

À votre connaissance, quelles plateformes logicielles ont été utilisées au Canada?

Mme Sharon Polsky: Je ne le sais pas précisément. J'ai parlé avec des collègues qui ont fait des recherches dans ce domaine, et on m'a assuré qu'il y en avait plusieurs, mais on n'en parle pas. Les faux-fuyants sont une chose merveilleuse. Si vous décrivez un outil comme un outil d'enquête numérique, il n'est pas dit que c'est un logiciel espion. Cela lui donne un air de légitimité. Je ne sais pas en particulier lequel est utilisé et lequel ne l'est pas.

M. James Bezan: Croyez-vous que le ministre Mendicino a recouru à des faux-fuyants hier? Pensez-vous que, après son témoignage, il a rétabli la confiance dans nos institutions sur la question de savoir si elles surveillent ou non les Canadiens?

Mme Sharon Polsky: J'ai trouvé ses réponses intéressantes, en particulier lorsqu'il nous a assuré à plusieurs reprises que ces outils logiciels ne sont utilisés que dans les limites prévues par la Loi, même si je crois que c'est lui, ou peut-être quelqu'un d'autre, qui a dit qu'il y a des dispositions dans la loi sur la sécurité nationale qui permettent l'utilisation expresse de ces outils sans autorisation judiciaire. Mais même cela reste dans les limites de la Loi.

M. James Bezan: Hier, il a admis que la GRC utilisait les appareils d'enquête sur appareil depuis 2012 et avant, mais il a contourné la question de savoir si d'autres organismes gouvernementaux les utilisent ou non.

Croyez-vous que les Canadiens ont le droit de savoir si le SCRS, le CST, l'ASFC ou le ministère de la Défense nationale utilisent également ces outils?

Mme Sharon Polsky: Je pense que les Canadiens ont le droit de savoir. Il est possible de révéler l'utilisation de ces outils sans compromettre les enquêtes policières.

● (1215)

M. James Bezan: À quel point est-ce dangereux pour nos libertés civiles et notre capacité de légiférer de manière appropriée sur l'utilisation de ces outils lorsque nous avons un gouvernement qui n'a pas reconnu les faits essentiels, à savoir qui fait quoi avec les outils d'enquête sur appareil?

Mme Sharon Polsky: Je me souviens que notre premier ministre a déclaré il y a plusieurs années que les Canadiens méritent — je paraphrase — le gouvernement le plus transparent et le plus responsable qui soit. J'en conviens, mais en tant que contribuable, en tant que citoyenne canadienne, je suis sceptique quant à l'atteinte de cet objectif. En tant que praticienne de l'accès à l'information et de la protection de la vie privée depuis de très nombreuses années, et connaissant de nombreuses personnes dans l'industrie, y compris dans notre capitale nationale, il me semble que la façon dont les lois sur l'accès à l'information ont été rédigées servent à créer un bouclier plutôt qu'à voir ce qui se passe.

Le président: Il vous reste 10 secondes.

M. James Bezan: Je tiens à remercier nos témoins d'être avec nous aujourd'hui.

Le président: Merci, monsieur Bezan.

Madame Hepfner, vous avez la parole.

Mme Lisa Hepfner: Merci, monsieur le président.

J'aimerais revenir à M. Therrien et à certaines des conversations que nous avons eues durant l'heure précédente.

On a beaucoup répété que la surveillance judiciaire ne suffit pas. Je pense que ce que vous nous avez dit, c'est que c'est une assez bonne protection et que ce n'est pas la seule protection dont nous disposons pour nous assurer que la GRC remplit son mandat en respectant la lettre de la loi. Par exemple, si elle devait recueillir des renseignements à l'aide de cette technologie et les présenter au tribunal pour qu'il les utilise dans la poursuite de ses suspects, et que celui-ci constatait qu'elle ne l'avait pas utilisée correctement, alors les preuves ne seraient pas valables et n'auraient aucune valeur, et il ne servirait donc à rien pour la GRC d'utiliser cette technologie sans respecter la lettre de la loi.

Je me demande si vous souscrivez à cette affirmation et si vous pouvez en dire un peu plus à ce sujet.

M. Daniel Therrien: Je pense que cela représente assez bien ce que j'ai dit. Les mesures de protection de la vie privée prévues dans la partie VI du Code criminel sont bonnes. Elles pourraient bien être perfectibles, surtout compte tenu de la nature très invasive des outils d'enquête sur appareil.

Mme Lisa Hepfner: Veuillez nous en dire plus à ce sujet. Que voulez-vous dire?

M. Daniel Therrien: Oui, les mesures de protection du Code criminel sont bonnes. Sont-elles idéales? Sont-elles parfaites? Sont-elles perfectibles? Je vous laisse le soin de répondre à cette question. Je pense qu'il est certainement possible d'apporter des améliorations, mais elles sont bonnes. Nous avons un bon point de départ.

Mme Lisa Hepfner: Nous avons également entendu dire, comme l'un de mes collègues l'a mentionné hier, que nous, les députés, pourrions être davantage exposés au risque que nos téléphones cellulaires soient visés par des acteurs extérieurs et des personnes à l'extérieur du pays qui ne se soucient peut-être pas de respecter le Code criminel. Que pensez-vous de cette question et du niveau de risque dans notre pays en provenance de l'extérieur du Canada?

M. Daniel Therrien: Le droit canadien régit les institutions canadiennes, y compris la GRC, et dans l'ensemble, nous avons de bonnes règles. Comme nous le savons, un certain nombre de pays du monde ne sont pas démocratiques et ne se soucient pas beaucoup de la primauté du droit, et il est tout à fait possible, voire probable — la GRC semble dire que c'est un fait — que d'autres États interceptent les communications de ressortissants étrangers, y compris de Canadiens, à leurs propres fins. Selon la GRC, c'est un fait.

Mme Lisa Hepfner: Comment le Canada se compare-t-il aux autres pays lorsqu'il s'agit de valoriser le droit à la vie privée de ses citoyens?

M. Daniel Therrien: Il est clair que le Canada est un pays régi par la Charte, la primauté du droit, et que, de façon générale, il jouit d'une bonne réputation en matière de défense des droits de la personne. En même temps, il a été mentionné il y a quelques minutes que la Loi sur la protection des renseignements personnels qui s'applique au secteur public a 40 ans. Elle a été adoptée lorsque les documents détenus par le gouvernement étaient conservés par écrit dans des classeurs et que les renseignements ne pouvaient pas être obtenus ou divulgués aussi facilement qu'en 2022.

Dans l'ensemble, il est évident que nous sommes un pays qui respecte la primauté du droit, mais nos lois, en particulier celles sur la protection des renseignements personnels, ont grand besoin d'être améliorées du point de vue de la vie privée.

● (1220)

Mme Lisa Hepfner: Dans la minute et demie qu'il me reste, vous pourriez peut-être passer en revue certaines de vos idées, que vous avez déjà évoquées aujourd'hui, j'en suis sûre, pour améliorer nos lois sur la protection des renseignements personnels afin que nous puissions nous assurer de respecter la norme la plus élevée qui soit.

M. Daniel Therrien: Les lois du Canada, pour le secteur tant public que privé, devraient reconnaître la vie privée comme un droit de la personne fondamental. C'est le point de départ. Nous devrions nous assurer que le Commissariat à la protection de la vie privée du Canada, tant pour le secteur public que pour le secteur privé, a le pouvoir de non seulement faire des recommandations, mais de rendre des ordonnances pour le secteur privé et le secteur public lorsqu'il constate des violations de la Loi. Il devrait aussi y avoir des sanctions financières, certainement dans le secteur privé, pour que l'on s'assure que ces lois sont respectées.

Je dirais, parce que je pense que c'est pertinent pour cette étude particulière et que cela a été mentionné il y a une minute concernant l'utilisation de ces technologies intrusives dans le secteur privé, que, en 2022, l'information circule largement entre le secteur privé et le secteur public, et il est important que, à tout le moins, les lois du secteur public et du secteur privé soient compatibles et complémentaires. Idéalement, elles devraient être réunies en une seule loi, car les données ne connaissent pas de frontières entre le secteur public et le secteur privé. Encore une fois, à tout le moins, les règles devraient être similaires et complémentaires entre le secteur public et le secteur privé.

Mme Lisa Hepfner: C'est très utile. Merci.

Le président: Merci.

[*Français*]

Monsieur Villemure, vous avez la parole pour six minutes.

M. René Villemure: Je vous remercie beaucoup, monsieur le président.

Bonjour, madame Polsky. Je vous souhaite la bienvenue au Comité. Nous sommes très heureux de vous recevoir aujourd'hui.

Depuis le début, il est question de vie privée et de confiance. Nous voulons générer et maintenir la confiance.

Plusieurs concitoyens de ma circonscription me disent qu'ils n'ont rien à cacher et ils se demandent donc pourquoi il faut s'occuper de ces choses. Je ne suis pas certain que les gens comprennent le caractère intrusif des logiciels espions, par exemple.

Seriez-vous en mesure de nous l'expliquer afin que nous puissions expliquer à nos concitoyens ce à quoi ils doivent faire face?

[*Traduction*]

Mme Sharon Polsky: Eh bien, des gens m'ont dit: « Je n'ai rien à cacher », mais quand j'ai répondu: « Montrez-moi votre relevé bancaire », cela les a rendus mal à l'aise. Les gens ont effectivement des choses à cacher, mais il s'agit plutôt de l'idée que, lorsque je souhaite communiquer une information particulière à mon sujet, je devrais avoir le choix de le faire.

Ceux qui veulent afficher leur vie en ligne, les moindres détails de leur vie, c'est leur choix, mais pour paraphraser la sénatrice Simons, les gouvernements ne sont pas toujours bienveillants. Je regarde la Hongrie et la Pologne, mais la Hongrie en particulier, qui a changé ces dernières années pour devenir plutôt autoritaire. Son autorité de protection des données, dont on pourrait s'attendre à ce qu'elle joue un rôle semblable à celui de notre commissaire à la protection de la vie privée, a statué que l'utilisation de Pegasus contre les journalistes du pays ne violait pas la loi, parce qu'il y avait un élément de sécurité nationale.

Les choses qui sont acceptables aujourd'hui peuvent être changées sur un coup de tête, utilisées contre vous et sorties de leur contexte. Ce n'est pas nouveau, cela existe depuis des temps immémoriaux, mais nous devons avoir le choix. Le fait que nos renseignements ou les renseignements nous concernant soient recueillis, pris, assemblés, évalués et analysés par quelqu'un que nous ne connaissons pas, que nous n'avons jamais rencontré et à qui nous n'avons jamais donné la permission — que vont-ils en faire? — nous ramène aux audiences de McCarthy. C'est effrayant.

Je suis là depuis longtemps, et il n'y a pas grand-chose qui m'effraie. Ce qui se passe maintenant est effrayant, et c'est ce dont les gens doivent se rendre compte. Ce n'est pas seulement de la bienveillance.

● (1225)

[*Français*]

M. René Villemure: Y aurait-il lieu d'avoir un débat public sur la protection de la vie privée ou des programmes de sensibilisation afin que les gens soient plus à même de comprendre ce à quoi ils doivent faire face?

[*Traduction*]

Mme Sharon Polsky: Oh, ce serait merveilleux. Les ordinateurs de bureau existent depuis près de 50 ans, et à ma connaissance, il n'y a pas encore d'éducation approfondie, que ce soit pour les plus jeunes écoliers ou même pour les universitaires. On leur apprend peut-être à coder, mais tout le monde n'a pas besoin de coder, et savoir coder ne signifie pas que vous comprenez la vie privée, ce qu'est la vie privée, comment elle peut être compromise et comment vous protéger pour éviter de cliquer sur la mauvaise chose et de mettre en danger votre appareil, votre entreprise et, peut-être, dans votre cas, le pays en raison de la sécurité nationale.

Au fil des ans, j'ai discuté avec divers membres de la magistrature de tout le pays, qui m'ont dit les uns après les autres: « Je ne sais pas ce qu'est cette histoire de vie privée. Je suis à cette conférence pour l'apprendre, même si je juge des affaires qui sont délicates sur le plan de la vie privée. » Il n'y a pas eu suffisamment d'éducation, et il doit y avoir un volet d'éducation obligatoire consacré, intégré dans une stratégie pancanadienne, si vous le voulez, afin que les provinces et les territoires puissent être encouragés à intégrer cette question comme une partie obligatoire du programme d'études, dès les premières années.

[*Français*]

M. René Villemure: Pour le moment, ne devrions-nous pas imposer un moratoire sur l'utilisation de ces technologies, le temps de mieux les comprendre, de mieux les expliquer et de mieux légiférer, dans notre cas?

[*Traduction*]

Mme Sharon Polsky: Eh bien, ce serait formidable, mais au cours des dernières années, nous avons vu une multitude de villes, d'États et de pays déclarer des moratoires sur la reconnaissance faciale, et maintenant ils reviennent en arrière en disant que ce serait peut-être une meilleure chose s'ils l'avaient. C'est une mesure temporaire. Je pense qu'il est plus important de s'attaquer à la source du problème, à savoir les logiciels défectueux qui permettent aux logiciels espions, aux rançongiciels et aux autres logiciels malveillants d'être efficaces.

[*Français*]

M. René Villemure: Je vous remercie beaucoup.

[*Traduction*]

Le président: Vous avez une autre minute.

[*Français*]

M. René Villemure: Monsieur Therrien, j'aimerais revenir sur un sujet que vous avez évoqué brièvement. Le droit à la vie privée est traité dans plusieurs projets de loi et il a fait l'objet de plusieurs révisions dans les lois concernant le secteur privé et le secteur public.

N'y aurait-il pas lieu de créer une seule loi? Je comprends que cela pourrait être complexe. Or cela pourrait permettre de corriger les failles existantes dans les lois en question.

M. Daniel Therrien: C'est la situation dans certains pays. Puisque les données voyagent, si je peux m'exprimer ainsi, entre les secteurs privé et public, ce serait une bonne idée.

J'ajouterais cependant que nous avons attendu 40 ans pour avoir les modifications à la Loi sur la protection des renseignements personnels concernant le secteur public et que nous avons attendu 20 ans pour avoir des modifications à celle concernant le secteur privé. Le risque de tout mettre dans une loi au Canada aujourd'hui serait de retarder l'adoption de la loi relative au secteur privé, qui est présentement devant le Parlement.

Sur le plan des principes, les secteurs privé et public devraient être réglementés d'une façon semblable. Le contexte est un peu différent parfois, mais les lois devraient avoir des principes semblables, sinon identiques.

M. René Villemure: Je vous remercie beaucoup.

[*Traduction*]

Le président: Merci.

Nous passons maintenant à M. Green, pour un maximum de six minutes.

M. Matthew Green: Merci beaucoup.

Monsieur Therrien, je suis sûr que vous savez que la présidente du Conseil du Trésor est responsable d'établir des politiques et de prescrire des formulaires concernant l'application de la Loi sur la protection des renseignements personnels dans le secteur public. Nous savons qu'elle a ce mandat depuis un certain temps.

Fort de votre expérience à titre de commissaire à la protection de la vie privée, pourriez-vous nous dire dans quelle mesure les ministères et les organismes visés par la Loi sur la protection des renseignements personnels ont présenté de façon proactive des politiques et des mesures de résultats et de responsabilisation dans leurs plans ministériels, dans le cadre de leurs rapports aux comptes publics et au Commissariat? Pensez-vous qu'ils ont suivi le rythme de la technologie telle qu'elle est aujourd'hui?

M. Daniel Therrien: C'est une excellente question.

Je dirais que, pendant mon mandat, le Conseil du Trésor, en priorité, à cause de ressources limitées probablement, a consacré plus de temps aux questions d'accès à l'information qu'aux questions de protection de la vie privée. Il n'était pas absent du paysage de la vie privée, mais il a certainement donné la priorité à l'accès à l'information. Un projet de loi sur l'accès à l'information a été présenté, etc.

En résumé, il n'y a pas eu d'absence d'activité, mais il n'y a pas eu beaucoup d'activité.

● (1230)

M. Matthew Green: Est-il juste de dire que, même si, dans son esprit, la politique du Conseil du Trésor demandait à tous les organismes d'adopter des mesures de protection accrues en vertu de la Loi sur la protection des renseignements personnels, elle n'a pas nécessairement donné lieu à de nouvelles politiques proactives qui suivent le rythme de la technologie actuelle?

M. Daniel Therrien: Oui, même si je dirais que, au cours de la dernière année environ, il y a eu des faits nouveaux intéressants — une politique sur l'intelligence artificielle, par exemple — mais pendant mon mandat, il n'y a pas eu beaucoup d'activité. Il y a eu plus de progrès récemment.

M. Matthew Green: Au cours de votre mandat, quelle part de cette activité d'amélioration proactive, d'autoréflexion et de vérification provenait des organismes d'application de la loi et de sécurité publique, plus précisément de la GRC? La GRC a-t-elle montré la voie en améliorant ses processus de protection de la vie privée?

M. Daniel Therrien: Non. Si nous regardons la reconnaissance faciale et la création de ce qu'elle appelle le PNIT, c'était à notre demande. Ce n'était pas proactif de sa part.

M. Matthew Green: Bien sûr. Est-il aussi juste de dire que, dans certaines de vos discussions — j'espère que nous pouvons être francs ici —, ils n'étaient peut-être pas toujours disposés à vous fournir les renseignements nécessaires pour que vous puissiez vous acquitter de vos tâches en temps opportun?

M. Daniel Therrien: Je pense qu'ils fonctionnaient dans le cadre de la Loi telle qu'elle est.

M. Matthew Green: C'est une distinction importante, parce que ce qui nous est présenté aujourd'hui n'est pas nécessairement la position selon laquelle la GRC est considérée comme un organisme malhonnête ou qui ne respecte pas la Loi, mais ce sont les lacunes, à mon avis. En fait, dans son témoignage, le sous-commissaire Larkin a laissé entendre qu'il y avait des lacunes dans la Loi.

Diriez-vous aussi que, même ce qui est actuellement légal, et je pense que nous avons établi que c'est assez dépassé, ce n'est pas nécessairement éthique, compte tenu de la façon dont la technologie a dépassé la législation?

M. Daniel Therrien: Que ce soit éthique ou non, il y a certainement des améliorations qui sont possibles, compte tenu du caractère intrusif de la technologie, au-delà de la partie VI du Code criminel. Oui.

M. Matthew Green: Je pense qu'il y aura un long débat sur l'éthique, mais je dirais au Comité que si nous avons une technologie qui va au-delà de l'esprit de la Loi actuelle et qui est reconnue comme telle, alors dans certains cas, qu'il s'agisse de la technologie Stingray ou de l'opération Wide Awake, c'est-à-dire la surveillance des médias sociaux, ou d'autres, s'ils ne divulguent pas ces choses de façon proactive, cela ne donne pas aux législateurs la possibilité de suivre le rythme. Je pense que c'est dans cet esprit que nous sommes ici aujourd'hui.

J'ai fait allusion à la Convention européenne des droits de l'homme, qui a établi la transparence, la responsabilisation, la protection de la vie privée dès la conception et les évaluations d'impact sur la protection des données. Il s'agit d'un texte de loi relativement moderne. Selon vous, comment le Canada se compare-t-il à cela?

M. Daniel Therrien: Nous avons en général des politiques, pas toujours respectées, dont l'esprit est similaire, mais ce ne sont pas des exigences légales. Je pense qu'il serait extrêmement utile de transformer ces règles stratégiques en lois afin que l'on augmente considérablement la probabilité qu'elles soient bel et bien mises en œuvre.

M. Matthew Green: J'en conviens. J'ai travaillé dans le domaine des services publics, de l'approvisionnement et des comptes publics, et je suis maintenant membre du Comité, et je peux vous dire que nous avons un gouvernement qui excelle dans la rédaction de bonnes politiques. Il rédige en fait des politiques décentes. Le problème, c'est que nous n'avons jamais les résultats. Nous n'avons jamais les résultats mesurables. Nous n'avons jamais les résultats attendus lorsqu'il s'agit de suivre les directives de la présidente du Conseil du Trésor et de voir à ce qu'elles soient mises en œuvre au gouvernement.

De ce point de vue, ce que j'entends aujourd'hui, et nous pouvons faire des distinctions entre ce qui est normatif ou non et ce qui est préambule ou non, je suis fermement convaincu que si nous ne demandons pas aux organismes d'application de la loi de s'améliorer, d'accroître leur transparence et de fournir des mesures claires de responsabilisation et de protection de la vie privée dès la conception, cela ne se produira pas.

Croyez-vous que, si nous ne fournissons pas ces directives, cela ne se produira pas?

M. Daniel Therrien: Oui. De plus, je pense que ces exigences peuvent se situer à un niveau de généralité suffisant, mais tout de même important, sans être trop normatives et empêcher les responsables, que ce soit la police ou d'autres, d'exercer leur jugement. Mais...

● (1235)

Le président: Merci.

M. Matthew Green: Merci.

Le président: Nous allons maintenant passer à M. Williams, pour un maximum de cinq minutes.

M. Ryan Williams: Merci, monsieur le président.

Madame Polsky, je suis heureux de vous revoir.

Après que la GRC a été surprise à utiliser des identificateurs d'appareils mobiles, ou IMSI, en 2017, elle a dit qu'elle voulait lancer un débat public sur les pouvoirs de la police et la vie privée. Cette discussion n'a clairement jamais été entamée. Souscrivez-vous à cette déclaration?

Mme Sharon Polsky: À ma connaissance, elle ne s'est pas engagée dans cette étude.

M. Ryan Williams: Pensez-vous que l'équilibre entre les pouvoirs de la police et la vie privée devrait être changé? À quoi cela devrait-il ressembler?

Mme Sharon Polsky: Je pense que les policiers doivent reconnaître qu'ils ne seront pas toujours en uniforme et que cela les touche individuellement aussi facilement que vous et moi et n'importe qui d'autre.

Les membres des forces de l'ordre sont comme tout le monde. Eux aussi manquent d'éducation fondamentale sur les droits et les responsabilités en matière de protection de la vie privée et sur la législation. Ils sont chargés de faire respecter la loi, et c'est ce qu'ils font. Ils voient les choses sous cet angle, comme il se doit, mais il faut les encourager à les voir sous d'autres angles.

M. Ryan Williams: Que doit faire le législateur pour réglementer correctement ces types d'utilisation de logiciels espions par la GRC, le SCRS et le CST, par exemple?

Mme Sharon Polsky: Tout d'abord, je pense que si les logiciels espions sont réglementés par la GRC et les organismes fédéraux, cela ne concerne pas les agences d'application de la loi municipales et provinciales, et il faut donc que ce soit global.

Je pense qu'il s'agit de rédiger des lois — encore une fois, sans l'influence directe ou indirecte de l'industrie — qui font porter la responsabilité en premier lieu sur les entreprises de matériel et de logiciels et sur leurs dirigeants, qui vendent des produits pleins de vulnérabilités permettant des attaques par des logiciels espions, des rançongiciels et des maliciels. Il faudrait interdire l'achat ou l'utilisation par le gouvernement fédéral, directement ou indirectement, de logiciels espions par une loi, un règlement ou un décret, avec des interdictions équivalentes dans chaque province et territoire, et travailler avec les gouvernements étrangers pour interdire la vente, l'exportation, la distribution et l'utilisation de logiciels espions commerciaux et l'investissement dans ceux-ci.

Nous avons déjà des accords internationaux de libre-échange qui comportent des dispositions obligatoires sur l'échange transfrontalier d'information et toutes sortes d'autres dispositions. Ils doivent inclure des dispositions dans le cadre desquelles les signataires acceptent de criminaliser et de poursuivre les personnes et les organisations qui créent, mettent à l'essai, commercialisent, financent et distribuent des logiciels espions, ainsi que les dirigeants et les investisseurs. Il doit y avoir des sanctions parce que, autrement, c'est comme une politique: c'est dans les livres, mais si quelqu'un d'autre dans un pays peut utiliser ces produits contre nous, ses propres gouvernements doivent intervenir pour l'arrêter, parce que c'est dans ce pays, bien sûr. C'est hors de notre portée.

M. Ryan Williams: Pour renchérir sur le sentiment ou la déclaration de ma collègue plus tôt... Quelle bonne politique mise en œuvre dans d'autres pays devrait être mise en œuvre ici, au Canada?

Mme Sharon Polsky: Une des différences les plus importantes, à mon avis — une distinction — que le RGPD en Europe a fait ressortir, c'est que lorsqu'une évaluation des facteurs relatifs à la vie privée est effectuée, lorsqu'une organisation a un responsable de la protection des données, ce qui est obligatoire, en vertu du RGPD, c'est mettre l'accent sur le risque pour la personne dont les renseignements sont recueillis, utilisés, etc. Ce n'est pas le risque pour l'organisation. D'après mon expérience, c'est trop souvent ainsi que les organisations canadiennes voient les choses.

D'abord, s'ils ont une EFVP préliminaire — parce que nous sommes occupés, nous sommes une grande organisation —, les rares personnes qui comprennent vraiment la situation sont trop occupées pour faire une EFVP pour tout le monde, alors ils la renvoient au ministère et disent: « Voilà, faites une EFVP préliminaire, et vous me direz si vous pensez que nous devons faire une EFVP. » Ils ne savent pas ce qu'ils regardent, alors bien sûr, c'est facile de dire: « Nan, cela n'a aucune incidence sur les renseignements personnels, donc nous n'avons pas besoin d'une EFVP. » C'est là que cela s'arrête. C'est un système défectueux.

Lorsqu'ils font une EFVP... certaines d'entre elles sont très superficielles. On parle des avantages d'un produit ou d'un nouveau système, mais on ne parle pas du risque pour la personne. C'est comme si leur rôle était de protéger contre le risque pour l'organisation. Il faut que cela change.

● (1240)

M. Ryan Williams: Monsieur le président, ma dernière question pour...

Le président: Vous êtes...

M. Ryan Williams: Ce sera pour un oui ou un non. Ce sera tout.

Le président: Vous avez 10 secondes.

M. Ryan Williams: Ma question s'adresse aux deux témoins. Serait-il possible d'éviter l'EFVP?

M. Daniel Therrien: Non.

Mme Sharon Polsky: Non.

M. Ryan Williams: Merci beaucoup.

Le président: Bien joué.

Nous allons maintenant passer à notre prochain intervenant, qui sera M. Erskine-Smith.

Bienvenue à nouveau au comité de l'éthique.

M. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Merci, monsieur Kelly. Je suis heureux d'être de retour et de vous voir.

Je suis particulièrement heureux de vous revoir, monsieur Therrien. J'ai aimé recevoir vos conseils et votre orientation au fil des ans, lorsque je siégeais au Comité.

Je vais commencer par ce que j'ai jugé être le point de vue de la GRC: « Nous ne pouvons pas divulguer le fournisseur en raison de la sécurité nationale. » Pourtant, du point de vue des marchés publics gouvernementaux, c'est assez inquiétant pour moi, car je vois que certaines de ces technologies — et je sais que la GRC a dit qu'elle n'utilisait pas Pegasus, mais Pegasus est un exemple — ont été utilisées pour porter gravement atteinte aux droits de la personne dans le monde, en attaquant des journalistes et d'autres défenseurs de ces droits.

Dans l'intérêt public, ne devrions-nous pas savoir qui est le fournisseur afin de pouvoir exercer une certaine diligence raisonnable en matière de marchés publics?

M. Daniel Therrien: Qu'il y ait une transparence dans le processus d'approvisionnement est certainement une très bonne idée. C'est nécessaire, en fait. Quant à savoir si le nom d'un fournisseur particulier devrait être rendu public, je reviendrais à la norme générale: il devrait y avoir de la transparence en règle générale, sauf si les méthodes deviennent inefficaces à cause de la transparence.

M. Nathaniel Erskine-Smith: Je pense que c'est la bonne norme. Il est difficile d'imaginer que le fait de connaître le nom d'un fournisseur puisse porter atteinte à la sécurité nationale, malgré les protestations que nous avons entendues hier.

Pour en venir à la question principale, nous avons parlé de la nature de l'outil et de son étendue en ce qui concerne la collecte de données, mais je veux adopter une approche légèrement différente, monsieur Therrien, parce que ce que ces outils ont tendance à faire et ce qui les rend manifestement différents des autres outils, c'est qu'ils tirent parti d'une vulnérabilité existante dans la technologie actuelle et l'exploitent. Vous avez des forces de l'ordre qui exploitent une vulnérabilité, et cette vulnérabilité influence fondamentalement tous les Canadiens, parce qu'elle se trouve sur tous les appareils.

N'y a-t-il pas un argument selon lequel les forces de l'ordre devraient reconnaître cette vulnérabilité et en informer l'entreprise afin qu'elle soit corrigée sur tous nos appareils?

M. Daniel Therrien: C'est une question difficile. Oui, si les représentants du gouvernement voient une vulnérabilité dans un système, ils devraient en informer le créateur ou le fournisseur du système, en tant que principe généralement applicable et mis en œuvre, oui. Cela dit, le cryptage est un défi pour les forces de l'ordre, et je pense donc faire une distinction entre les lois qui imposent la création de portes dérobées et les lois qui autorisent la police à contourner le cryptage au moyen de vulnérabilités existantes pendant une certaine période, parce que c'est peut-être le seul moyen de mener à bien l'enquête.

Bien franchement, je ne sais pas quelle est la meilleure solution à ce problème. Je suis d'accord avec vous pour dire qu'il y a une obligation d'informer le fournisseur ou le créateur à un moment donné, mais comment la police...? Selon moi, ce qui est fait ici est moins problématique que les lois créant des portes dérobées, en particulier lorsque le système est soumis à un contrôle judiciaire.

M. Nathaniel Erskine-Smith: Parlons de cette surveillance dans le temps qu'il me reste.

Je suis réconforté par le fait que la GRC a déclaré qu'elle n'a utilisé cette technologie que dans le cadre d'une surveillance judiciaire, mais bien sûr, il aurait été bon qu'elle soit plus proactive dans la divulgation de son utilisation de la technologie. Nous avons maintenant un modèle, je pense, lorsque nous regardons les Stingray, Clearview AI, et maintenant, cette technologie d'espionnage, et encore une fois, nous ne savons pas qui est le fournisseur.

Pensez-vous que le commissaire à la protection de la vie privée devrait intervenir? Quand je vois la GRC nous dire que 9 demandes sur 10 n'ont pas reçu d'approbation interne, je ne sais pas quel est ce cadre d'approbation interne, très franchement. Je pense que si j'étais responsable de la GRC, je m'engagerais de manière proactive avec le commissaire à la protection de la vie privée pour établir ce cadre interne. Cela vous paraît-il logique?

● (1245)

M. Daniel Therrien: Oui, absolument.

M. Nathaniel Erskine-Smith: C'est aussi logique pour moi.

M. Daniel Therrien: C'est ce que nous avons recommandé pour la reconnaissance faciale, ce qui a conduit au processus du PNIT. Oui, le commissaire à la protection de la vie privée devrait intervenir pour s'assurer que ces processus sont solides et robustes.

M. Nathaniel Erskine-Smith: C'est vrai, parce que vous avez ensuite le cadre d'approbation interne en consultation avec le commissaire à la protection de la vie privée, puis le cadre judiciaire en aval.

Merci, monsieur Therrien. Je vous remercie de votre service public. Prenez soin de vous.

Le président: Merci, monsieur Erskine-Smith.

[*Français*]

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

M. René Villemure: Je vous remercie, monsieur le président.

Monsieur Therrien, diriez-vous que la GRC a développé une culture de protection de la vie privée?

M. Daniel Therrien: La GRC a une culture d'application de la loi telle qu'elle est.

Il est vrai, comme cela a été dit, que la GRC n'a pas d'expertise particulièrement élevée en ce qui a trait à la vie privée. Au cours de la dernière année de mon mandat, j'ai noté une volonté, de la part de la GRC, d'augmenter les connaissances liées à la vie privée, mais ce n'est pas son réflexe premier.

M. René Villemure: Nous sommes sur le bon chemin.

N'est-ce pas?

M. Daniel Therrien: Oui.

M. René Villemure: Lors du précédent tour de questions, Mme Polsky a parlé des évaluations des facteurs relatifs à la vie privée en disant que c'est quelque chose que nous pouvons faire, mais que, en fin de compte, cela ne donne peut-être rien.

Êtes-vous d'accord sur cette affirmation?

M. Daniel Therrien: C'est un peu pour cela que je vous encourage non seulement à prévoir l'obligation, sur le plan juridique, de mener des EFVP, mais aussi à inscrire dans la loi le contenu et le but de ces évaluations.

Il y a un risque réel. J'ai vu beaucoup de cas où les évaluations sont un exercice purement mécanique, ce qui ne sert à rien. Le but, c'est de s'assurer que les programmes et les activités sont conçus de façon à respecter la vie privée et, au surplus, la vie privée comme un droit fondamental. Le but d'une évaluation, c'est d'être proactif.

M. René Villemure: Je vous remercie beaucoup.

Madame Polsky, en moins d'une minute, croyez-vous qu'il est temps d'entamer un débat public sur le sujet afin que les citoyens puissent mieux comprendre ce dont il est question?

[*Traduction*]

Mme Sharon Polsky: Absolument, et je pense que les Canadiens doivent être sollicités pour qu'ils puissent comprendre ce qui est en jeu non seulement sur le plan national, mais aussi sur le plan personnel. Encore une fois, je reviens à l'éducation, et c'est obligatoire, parce que sinon, ils n'ont pas le choix, que ce soit à titre personnel ou dans le cadre d'une entreprise ou d'un gouvernement, de croire sur parole un fournisseur ou quelqu'un d'autre, sans pouvoir avoir une pensée critique et poser les questions qui doivent être posées et savoir s'ils reçoivent des réponses légitimes.

[*Français*]

M. René Villemure: Je vous remercie beaucoup.

[*Traduction*]

Le président: Merci.

Nous passerons à M. Green pour deux minutes et demie.

M. Matthew Green: Merci.

J'aimerais revenir à la fin de ma dernière question. Je crois que M. Therrien était sur le point d'expliquer la façon dont nous pouvons combler l'écart entre les directives en matière de politique établies qui relèvent de la présidente du Conseil du Trésor dans le cadre de la Loi sur la protection des renseignements personnels et tous les conseils et les organismes, y compris les organismes d'application de la loi, pour commencer à mettre en place la culture axée sur la valeur sous-jacente du respect de la vie privée en tant que véritable droit fondamental.

M. Daniel Therrien: À ce chapitre, la Loi est essentielle. Au Canada, nous avons des politiques qui favorisent la protection de la vie privée, mais parfois, elles sonnent creux. C'est un exercice qui consiste à cocher des cases. Pour que les EFVP et la protection de la vie privée dès la conception aient un sens, pour que la vie privée soit reconnue comme un droit fondamental et que l'application de la loi soit adéquate, y compris les ordonnances et les amendes, les secteurs privé et public ne peuvent plus tenir de beaux discours sans assurer la protection de la vie privée.

Les politiques sont bonnes, mais elles doivent être soutenues par des normes juridiques sérieuses et une surveillance indépendante.

M. Matthew Green: C'est un sujet que nous abordons au Comité en si peu de temps, pour répondre à la récente utilisation de cette technologie particulière à la GRC. Je pense que, comme vous l'avez laissé sous-entendre, cela ne se limite pas à cela. Je pense qu'il est juste de dire que si la GRC utilise cette technologie, c'est probablement le cas au CST et au SCRS... bien qu'ils aient des contraintes et des exigences différentes.

Une chose que nous n'avons pas abordée, c'est la possibilité pour le gouvernement de faire indirectement ce qu'il ne peut pas faire directement. Pourriez-vous finir en commentant les façons dont nous pourrions nous assurer que notre gouvernement n'utilise pas, même si c'est peut-être légal — je dirais même contraire à l'éthique — des renseignements illégaux, obtenus de manière illégale de nos partenaires étrangers dans le cadre de la sécurité internationale avec les organismes canadiens?

● (1250)

Le président: Veuillez répondre très rapidement si vous le pouvez, car nous n'avons plus de temps.

M. Daniel Therrien: Je répondrai au sujet du secteur privé. Dans l'enquête du Commissariat à la protection de la vie privée du Canada sur la reconnaissance faciale, nous recommandons que la Loi soit précisée, que le gouvernement, l'État, ne puisse pas faire indirectement, par l'intermédiaire du secteur privé, ce qui ne peut pas faire directement. Je pense que c'est une grande partie de la réponse.

M. Matthew Green: Merci.

Le président: Merci.

Pour les deux dernières séries de questions, nous allons céder la parole à M. Kurek pour cinq minutes, suivi de Mme Khalid.

M. Damien Kurek: Merci beaucoup.

Monsieur Therrien, les mandats d'écoute électronique utilisés par les organismes d'application de la loi, en vertu du Code criminel, sont-ils automatiquement sous scellés?

M. Daniel Therrien: Je pense qu'ils sont généralement mis sous scellés. Cela dépasse un peu mon domaine d'expertise, mais ils sont certainement scellés de manière générale.

M. Damien Kurek: D'accord. Merci beaucoup.

Madame Polsky, nous avons aujourd'hui entendu quelques témoignages très intéressants; je vais donc vous poser une série de questions. L'une concerne la lettre que la commissaire de la GRC avait envoyée au Comité refusant de communiquer certains renseignements que le Comité avait demandés. Cela vous inquiète-t-il?

Mme Sharon Polsky: Oui, beaucoup. Mon avis, en tant que Canadienne et en tant que contribuable, c'est que le gouvernement et nos organismes d'application de la loi sont là pour servir le public, pas pour s'en cacher. Ils ne semblent pas dignes de confiance. La confiance doit être méritée. Refuser catégoriquement de comparaître devant un comité parlementaire et dire non... c'est surprenant. Cela me pousse à me demander s'ils cachent quelque chose.

M. Damien Kurek: D'accord. Je comprends.

Hier, le ministre n'a pas été franc, quand certains d'entre nous, y compris moi, lui avons posé des questions concernant le recours aux exceptions au titre de la sécurité nationale. Est-il préoccupant pour vous que le ministre responsable de ces organismes ne soit pas franc sur la question de savoir si des exceptions ont été ou non utilisées pour contourner certaines des procédures judiciaires prévues par le Code criminel?

Mme Sharon Polsky: Ce qui est certainement préoccupant, c'est le manque de clarté. Cela semblait simplement vague.

M. Damien Kurek: Étant donné qu'il y a des questions liées à l'intégrité opérationnelle et à la garantie que l'intégrité des enquêtes soit maintenue, et que l'actuel et l'ancien commissaire à la protection de la vie privée ont tous deux expliqué que des mesures de protection étaient en place, pensez-vous qu'il est préoccupant que, pour ce qui est de cette question et aussi d'autres domaines antérieurs, la GRC n'ait répondu à des préoccupations en matière de protection de la vie privée qu'après un tollé du Parlement ou des médias concernant des choses comme les outils d'enquête sur appareil, Clearview AI, pour ce qui est de la reconnaissance faciale et ce genre de chose?

Mme Sharon Polsky: Je pense que le problème est qu'ils ne collaborent pas à l'avance avec le Commissariat à la protection de la vie privée du Canada; ils le font seulement après qu'ils sont pris la main dans le sac. Je pense que, en n'étant pas francs, ils ne se rendent pas service à eux-mêmes ni à tous les organismes d'application de la loi dans tout le pays.

Cela les met également sur la défensive, s'ils ne disent pas « Nous devons utiliser ce type d'outil. » Cela ne donne aucune information sur l'enquête. Le fait d'être général comme cela ne mine pas les enquêtes. Cela ne révèle aucune information délicate. Il faut aider à éduquer le public sur la raison pour laquelle on a besoin de ce type d'outil particulier. Il ne faut pas attendre de se retrouver sur la sellette, puis esquiver, comme beaucoup d'entre eux l'ont fait hier.

● (1255)

M. Damien Kurek: En ce qui concerne les mesures spécifiques, madame Polsky, pensez-vous qu'il faut énoncer dans la loi sur la protection de la vie privée qu'il doit y avoir une divulgation proactive, plutôt que d'attendre que des comités parlementaires ou des journalistes doivent courir derrière la GRC ou d'autres entités du gouvernement pour tenter d'amener le public à comprendre certaines de ces préoccupations en matière de protection de la vie privée?

Mme Sharon Polsky: Oui. Il est nécessaire d'inclure cela dans la Loi. Cela doit être clair, et non pas ouvert à l'interprétation par toute organisation qui veut utiliser la Loi à son avantage, et pas par souci de clarté. Cependant, je mets en garde contre le fait de dire que nous avons un nouveau projet de loi, le projet de loi C-27, la loi sur l'intelligence artificielle et les données, et que cela la protégera. Ce n'est pas le cas, car toute organisation mandatée, si l'on veut, par le CST ou le SCRS, peut faire ce que le gouvernement ne peut pas faire.

Le président: Merci, madame Polsky.

M. Damien Kurek: Merci.

Le président: Nous terminerons par Mme Khalid pour ce groupe de témoins.

Allez-y pour les cinq dernières minutes.

Mme Iqra Khalid: Merci beaucoup, monsieur le président.

Encore une fois, merci aux témoins.

Monsieur Therrien, si vous le voulez bien, je poursuivrai avec vous.

Maintenant, nous avons entendu parler de la portée du logiciel espion, de son utilisation et de sa nature intrusive, non seulement dans le cas des Canadiens, mais des gens en général. L'Union européenne a été impliquée par exemple dans la mise en place de Pegasus... disant qu'il viole des droits. Pensez-vous que des Canadiens doivent pouvoir vendre à quiconque un logiciel espion comme Pegasus? Par exemple, j'ai mentionné dans mes précédentes questions le groupe Awz. Des organisations comme celles-ci devraient-elles pouvoir vendre cette technologie extrêmement intrusive? Le gouvernement devrait-il réglementer non seulement l'utilisation de cette technologie dans notre pays, mais également la vente de celle-ci à l'étranger?

M. Daniel Therrien: Oui, il devrait y avoir des lois pour réguler la vente, l'importation et l'exportation de ces technologies. Doivent-elles être complètement interdites? Nous constatons dans cette étude qu'il pourrait y avoir des cas rares où l'intérêt du public permettrait à l'État d'utiliser cette technologie, mais il doit absolument y avoir des lois concernant la vente, l'importation et l'exportation.

Soit dit en passant, même si le gouvernement, l'État et la police ont des motifs légitimes d'utiliser exceptionnellement ce type de technologie avec une autorisation judiciaire, je ne trouve vraiment aucune raison valable pour laquelle une personne du secteur privé devrait pouvoir utiliser cette technologie. Je n'ai peut-être pas suffisamment d'imagination, mais je ne trouve aucune raison convaincante pour laquelle le secteur privé devrait pouvoir l'utiliser.

Mme Iqra Khalid: Je vous remercie beaucoup.

Je sais que certains des députés ont parlé de l'obligation d'un ministre de rendre des comptes et de sa responsabilité, par exemple, de superviser le travail de la GRC. Vous avez dit que les décisions opérationnelles ne sont pas prises par les ministres, et que, en fait, ils n'y participent pas.

Pourriez-vous peut-être nous en dire davantage sur l'importance de cette division ou séparation des pouvoirs et des responsabilités?

M. Daniel Therrien: La Cour suprême a certainement une jurisprudence sur la notion d'indépendance de la police, qui définit les limites de l'influence politique sur le travail des forces de police. En même temps, j'ai laissé entendre qu'il pourrait y avoir certaines prescriptions légales applicables à la police, par exemple, à l'aide de la Loi sur la protection des renseignements personnels. La partie VI du Code criminel, qui a été souvent mentionnée, comporte des exigences en matière de transparence imposées au gouvernement par la Loi, et elles incluent donc la police. Vous voulez peut-être consulter ces exigences relatives à la transparence pour voir si elles doivent être améliorées. Elles sont bonnes, mais elles sont probablement perfectibles.

Mme Iqra Khalid: Merci beaucoup de cette réponse.

La dernière question que je veux vous poser concerne la partie de la motion qui semble insinuer que la GRC met sur écoute ou surveille les députés.

Compte tenu de votre grande expérience au Commissariat à la protection de la vie privée et ailleurs, hypothétiquement, si des députés étaient de connivence avec d'autres pour planifier ou mener des activités illégales au Canada — par exemple, s'ils avaient travaillé avec le convoi qui a occupé Ottawa pendant deux ou trois semaines —, y aurait-il une autre sorte de privilège parlementaire qui empêcherait la GRC d'assurer la surveillance, y compris au moyen des outils d'enquête sur appareil, si une ordonnance d'un tribunal a été obtenue de manière adéquate?

● (1300)

M. Daniel Therrien: Personne n'est au-dessus de la loi, tous les Canadiens sont donc soumis à la loi, y compris au droit pénal, et peuvent faire l'objet d'enquêtes.

Je pense que les responsables de la GRC ont dit hier que, bien que ce soit une possibilité, il existe des mécanismes internes pour s'assurer que la surveillance d'un député nécessite l'autorisation d'une instance supérieure au sein de la GRC. Je ne sais pas si des députés sont surveillés de cette façon, mais certainement, en principe, personne n'est au-dessus de la loi.

Mme Iqra Khalid: Merci beaucoup de cette réponse, monsieur Therrien.

Le président: Merci. Votre temps est écoulé.

Tout d'abord, j'aimerais remercier nos deux témoins et les laisser partir maintenant.

Nous avons maintenant un peu de temps pour traiter quelques travaux du Comité, mais avant cela, les analystes ont demandé à avoir deux ou trois minutes pour m'informer; je vais donc suspendre la séance. Nous allons rester sur cet appel pour que la séance demeure publique. La séance est toujours en cours, mais je suspends les travaux.

● (1300)

_____(Pause)_____

● (1305)

Le président: Nous reprenons nos travaux; j'invite donc tout le monde à retourner à sa place.

J'ai ici quelques notes concernant cette étude qui pourraient même toucher la façon dont nous poursuivrons le reste de notre journée aujourd'hui.

Les analystes m'ont informé des contraintes de production liées à la préparation d'un rapport pour se conformer aux délais énoncés dans la motion que nous avons adoptée en juillet, alors nous terminerons l'étude aujourd'hui. Ce sera le dernier jour pour entendre les témoignages concernant cette étude.

Le délai le plus court pour obtenir une ébauche du rapport en vue d'un examen par le Comité est le 12 septembre. Nous nous sommes engagés dans notre motion à déposer le rapport la semaine suivante.

La semaine du 12 septembre est une semaine très difficile pour au moins quatre des membres du Comité en ce qui concerne la disponibilité. Autrement, je suis sûr que ce serait une excellente semaine pour nous. En fait, je pense qu'il nous sera très difficile de présenter ce rapport dans le respect des délais de la motion. Mon intention, en tant que président, serait de convoquer, à ma discrétion, les réunions appropriées pour que nous puissions faire de notre mieux pour présenter le rapport au Parlement dès que possible, compte tenu des contraintes qu'auront les analystes et l'équipe de production ainsi que les services de traduction et, peut-être des contraintes de certains des membres du Comité cette semaine-là.

Nous devrions peut-être tenir une réunion la semaine du 12 avant la reprise des travaux du Parlement. Nous verrons.

En ce qui concerne les instructions relatives à la rédaction, je demanderai aux membres de communiquer aux analystes, par l'intermédiaire du greffier, toute instruction particulière qu'ils pourraient avoir. De cette façon, nous pouvons peut-être nous passer d'une réunion consacrée à la production de documents.

Je ne suis pas sûr que l'on puisse débattre de ce sujet. Je sais que les membres pourraient vouloir se prononcer sur la façon de traiter les motions également.

Je vois que c'est le cas de M. Green et de Mme Khalid.

Allez-y, monsieur Green.

● (1310)

M. Matthew Green: Merci.

Je pense que nous recevons de très bonnes informations ici. En fait, dans son témoignage d'hier, le sous-commissaire de la GRC s'est porté volontaire pour nous fournir l'évaluation des facteurs relatifs à la vie privée, et il en est même ressorti qu'ils seraient disposés à nous communiquer plus d'information à huis clos.

Vous remarquerez dans ma réponse d'hier qu'il pourrait être utile à notre étude de permettre que l'évaluation nous parvienne et que nous ayons la possibilité de réexaminer la discussion à huis clos pour apprécier la transparence et la franchise des décisions qui ont été prises et la façon dont les responsables sont arrivés à ces décisions.

Monsieur le président, je pense que, sans cela, il nous manquera une importante composante de cette étude, et nous devrions alors revenir avec une sorte d'amendement ou la reprendre. Sur le plan de la procédure, je pense qu'il serait plus facile de trouver un moyen d'ajourner, d'interrompre ou de suspendre la séance, quel que soit le terme approprié sur le plan de la procédure, jusqu'à ce que nous recevions cette information et que nous soyons en mesure de formuler nos dernières conclusions en ce qui concerne la rédaction du rapport final.

Le président: Merci.

Madame Khalid, allez-y.

Mme Iqra Khalid: Merci, monsieur le président. Je vous en suis reconnaissante.

Je suis d'accord avec vous pour ce qui est du temps. Je suis consciente des difficultés qu'auront nos analystes. Je suis également consciente des efforts qu'ils déploient pour s'assurer que nous sommes bien soutenus dans le travail que nous faisons.

Je me demande s'il serait faisable que nous tenions cette réunion supplémentaire et que nous prolongions le délai de présentation des documents peut-être à la fin de la première semaine de notre retour, la semaine du 19 septembre. Je pense que cela serait très pratique et conviendrait à tous nos emplois du temps et que cela donnerait également assez de temps à nos analystes pour mettre tout cela en place.

J'aimerais avoir votre avis à ce sujet, monsieur le président.

Le président: Le problème avec cela — et nous sommes libres de changer d'avis et de revoir les décisions que nous avons prises —, c'est que le Comité a pris la décision de présenter le rapport au Parlement cette semaine-là. C'est pourquoi je soulève la question maintenant, car je constate qu'il nous sera difficile de respecter ce que nous nous sommes engagés à faire, et que nous ne serions peut-être pas en mesure de présenter rapidement le rapport, si nous attendions jusqu'à cette semaine-là pour demander aux analystes de produire l'ébauche ou travailler sur celle-ci.

Je cède la parole à M. Bezan, puis à M. Villemure.

M. James Bezan: Monsieur le président, je dirai simplement que, d'après le témoignage que nous avons entendu et les conversations que M. Green a eues avec la GRC, je pense qu'il serait utile de tenir quelques séances à huis clos pour obtenir plus de détails. Je pense également que, à en juger d'après le témoignage d'hier, il se peut que le SCRS et d'autres organismes policiers au pays, le CST et le ministère de la Défense nationale utilisent aussi cette technologie, et nous voulons peut-être les entendre.

Plutôt que d'être astreints à une contrainte temporelle, et je m'en remettrai à M. Villemure qui a proposé la motion... nous devrions peut-être envisager de prolonger cette étude plutôt que de nous empresser de déposer le rapport. Je pense que c'est une chose que nous devons approfondir, surtout que nous commençons à parler des évaluations des facteurs relatifs à la vie privée, de mettre à jour le Code criminel pour nous assurer que les mandats sont suffisants ou d'établir s'ils doivent être améliorés pour aborder la question des outils d'enquête sur appareil.

Nous devons également parler des applications commerciales de cette technologie et de la question de savoir si, d'après les divers fournisseurs qui existent, nous devrions ou non peut-être en entendre quelques-uns également, et savoir qui utilise leur technologie et si elle est téléchargée par des acteurs malveillants, s'ils font partie de l'État ou du secteur privé et comment cela pourrait potentiellement avoir des répercussions sur notre vie privée en tant que Canadiens.

● (1315)

Le président: Merci.

Cela pourrait être la direction que nous allons adopter.

Sachez que plus l'on ajoute de réunions, plus il faudra de temps pour arriver à l'ébauche.

M. James Bezan: Je comprends.

Le président: Tant que tout le monde le comprend, car c'est le conflit qui existe dans la motion actuelle qui prévoit la tenue de notre étude.

Allez-y, monsieur Villemure.

[*Français*]

M. René Villemure: Je vous remercie beaucoup, monsieur le président.

Je crois que les deux jours de témoignages nous ont appris bien des choses. Nous avons beaucoup d'éléments à inclure dans un éventuel rapport. Cependant, la bonne volonté des gens de la GRC et le fait qu'ils sont disposés à revenir après avoir fait l'évaluation des facteurs relatifs à la vie privée sont incontournables. Nous ne pouvons pas clore notre travail si nous ne voyons pas cela.

Je ne suis pas certain que nous devons aller dans toutes les ramifications mentionnées par M. Bezan. Je crois que notre travail serait assurément incomplet si nous ne prenions pas la main que nous tend la GRC, pour une fois qu'elle nous la tend.

[*Traduction*]

Le président: Merci.

Si je puis me permettre, je retiendrais de cette discussion qu'il y a un consensus pour tenir des réunions supplémentaires, particulièrement une réunion à huis clos, et ne pas s'empresser de préparer le rapport et de le présenter à la Chambre. S'il y a un consensus à cet égard, je considérerai alors que c'est réglé et que la prochaine réunion se tiendra à la demande du président, au besoin.

Monsieur Bezan, vous avez la parole.

M. James Bezan: Monsieur le président, avec cela, je souhaiterais de nouveau déposer ma motion d'hier. Je la lirai aux fins du compte rendu:

> Que, conformément à la motion adoptée par le comité le 26 juillet 2022, le comité réitère sa demande de tous les documents décrits dans sa motion initiale; que tous les documents reçus de la GRC, y compris les mandats, les listes de mandats, la portée des mandats et les affidavits soumis à l'appui des demandes de mandats, soient étudiés par le comité à huis clos seulement, et selon les paramètres suivants : que tous les documents émis en vertu de cette motion soient fournis au bureau du légiste et du conseiller parlementaire dans les 15 jours suivant l'adoption de cette ordonnance; que tous les documents pertinents soient étudiés par le légiste et le conseiller parlementaire dans les sept jours suivant leur réception, afin de déterminer s'ils contiennent des renseignements personnels s'ils sont liés à des opérations policières en cours ou à la sécurité nationale; que tous les documents soient distribués aux membres du comité, dans les plus brefs délais, après avoir été étudiés.

Encore une fois, je rappellerai à mes collègues qu'il ne s'agit pas d'une chasse aux sorcières. Le but est de tenter de comprendre les mécanismes en cause et les circonstances dans lesquelles les mandats sont utilisés pour les outils d'enquête sur appareil, et il faut davantage examiner cette technologie. Nous pouvons le faire dans le cadre du processus de documentation, mais je ne veux pas porter atteinte aux droits à la protection de la vie privée des gens. Je ne veux pas miner les enquêtes actuelles auxquelles participe actuellement la GRC ni soulever des informations considérées comme représentant un risque pour la sécurité nationale. Nous tentons de nous assurer que le légiste et le conseiller parlementaire puissent accéder à ces documents, les caviarder, les vérifier et nous fournir seulement l'information dont nous avons besoin pour notre étude.

Le président: Merci.

Madame Khalid, vous avez la parole.

Mme Iqra Khalid: Merci beaucoup, monsieur le président.

Bien que je comprenne l'importance de cette motion, j'aimerais proposer un amendement. L'amendement a été envoyé par courriel aux adresses électroniques personnelles de tous les membres. Je le lirai aux fins du compte rendu:

> Que la motion soit modifiée par adjonction, après les mots « motion initiale », de ce qui suit : « à l'exception des mandats sous scellés ».

Monsieur le président, la raison pour cela, c'est que l'ordonnance de mise sous scellés est faite par un juge. Si un juge a pris la décision de mettre sous scellés un mandat, la GRC ne pourra pas le contester ou nous fournir cette information. Par conséquent, il n'est pas logique que nous essayions de tenir la GRC responsable d'une chose qu'elle ne peut simplement pas faire.

C'est une motion pratique. Évidemment, tous les documents énoncés par M. Bezan s'appliquent toujours. Je pense simplement que cet amendement est un détail technique visant à garantir que nous ne demandons pas à la GRC de faire une chose qu'elle ne peut pas faire.

● (1320)

Le président: Merci.

Quelqu'un veut-il intervenir au sujet de l'amendement?

Monsieur Bezan, vous avez la parole.

M. James Bezan: Je dirais simplement que je crois que l'article 187 du Code criminel prévoit que tous les documents relatifs à un mandat en vertu de la partie VI du Code criminel, qui comprend la vidéosurveillance et la mise sur écoute, soient automatiquement mis sous scellés; c'est donc une manière un peu détournée de s'assurer que tous les mandats ne soient jamais communiqués à notre comité. C'est du camouflage.

Le président: Madame Khalid, allez-y.

Mme Iqra Khalid: Monsieur le président, je m'oppose à ce que tout ce que nous faisons pour essayer d'équilibrer le travail du Comité soit appelé camouflage. Ce n'est absolument pas le cas. Ce que nous essayons de faire, c'est de nous assurer que la GRC, puisque ses représentants ont été disposés à nous parler, puisse continuer de nous fournir des documents d'une manière convenable. C'est très injuste que M. Bezan nous accuse de camouflage pour une très petite modification, qui en limite seulement la portée, pour que nous n'ayons pas à convoquer des commissaires à comparaître devant le Parlement et à les accuser de mépris, ou nous prêter à tout autre jeu que l'opposition pourrait vouloir jouer.

Le président: Je vois qu'il n'y a aucune autre intervention au sujet de l'amendement alors nous allons procéder de nouveau en mode hybride. Nous allons procéder à l'envers et demander si quelqu'un s'oppose à l'amendement.

M. James Bezan: Je vote contre.

Le président: Je vois qu'on est contre l'amendement. Nous allons demander au greffier de procéder à la mise aux voix de l'amendement.

Il y a égalité. Je votre contre.

(L'amendement est rejeté par 6 voix contre 5 [*Voir le Procès-verbal*]).

Le président: Nous revenons maintenant à la motion initiale.

Y a-t-il d'autres interventions sur la motion? Comme je n'en vois aucune, quelqu'un s'oppose-t-il à la motion?

Mme Iqra Khalid: Je m'y oppose, monsieur le président.

Le président: D'accord, je demanderais alors au greffier de mettre la motion aux voix.

Il y a égalité. Je vote en faveur de la motion.

(La motion est adoptée par 6 voix contre 5 [*Voir le Procès-verbal*]).

Le président: Il nous reste deux ou trois minutes, mais je pense, ou j'espère, que nous avons fini pour le moment. Nous serons de retour cet après-midi.

En fait, permettez-moi d'être clair à propos de cet après-midi. Nous aurons trois témoins qui comparaîtront ensemble dans un seul groupe. Selon le temps et si les membres ont épuisé toutes leurs questions, nous pourrions avoir un peu de temps à la fin. Nous nous arrêterons à 17 heures, si vous me le permettez, au cas où quelqu'un devrait voyager ou autre chose et partir à 17 heures.

Sur ce, la séance est levée.