CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

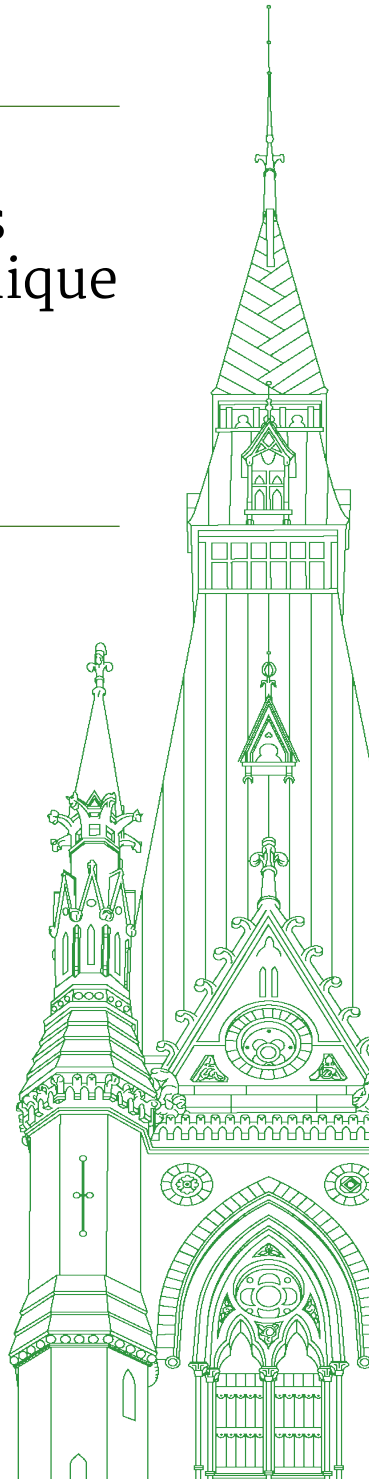
44e LÉGISLATURE, 1re SESSION

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

TÉMOIGNAGES

NUMÉRO 031

Le lundi 8 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 lundi 8 août 2022

● (1505)

[*Traduction*]

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

Nous demandons aux photographes qui ont un appareil photo de quitter la salle.

Bienvenue à la 31e réunion du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique. Conformément au paragraphe 108(3) du Règlement et à la motion adoptée par le Comité le mardi 26 juillet 2022, nous menons une étude des outils d'enquête sur appareil utilisés par la Gendarmerie royale du Canada, la GRC.

La réunion se déroulera selon une formule hybride, conformément à l'ordre adopté par la Chambre le jeudi 23 juin 2022.

La première heure de la réunion sera consacrée à l'honorable Marco Mendicino, conseiller privé, député et ministre de la Sécurité publique.

J'invite sans plus tarder le ministre, s'il est prêt, à nous transmettre ses remarques liminaires.

Monsieur le ministre, avez-vous un casque d'écoute approprié?

L'honorable Marco Mendicino (ministre de la Sécurité publique): Je me trouve au bureau régional du Québec et je me suis laissé dire que nous utilisons le matériel approuvé par le Bureau du Conseil privé. S'il y a un problème, veuillez m'en informer.

Le président: Je vais prendre quelques instants pour faire le tour des gens dans la salle et des interprètes. Entendez-vous bien le ministre?

Aucun problème signalé dans la salle, et aucune réaction non plus du côté des interprètes. Certaines personnes me font un signe de la tête. Tout semble bien fonctionner.

Sur ce, je vous remercie, monsieur le ministre. Vous pouvez nous présenter…

Mme Iqra Khalid (Mississauga—Erin Mills, Lib.): Je voudrais invoquer le Règlement, monsieur le président.

Le président: Je suis désolé, mais je dois entendre le rappel au Règlement avant que vous commenciez, monsieur le ministre.

Madame Khalid, vous souhaitez invoquer le Règlement?

Mme Iqra Khalid: Oui, monsieur le président. Je voudrais revenir sur notre dernière réunion. Vers la fin, le Comité a accepté de procéder à un dernier tour de questions et, à la demande d'un membre de l'opposition, monsieur le président, vous avez accordé cinq minutes à chaque intervenant pour ce tour supplémentaire. Ce n'était pas ce qui était prévu aux motions de régie interne.

J'aimerais relire une des motions de régie interne adoptées à l'unanimité par le Comité le 13 décembre 2021. Conformément à la motion présentée par la députée Lisa Hepfner, il a été convenu:

> Que cinq minutes soient accordées aux témoins pour leur déclaration d'ouverture; et que dans la mesure du possible, les témoins présentent leurs notes d'allocution au Comité 72 heures avant leur comparution; et que pendant l'interrogation des témoins, à la discrétion de la présidence, le temps alloué au premier tour de questions soit de six minutes pour le premier intervenant de chaque parti tel qu'il suit: Parti conservateur, Parti libéral, Bloc québécois, Nouveau Parti démocratique. Que pour le deuxième tour et les tours subséquents, l'ordre et le temps alloué à chaque intervenant soient répartis de la façon suivante: Parti conservateur, cinq minutes, Parti libéral, cinq minutes, Bloc québécois, deux minutes et demie…

Le président: Excusez-moi de vous interrompre, madame Khalid, mais je connais très bien la motion et son contenu. Je vous rappelle qu'au cours de la réunion, quand un membre m'a demandé d'ajouter un tour de questions de cinq minutes parce que nous avions terminé les trois premiers tours, j'ai cru comprendre que le Comité a donné son accord unanime pour que nous procédions comme je l'ai fait. J'ai simplement permis aux députés d'utiliser le temps restant à la fin d'une longue réunion pour poser d'autres questions, et j'ai alloué cinq minutes supplémentaires à chaque parti.

Je déduis de votre intervention que vous refuserez dorénavant toute dérogation à cette motion, et j'en prends bonne note. De toute façon, je ne crois pas que cette situation se représentera puisque l'ordre du jour des prochaines réunions est très chargé.

Est-ce que cela vous convient? Puis-je demander au ministre de nous présenter ses remarques?

Mme Iqra Khalid: Oui. Merci.

M. Matthew Green (Hamilton-Centre, NPD): J'aurais un rappel au Règlement, monsieur le président.

Le président: Désolé, il y a un autre rappel au Règlement.

Monsieur Green, allez-y.

M. Matthew Green: Le ministre nous a-t-il présenté ses remarques liminaires avant la réunion comme il est prévu dans le Règlement et les motions de régie interne?

Le président: Je n'ai rien reçu de tel. Je vais demander à la greffière si nous avons reçu quelque chose.

Effectivement, la greffière a reçu les remarques liminaires du ministre, mais elles ne semblent pas avoir été transmises aux députés. Personnellement, je ne les ai pas reçues. Le nécessaire sera fait pour les distribuer aussi rapidement que possible.

Merci, monsieur Green.

Sur ce…

Oui? Le temps que le ministre a à nous consacrer file, mais allez-y.

[*Français*]

M. René Villemure (Trois-Rivières, BQ): Nous ne voyons pas le ministre, monsieur le président.

L'hon. Marco Mendicino: Puis-je commencer, monsieur le président?

[*Traduction*]

Le président: Nous essayons de régler un problème technique…

L'hon. Marco Mendicino: Pas de souci.

Le président: Je crois que c'est un peu mieux. Il y avait bel et bien un problème, mais je crois qu'il a été réglé.

Monsieur le ministre, vous avez la parole.

L'hon. Marco Mendicino: Merci beaucoup, monsieur le président, et merci, chers collègues.

Je tiens d'abord à remercier le Comité pour ses études sur le croisement de la technologie et des services de police, y compris le rapport récent sur la technologie de reconnaissance faciale. Je me réjouis de l'occasion qui m'est donnée de parler de l'adoption de nouveaux outils et de nouvelles technologies, surtout en ce qui concerne la transparence, la protection de la vie privée et les normes juridiques et éthiques.

La technologie et les services de police ont toujours été étroitement liés mais, aujourd'hui, la technologie progresse de façon exponentielle.

● (1510)

[*Français*]

Cette progression s'étend de l'évolution de la technologie mobile et sans fil jusqu'à la superinformatique, à l'analyse avancée, à la biométrie, à la surveillance, à la criminalistique, et j'en passe.

Il est impératif que les organismes d'application de la loi suivent le rythme du changement. Cela est essentiel pour que nous puissions poursuivre ceux qui se servent des nouvelles technologies à des fins malveillantes.

Cela est nécessaire pour accroître l'efficacité, mais aussi pour examiner de près la façon dont les organismes d'application de la loi choisissent et mettent en œuvre ces technologies afin de garantir le respect de la vie privée et des droits et libertés des Canadiens. Nous devons trouver un juste équilibre.

[*Traduction*]

Pour ma part, chers collègues, je suis heureux de vous donner un aperçu des outils utilisés par la GRC.

La GRC utilise des technologies d'enquête et des outils scientifiques de pointe dans les domaines de la criminalistique, des empreintes digitales, des données biométriques et génétiques, et de la surveillance, entre autres. Par exemple, les Services des sciences judiciaires et de l'identité font partie intégrante des Services nationaux de police et s'appuient souvent sur des sciences et des technologies de pointe.

Grâce à ces services, une technologie révolutionnaire permet de détecter les preuves biologiques recueillies sur les scènes de crime, d'examiner les armes à feu, les pièces saisies et la fausse monnaie ou les pièces d'identité suspectes, de dépister un large éventail de drogues et de poisons, et de fournir des témoignages scientifiques d'experts devant les tribunaux.

En ce qui a trait plus particulièrement aux technologies d'enquête, les dernières technologies permettent à la GRC de relier les crimes entre eux, de sécuriser, d'enregistrer et de documenter les scènes de crime, d'identifier les suspects et les victimes et, en général, d'assurer la sécurité des Canadiens et des collectivités.

Le programme Équipe d'accès secret et d'interception de la GRC utilise une technologie approuvée pour recueillir des données qui ne peuvent être recueillies au moyen de techniques d'écoute téléphonique traditionnelles ou d'autres techniques d'enquête moins intrusives. Ce programme n'est utilisé que sur autorisation judiciaire pour les infractions les plus graves.

De plus, leur programme spécial « I » est principalement chargé du mandat de surveillance électronique légale de la GRC. Il s'agit de l'unité responsable de toutes les interceptions de communications privées qui peuvent être obtenues au titre de la partie VI du Code criminel. Il s'agit d'installations techniques et de déploiements d'équipement de surveillance électronique à l'appui des enquêtes policières. La surveillance et l'analyse des données et des communications qui ont été légalement interceptées en font aussi partie.

[*Français*]

Toutefois, chers collègues, pour tous ces exemples, je tiens à préciser que la transparence, la responsabilité, la protection de la vie privée ainsi que le respect des droits fondamentaux et de la loi sont primordiaux. Le commissaire à la protection de la vie privée fait écho à ces sentiments, et le gouvernement est déterminé à faire en sorte que cela soit fondamental pour toutes les activités, y compris la formation et les processus opérationnels.

En particulier, l'un des résultats principaux de l'enquête et du rapport du commissaire sur l'utilisation de la reconnaissance faciale était la nécessité d'un processus centralisé pour l'adoption de nouveaux outils et de nouvelles technologies.

En mars de l'année passée, la GRC a créé le Programme national d'intégration des technologies, ou PNIT.

[*Traduction*]

Le Programme national d'intégration des technologies, le PNIT, vise à centraliser, à normaliser et à rendre plus transparents les processus qui régissent la façon dont la GRC identifie, évalue, suit et approuve l'utilisation des nouvelles technologies et des outils d'enquête. Il sera le premier point de contact pour tout service intéressé par l'utilisation d'une nouvelle technologie opérationnelle. Il veillera à ce qu'une évaluation approfondie de la technologie soit effectuée, en s'assurant qu'elle respecte toutes les normes en matière de confidentialité, de droit et d'éthique.

Le PNIT a commencé à accepter de nouvelles technologies à des fins d'évaluation et continuera d'augmenter sa capacité à mesure qu'il deviendra pleinement opérationnel.

Je tiens à souligner que la GRC collabore pleinement avec le Commissariat à la protection de la vie privée pour s'assurer que les répercussions sur la vie privée sont évaluées pour toutes les nouvelles utilisations de la reconnaissance faciale envisagées.

Les considérations juridiques sont également prises en compte pour l'utilisation de la technologie à toutes les étapes, notamment par l'application du Code criminel, qui prévoit des dispositions pour l'autorisation judiciaire et exige que nous fassions un rapport annuel au Parlement sur l'utilisation de la surveillance électronique.

Compte tenu du mandat de la GRC et de la nécessité de préserver sa capacité à utiliser efficacement les outils d'enquête sur appareil, nous ne sommes pas en mesure de discuter de certains détails techniques ou opérationnels de ces outils. Toutefois, je peux confirmer que la GRC recourt à ces outils uniquement pour des raisons d'intégrité opérationnelle et de sécurité.

Je comprends qu'il y a des contraintes de temps et je m'arrête ici. Je répondrai volontiers aux questions du Comité.

● (1515)

Le président: Effectivement, mais je vous ai quand même laissé quelques secondes de plus pour conclure. Merci, monsieur le ministre.

Je donne la parole à M. Bezan. Vous disposez de six minutes.

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

Je remercie le ministre Mendicino de participer à notre réunion.

Monsieur le ministre, quand avez-vous entendu parler la première fois de l'utilisation par la GRC d'outils d'enquête sur appareil similaires à la technologie Pegasus?

L'hon. Marco Mendicino: Tout d'abord, je tiens à ce que les membres du Comité comprennent bien que la technologie Pegasus n'est pas utilisée par la GRC. Il faut que ce soit bien clair.

M. James Bezan: Quelle technologie utilisez-vous?

L'hon. Marco Mendicino: Ensuite, comme je l'ai mentionné à la fin de mes remarques, monsieur Bezan, certaines techniques d'enquête doivent rester confidentielles. C'est essentiel pour préserver l'intégrité des opérations et traduire les suspects en justice, le cas échéant. Tout cela se fait dans le respect de la Charte et des droits à la vie privée.

M. James Bezan: Avez-vous donné des directives pour mieux encadrer l'utilisation des outils d'enquête sur appareil par la GRC, le SCRS et d'autres organismes fédéraux?

L'hon. Marco Mendicino: C'est une excellente question, monsieur Bezan.

Le Code criminel impose des exigences en matière de responsabilité très strictes, notamment quant aux faits que la GRC peut invoquer pour obtenir l'autorisation judiciaire de recourir à ce genre de technique. D'autres mécanismes de protection font en sorte que seuls les agents désignés peuvent soumettre ce genre de demande au tribunal. Nous devons aussi présenter un rapport annuel au Parlement. Bien évidemment, j'examinerai toutes les suggestions que me fera le Comité dans le cadre de son étude.

M. James Bezan: Merci.

Cette technologie est-elle utilisée par l'ASFC, le SCRS ou d'autres agences fédérales qui relèvent de votre compétence?

L'hon. Marco Mendicino: Je tiens à réitérer que nous n'utilisons pas Pegasus, mais que nous utilisons bel et bien cette technique, en effet.

M. James Bezan: Depuis combien de temps le ministère de la Sécurité publique recourt-il à cette technique par l'intermédiaire de ses diverses agences?

L'hon. Marco Mendicino: À ma connaissance, la technique a commencé à être utilisée aux alentours de 2017, mais je crois que les représentants de la GRC qui sont en ligne pourraient vous donner une réponse plus précise.

M. James Bezan: Ils sont dans la salle. Ils pourront nous donner ces précisions tout à l'heure.

Mon expérience à la Défense nationale m'a appris que le ministre responsable peut en tout temps donner des instructions et des autorisations s'il est impossible d'obtenir un mandat parce qu'il est trop tard le soir ou la nuit, ou parce que c'est la fin de semaine. Avez-vous la compétence… À titre de ministre de la Sécurité publique, avez-vous également le pouvoir de donner à la GRC l'instruction de mener une mission de surveillance visant des Canadiens?

L'hon. Marco Mendicino: Je vous remercie de soulever cette question. Elle va me permettre de réitérer l'importance de l'indépendance opérationnelle.

Les représentants élus ne mènent pas d'enquêtes criminelles, et il ne leur appartient pas d'attribuer… [*Inaudible*]… les techniques d'enquête qui doivent être…

M. James Bezan: À titre de ministre responsable d'une agence, pouvez-vous donner une autorisation ministérielle s'il n'existe pas de capacité ou de possibilité… Par exemple, en cas de menace imminente pour la sécurité nationale, pouvez-vous autoriser une demande de mandat judiciaire pour effectuer une surveillance?

L'hon. Marco Mendicino: Monsieur Bezan, comme vous le savez, c'est la GRC qui peut demander ce genre d'autorisations, et le tribunal peut octroyer ce pouvoir au terme d'un processus rigoureux et sur la foi d'un affidavit présenté par un agent désigné.

M. James Bezan: Monsieur le ministre, ces outils d'enquête sur appareil ont-ils été utilisés pendant que la Loi sur les mesures d'urgence était en vigueur?

L'hon. Marco Mendicino: Pas à ce que je sache. Cela dit, et je me répète, les représentants des forces de l'ordre seront mieux placés que moi pour vous donner des détails d'ordre opérationnel.

M. James Bezan: Nous allons y revenir.

Comme vous le savez, la Défense nationale a fait des exercices d'entraînement en survolant le centre-ville d'Ottawa avec un avion King Air durant les manifestations. Des agents de la GRC ou du SCRS se trouvaient-ils à bord des avions pour surveiller les gens au sol durant ces soi-disant exercices d'entraînement?

L'hon. Marco Mendicino: Monsieur Bezan, je vous invite à nouveau à poser vos questions d'ordre opérationnel directement aux représentants des forces de l'ordre.

M. James Bezan: Quels renseignements avez-vous reçus concernant l'activation à distance de microphones et de caméras intégrés à des appareils mobiles par la GRC?

● (1520)

L'hon. Marco Mendicino: J'ai eu des discussions avec la GRC et les gens de mon ministère. J'ai aussi lu en détail le dernier rapport annuel sur l'utilisation de la surveillance électronique, déposé en 2020. Un autre rapport sera soumis sous peu pour 2021. C'est un des différents mécanismes mis en place pour assurer l'ouverture et la transparence à l'égard du public relativement au recours à cette technique d'enquête.

M. James Bezan: Comme nous le savons, Pegasus… Même si vous affirmez que la technologie Pegasus n'est pas utilisée au Canada, des agents étatiques y ont eu recours contre des politiciens dans d'autres pays, mais également contre des journalistes et des défenseurs des droits de la personne. Les États-Unis ont notoirement interdit l'utilisation de Pegasus sur leur territoire par suite d'un ordre de la Maison-Blanche et de l'intervention du Congrès.

Comment pouvez-vous nous assurer que les logiciels espions utilisés par la GRC et d'autres agences gouvernementales ne tomberont pas entre les mains d'agents étatiques mal intentionnés ici, au Canada?

L'hon. Marco Mendicino: Je vous remercie de poser cette autre excellente question, monsieur Bezan, et je peux vous assurer qu'elle a déjà été adressée aux responsables. Ils m'ont répondu que les services relevant de mon portefeuille n'utilisent pas cette technologie. J'ajouterai en terminant que des mécanismes de protection très stricts sont appliqués avant que l'utilisation de cette technique soit autorisée. Plus précisément, un agent désigné doit soumettre la demande à un juge d'une cour supérieure et l'appuyer par un exposé des faits détaillé.

Le président: Merci, monsieur le ministre, et merci, monsieur Bezan.

Je donne maintenant la parole à Mme Hepfner. Vous disposez de six minutes.

Mme Lisa Hepfner (Hamilton Mountain, Lib.): Merci, monsieur le président. Par votre entremise, je remercie le ministre de se joindre à nous cet après-midi.

Monsieur le ministre, lorsque j'étais journaliste, j'ai eu l'occasion de couvrir des procès pour actes terroristes. Corrigez-moi si je me trompe, mais je crois que durant votre ancienne vie de procureur, vous êtes intervenu dans des affaires de terrorisme et que, selon l'information que la GRC a fournie au Comité, le terrorisme fait partie de la poignée d'actes criminels contre lesquels elle recourt à cette technologie.

Pouvez-vous nous dire, d'après votre expérience, pourquoi la police pourrait être justifiée d'utiliser cette technologie lorsque les circonstances s'y prêtent et pourvu qu'elle se conforme aux protocoles et aux mécanismes de contrôle voulus?

L'hon. Marco Mendicino: Merci de poser cette question, madame Hepfner. J'ai rarement l'occasion de comparer des expériences tirées d'une ancienne profession dans le contexte que vous venez d'évoquer, soit les vôtres à titre de journaliste et les miennes à titre de procureur fédéral.

J'ai effectivement une bonne connaissance du processus rigoureux qui est suivi avant d'autoriser le déploiement de ce genre de technique de surveillance électronique. Cette autorisation est loin d'être facile à obtenir. Il faut franchir de multiples étapes, comme je l'ai expliqué dans mes réponses à M. Bezan.

Tout d'abord, la demande doit être soumise à un juge d'une cour supérieure, qui procédera à un examen très minutieux des faits afin d'y déceler des éléments de preuve ou d'information indiquant qu'une infraction très précise a été commise. Je tiens à souligner que, contrairement à ce que vous semblez sous-entendre dans votre question, l'autorisation d'utiliser ce genre d'outil d'enquête ou de faire de l'écoute électronique ne peut pas être demandée pour n'importe quelle infraction criminelle. La liste restreinte des infractions très graves pour lesquelles cette technique peut être autorisée figure à la partie VI du Code criminel.

Le juge doit ensuite peser différentes considérations et établir si, entre autres choses, l'interception ou l'utilisation d'une technique quelconque est justifiée et suffisamment pressante ou urgente pour autoriser l'État à y recourir en vue d'obtenir de l'information qui sera éventuellement déposée à titre de preuve dans une procédure pénale.

J'insiste sur l'attention accordée au détail. Il n'est pas rare qu'un tribunal demande aux agents de répondre à certaines questions avant de leur accorder l'autorisation sollicitée, justement parce que la priorité est toujours accordée à la protection de la vie privée, des droits des particuliers à cette vie privée, de même que des autres droits garantis par la Charte.

Le Code criminel prévoit un bon nombre de mécanismes de protection qui assurent l'équilibre entre le besoin de l'État d'avoir à sa disposition les outils requis pour protéger la sécurité et la paix des Canadiens sans brimer les droits que leur garantit la Charte.

● (1525)

Mme Lisa Hepfner: Vous avez dit, je crois, qu'un juge n'accorderait pas de tels mandats si la police disposait d'autres moyens de recueillir l'information voulue. C'est un moyen de dernier recours.

L'hon. Marco Mendicino: C'est exact. C'est le principe de la nécessité pour les besoins de l'enquête qui s'applique. Il faut que l'État fasse la démonstration, ou plus exactement que les forces de l'ordre fassent la démonstration, que tous les autres moyens possibles ont été épuisés avant de soumettre une demande d'autorisation judiciaire au titre de la partie VI. Cela comprend certaines des techniques visées par l'étude du Comité. Elles ne sont jamais considérées comme un premier recours ou comme un expédient. Ces techniques doivent être essentielles pour faire avancer une enquête et doivent être utilisées en dernier recours, puisqu'il est primordial de protéger la vie privée des gens.

Mme Lisa Hepfner: La surveillance de masse semble susciter beaucoup d'inquiétude. Comment pouvons-nous savoir si elle a eu lieu ou non? Comment nous assurer que la surveillance de masse, qui comme vous l'avez mentionné est interdite, est [*difficultés techniques*]?

L'hon. Marco Mendicino: C'est une question d'une grande importance. J'espère vraiment que votre étude et que le travail des membres du Comité contribueront à améliorer l'ouverture et la transparence concernant l'utilisation de ces techniques par les forces de l'ordre.

J'ajouterai qu'actuellement, le principal défi pour tous les agents étatiques chargés de protéger les Canadiens vient des méthodes de plus en plus complexes de chiffrement qui sont utilisées pour déjouer les forces de l'ordre et les moyens de détection. Des risques et des conséquences sont liés à ces technologies de chiffrement extrêmement perfectionnées puisqu'elles permettent à des individus de commettre impunément des crimes au détriment de la santé et de la sécurité des Canadiens.

Comme nous l'avons vu, certaines techniques ont pour seul objectif de contrer les efforts d'organisations criminelles complexes et d'autres agents, étatiques ou non, afin de protéger les Canadiens. Votre étude permettra certainement de réaliser des progrès en levant le voile sur ces techniques, et j'en dirais autant des rapports annuels sur l'utilisation de la surveillance électronique. J'invite de nouveau le Comité à prendre connaissance de ce rapport et à soumettre ses suggestions pour nous permettre de continuer à apporter les améliorations nécessaires. Je vous recommande aussi de vous intéresser au travail mené par les forces de l'ordre par l'entremise du Comité des parlementaires sur la sécurité nationale et le renseignement, le CPSNR, et de l'Office de surveillance des activités en matière de sécurité nationale et de renseignement, l'OSSNR. Tout ce travail contribuera à une transparence et à une ouverture accrues relativement à l'utilisation prudente et en dernier recours, je le répète, de ces techniques pour protéger la santé et la sécurité des Canadiens.

Mme Lisa Hepfner: Merci.

Je crois que mon temps est écoulé, monsieur le président.

Le président: En effet. Je vous remercie.

[*Français*]

Monsieur Villemure, vous avez la parole pour six minutes.

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

Monsieur le ministre, je vous remercie beaucoup d'être avec nous aujourd'hui.

Nous parlons d'une question de confiance. Je me demande ce que nous devons penser des révélations qui ont été faites par *La Presse* et le média web Politico.

Quel est l'effet de ces révélations sur la confiance des gens envers le ministère ou la GRC?

Vous nous dites que la GRC est pleinement engagée à l'égard du commissaire à la protection de la vie privée, mais, ce matin, ce dernier semblait nous dire que cet organisme ne l'était pas tant que cela.

Quel est l'effet cumulatif de cette situation sur la population?

L'hon. Marco Mendicino: Je vous remercie de la question.

Je suis totalement d'accord avec vous pour dire que la confiance est l'une des clés de l'ouverture et de la transparence.

Je remercie le Comité d'entreprendre cette étude. Cela va nous donner l'occasion d'étudier les technologies et les techniques utilisées par les services policiers, y compris la GRC.

Comme je l'ai déjà mentionné, monsieur le député, il y a beaucoup de défis sur le terrain en ce moment, dans un contexte géopolitique où des organisations criminelles utilisent le chiffrement pour contrecarrer les efforts des services policiers.

Cette étude est donc une importante occasion d'augmenter la transparence et de déterminer comment ces techniques sont utilisées par la GRC. Cela va contribuer à raffermir la confiance des gens.

M. René Villemure: C'est un fait, la technologie évolue rapidement. Il faut tenter de baliser quelque chose qui ne l'est pas.

L'hon. Marco Mendicino: Vous avez absolument raison.

M. René Villemure: Lors de votre présentation, vous avez mentionné que la GRC faisait une évaluation afin de voir si l'outil n'était pas trop intrusif.

Vous avez fait attention de ne pas nommer l'outil. Par contre, cette autoévaluation de la pertinence n'est pas très transparente. J'ai l'impression que la GRC s'évalue elle-même. Je reviens sur la question de la confiance, car cela me fait douter de la transparence de cette évaluation.

Quelle est votre observation à ce sujet?

● (1530)

L'hon. Marco Mendicino: C'est une bonne question.

D'une part, le processus prévu par le Code criminel pour l'obtention d'une autorisation d'écoute électronique inclut des critères auxquels il faut répondre. Il faut démontrer avec beaucoup de rigueur à un juge d'une Cour supérieure que les critères sont remplis. L'une des obligations des services policiers et de la GRC est de démontrer au juge qu'il n'y a aucune autre possibilité et que toutes les options pour faire avancer l'enquête ont été épuisées. C'est un exemple d'une mesure de protection qui est en place.

D'autre part, des mécanismes sont prévus, dont le rapport annuel présenté au Parlement. Dans ce rapport, il est fait mention de la date à laquelle l'autorisation a été donnée par la Cour supérieure.

J'invite tous les membres de ce comité à offrir d'autres suggestions pour renforcer les mécanismes de transparence, parce que cela contribuera encore davantage à raffermir la confiance. Nous devons maintenir la confiance partout pour pouvoir utiliser cet outil d'une façon qui respecte la Charte et tous les droits qu'elle prévoit.

M. René Villemure: Y aurait-il lieu de s'adjoindre une tierce partie, qui contribuerait au processus afin d'assurer une saine distance et éviter que la GRC ne s'évalue elle-même?

L'hon. Marco Mendicino: Je pense que oui.

Il y a déjà des tierces parties, dont le commissaire à la protection de la vie privée, l'Office de surveillance des activités en matière de sécurité nationale et de renseignement et le Comité des parlementaires sur la sécurité nationale et le renseignement.

Plusieurs agences ont l'autorité et le pouvoir d'étudier l'information, qui est traditionnellement protégée par les lois sur la sécurité nationale et par d'autres privilèges. Cela nous permet d'augmenter davantage la confiance. Des tierces parties sont déjà là pour nous aider à faire ce travail.

M. René Villemure: Je vous remercie beaucoup.

En ce qui a trait aux juges qui accordent les mandats demandés par les policiers, croyez-vous qu'ils ont la capacité technique d'évaluer l'ensemble de ces outils?

Ce sont quand même des choses compliquées.

L'hon. Marco Mendicino: C'est une excellente question.

La réponse est oui, les juges ont absolument les compétences nécessaires.

Les juges comprennent bien les critères prévus par la loi. Ils savent comment trouver l'équilibre entre le devoir de l'État de protéger tout le monde et le respect de tous les droits prévus par la Charte.

Les juges ont l'expertise, l'expérience et la compétence nécessaires pour faire cet exercice, pour chercher l'équilibre. C'est la raison pour laquelle j'ai confiance en ce processus. Des institutions sont là pour protéger tous les droits des Canadiens et des Canadiennes.

M. René Villemure: Même si cela se fait avec précaution, que de tierces parties sont là pour surveiller le processus et qu'il y une certaine obligation de reddition de comptes, nous pouvons quand même conclure que la GRC espionne des citoyens canadiens.

Est-ce exact?

L'hon. Marco Mendicino: Oui, c'est précisément le travail qui incombe à la GRC. Les fonctionnaires et les responsables sont là pour répondre à des questions techniques et opérationnelles, pour vous dire comment ces techniques sont utilisées sur le terrain dans le contexte des enquêtes.

Cependant, cela neveut pas dire qu'il n'y a pas de place à l'amélioration. C'est la raison pour laquelle j'encourage le travail que fait ce comité. J'invite les membres du Comité à offrir des suggestions et des recommandations pour renforcer la façon dont ces outils sont utilisés par les services policiers, y compris la GRC.

M. René Villemure: Rassurez-vous, c'est aussi notre but.

Je vous remercie.

L'hon. Marco Mendicino: D'accord.

Je vous remercie.

[*Traduction*]

Le président: Merci.

M. Green maintenant. Vous avez six minutes.

M. Matthew Green: Merci beaucoup.

De vos remarques liminaires, je retiens notamment que vous avez tenu à souligner la pleine collaboration de la GRC avec le Commissariat à la protection de la vie privée pour ce qui est de l'évaluation des répercussions des nouvelles utilisations envisagées de la reconnaissance faciale sur la vie privée. Ce n'est toutefois pas le thème de notre réunion.

Aujourd'hui, et vous vous êtes peut-être mépris dans vos remarques liminaires, nous nous intéressons aux outils d'interception sur appareil. Ce matin, durant la première partie de la réunion, nous avons réalisé que le commissaire à la protection de la vie privée n'avait pas été informé du sujet de la réunion.

Avez-vous un commentaire à nous livrer concernant la contradiction claire et évidente entre ce passage de vos remarques liminaires et les déclarations du commissaire sur ce qui fait l'objet de notre étude, soit les outils d'interception sur appareil?

● (1535)

L'hon. Marco Mendicino: Je dois tout d'abord vous remercier de cette question, monsieur Green.

Je trouve assez malencontreux que le commissaire à la protection de la vie privée ait déclaré qu'il a appris dans les médias que cette technique d'enquête est utilisée. J'en ai discuté avec la GRC, et je suis heureux de vous assurer, à vous et aux autres membres du Comité, qu'elle collabore étroitement avec le commissaire pour s'assurer d'utiliser cette technique — je tiens à répéter qu'elle est rarement utilisée et toujours selon un processus rigoureux d'approbation par un juge d'une cour supérieure — dans le respect de la Charte.

M. Matthew Green: Je suis convaincu que vous, ou le personnel qui vous a fait un compte rendu de son témoignage, avez entendu le commissaire à la protection de la vie privée recommander dans ses remarques liminaires que la Loi exige la réalisation d'une évaluation des répercussions sur la vie privée. Êtes-vous d'accord avec cette recommandation et seriez-vous prêt à la défendre?

L'hon. Marco Mendicino: Monsieur Green, je salue et j'appuie le travail du Comité et toute recommandation qu'il pourrait faire pour améliorer la transparence. Pour l'heure, je dois souligner, comme je l'ai fait dans mes réponses précédentes, que des mécanismes de transparence sont en place. Cela dit, parce que cette technologie revêt un caractère particulièrement sensible et que son usage doit être restreint et sujet, là encore, à l'autorisation d'un juge d'une cour supérieure sur la foi d'un affidavit produit par un agent désigné, nous devons toujours rester ouverts aux suggestions visant à mettre la barre encore plus haut.

M. Matthew Green: C'est ce que nous nous efforçons de faire, et c'est pourquoi je vais en profiter pour vous poser la question directement. À titre de ministre responsable, si on procède à la révision de la Loi sur la protection des renseignements personnels dont on parle actuellement, donneriez-vous votre appui à l'incorporation d'une telle exigence juridique?

L'hon. Marco Mendicino: Monsieur Green, je me ferai certainement un plaisir de prendre connaissance de toutes les recommandations du Comité. J'accorderai un grand soin à ce que toutes vos suggestions fassent l'objet d'un examen attentif et ouvert. Je me ferai également un devoir, monsieur Green, de bien examiner vos recommandations en tenant compte du cadre et de la structure qui ont été conçus pour assurer la transparence au sein de l'OSSNR…

M. Matthew Green: Nous avons bien noté que le Conseil du Trésor a intégré à ses politiques le principe de l'ouverture par défaut, suivant lequel il est demandé aux ministères de collaborer de manière proactive avec le commissaire à la protection de la vie privée sur les questions comme celles qui nous occupent aujourd'hui. Or, si je me fie à l'étude sur l'utilisation par Santé Canada de données sur les appareils mobiles que nous avons dû réaliser, ou à ce qui est ressorti au sujet de Clearview AI et à tout ce que nous avons sous les yeux aujourd'hui, le commissaire semble la plupart du temps en mode rattrapage par rapport aux activités de ces ministères.

Ce gouvernement semble loin de nourrir une culture de transparence et d'ouverture par défaut, et ces ministères ne semblent pas vraiment disposés à collaborer proactivement avec le commissaire à la protection de la vie privée. Nous en sommes à une troisième situation dont l'étude en comité aurait pu être évitée si ces agences s'étaient pleinement et officiellement engagées à réaliser une évaluation des répercussions sur la vie privée, si elles s'étaient montrées pleinement disposées à coopérer. Êtes-vous d'accord?

L'hon. Marco Mendicino: Je crois que les représentants de la GRC qui sont avec nous vous diront, et ce que moi-même je peux vous affirmer, monsieur Green, c'est qu'il faut toujours viser à faire mieux en matière de transparence. Le rapport annuel sur la surveillance électronique représente à mes yeux un des outils dont nous disposons pour lever le voile sur la manière dont ces techniques d'enquête sont utilisées pour protéger les Canadiens. Monsieur Greene, je me réjouis de prendre connaissance des suggestions que vous et vos collègues nous soumettrez parce que je crois fermement que la confiance repose sur la transparence.

M. Matthew Green: Et je vous en suis reconnaissant.

J'aimerais avoir des précisions sur les lois et les politiques qui garantissent que la GRC utilise les outils et les nouvelles technologies conformément aux exigences en matière de protection de la vie privée qui relèvent de votre responsabilité ministérielle.

L'hon. Marco Mendicino: En tout premier lieu, le Code criminel prévoit un processus très rigoureux et très transparent, comme je l'ai dit, et exige une honnêteté et une intégrité à toute épreuve devant les tribunaux. Ensuite, il y a la Loi sur la protection des renseignements personnels qui, c'est important de le mentionner…

M. Matthew Green: Ces agences n'ont-elles pas également un devoir d'intégrité devant la Chambre des communes et les comités?

L'hon. Marco Mendicino: Sans aucun doute, monsieur Green. Je ne…

M. Matthew Green: D'accord. Je me dois de profiter de votre passage devant nous pour vous faire remarquer que, dans le cadre de nos études précédentes, des membres de la GRC ont refusé de dire qui était responsable de l'acquisition de la technologie Clearview, même si c'était déjà de notoriété publique. Nous observons une culture de cynisme qui est reflétée dans une décision judiciaire mettant en cause le SCRS et la GRC.

À titre de ministre responsable, que faites-vous pour assurer que le devoir d'intégrité est exercé d'une manière qui garantit la transparence, l'intégrité et l'honnêteté pleines et entières des témoignages devant notre comité et la Chambre des communes?

L'hon. Marco Mendicino: En quelques mots, j'exige le respect de toutes les valeurs que vous venez de mentionner de la part de tous les services dont je suis responsable, et je m'assure que des mécanismes sont suivis pour atteindre le degré de transparence essentiel pour maintenir la confiance. C'est un exercice permanent, qui exige une réflexion constante, surtout si nous…

M. Matthew Green: J'aurais une dernière question. Nous avons parlé de la Loi sur la protection des renseignements personnels et de l'incorporation des droits à la vie privée dans le préambule. Nous avons depuis établi que le préambule n'est pas juridiquement contraignant. Seriez-vous favorable à l'incorporation des droits à la vie privée dans le cadre juridique de la prochaine version de la Loi sur la protection des renseignements personnels?

● (1540)

Le président: M. Green a utilisé tout son temps et il n'en reste plus pour la réponse. Peut-être la réponse pourrait-elle…

M. Matthew Green: Je vais lui laisser le temps de réfléchir. Il pourra nous faire part du fruit de cette réflexion durant mon prochain tour.

Le président: Monsieur le ministre, je peux vous donner du temps pour répondre par oui ou par non si vous le souhaitez.

M. Matthew Green: Allez-y.

L'hon. Marco Mendicino: La réponse brève, monsieur le président, est qu'elle prévoit déjà des mécanismes de protection des droits garantis par la Charte et à la vie privée. Cela dit, je serai ouvert à toute recommandation du Comité à ce sujet.

Le président: Je donne maintenant la parole à M. Williams.

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

Monsieur le ministre, merci d'être des nôtres.

Ce matin, le commissaire à la protection de la vie privée se trouvait dans cette salle et nous a parlé du maintien de la confiance à l'égard des institutions publiques.

Pensez-vous que c'est important de maintenir la confiance à l'égard des institutions publiques?

L'hon. Marco Mendicino: Absolument.

M. Ryan Williams: Vous avez mentionné en introduction que cette technologie, à votre connaissance, est utilisée depuis 2017. Est-ce exact?

L'hon. Marco Mendicino: C'est ce qu'on m'a dit.

M. Ryan Williams: Monsieur le ministre, trouvez-vous acceptable que depuis cinq ans, la GRC n'ait pas produit d'évaluation des répercussions sur la vie privée et qu'elle se prête à l'exercice maintenant? Le commissaire à la protection de la vie privée s'attendait à recevoir cette évaluation à la fin d'août. Est-il acceptable qu'il ait fallu attendre cinq ans pour une telle évaluation?

L'hon. Marco Mendicino: Comme je l'ai dit précédemment, je trouve déplorable que le commissaire à la protection de la vie privée vienne tout juste d'être mis de la partie, mais je tiens aussi à vous préciser, à vous et à l'ensemble du Comité, que des mécanismes de protection de la vie privée existent et sont appliqués lorsque les agents demandent l'autorisation judiciaire d'utiliser ce type de technologie. C'est une des importantes…

M. Ryan Williams: Monsieur le ministre, je vais répéter la question. Trouvez-vous acceptable qu'il ait fallu attendre cinq ans? Si je reviens à la déclaration du commissaire ce matin comme quoi il n'était au courant de rien avant juin, ce qui est manifestement beaucoup trop tardif, pensez-vous qu'un délai de cinq ans est trop long?

L'hon. Marco Mendicino: Je tiens à ce que vous compreniez bien que quand ces techniques sont utilisées, y compris les outils d'enquête sur appareil, il faut trouver un équilibre…

M. Ryan Williams: Monsieur le ministre, vous pouvez répondre par oui ou par non. Oui ou non?

L'hon. Marco Mendicino: J'ai déjà dit que des mécanismes de protection de la vie privée sont appliqués chaque fois que ces techniques sont utilisées.

M. Ryan Williams: Monsieur, si vous ne répondez pas à mes questions, à quoi bon les poser?

C'est très simple. Si un commissaire à la protection de la vie privée a des exigences qui sont tout à fait de base à l'égard de nos institutions, et vous avez dit clairement que nous devons nourrir la confiance envers ces institutions, ne serait-il pas normal que le gouvernement fasse ce qui s'impose pour qu'elles se conforment à ces exigences fondamentales?

L'hon. Marco Mendicino: Cela va de soi. C'est pourquoi j'ai dit que…

M. Ryan Williams: Merci, monsieur. Merci infiniment.

L'hon. Marco Mendicino: … nous collaborons avec la GRC… Je suis désolé, avec le commissaire à la protection de la vie privée.

M. Ryan Williams: Merci beaucoup, monsieur.

Le Comité étudie, comme vous l'avez évoqué dans vos remarques liminaires, la technologie de reconnaissance faciale et la mobilité des données. La technologie est en constante évolution. C'est l'exemple le plus récent, mais il y en a d'autres. Vous avez indiqué que cette technologie a commencé à être utilisée en 2017, alors il est permis de penser qu'il y aurait beaucoup plus à apprendre au sujet de son utilisation.

À votre connaissance, devrions-nous exiger que d'autres agences qui relèvent de votre compétence procèdent à une évaluation des répercussions sur la vie privée?

L'hon. Marco Mendicino: Je ne peux pas porter atteinte à l'indépendance du Comité et lui dicter ses sujets d'étude. Je salue toutefois la discussion que nous avons en ce moment sur ce qui doit être fait pour protéger la vie privée.

Des mécanismes de protection sont déjà en place, mais il y a certainement lieu de les moderniser étant donné que de nouvelles technologies sont utilisées pour contrer les tentatives de criminels organisés et d'autres agents malveillants de nuire à la santé et à la sécurité des Canadiens.

M. Ryan Williams: Monsieur le ministre, pensez-vous qu'une modernisation de la législation canadienne en matière de protection de la vie privée sera nécessaire à court terme? C'est une demande qui vous a été faite dans les témoignages entendus aujourd'hui et dans d'autres que le Comité a reçus précédemment. Y aurait-il lieu d'accélérer cette modernisation à votre avis?

L'hon. Marco Mendicino: Je pense qu'il faut toujours chercher les meilleures façons de protéger la vie privée des Canadiens. C'est dans cette optique, comme je l'ai dit, que j'appuie totalement l'étude en cours.

M. Ryan Williams: Monsieur le ministre, pour ce qui concerne les processus d'approvisionnement pour ce genre de technologie… Quelqu'un prend ces décisions, de toute évidence, mais est-ce que votre cabinet en est informé?

L'hon. Marco Mendicino: Pour ce qui concerne l'approvisionnement, différentes décisions opérationnelles sont prises de manière indépendante. Comme de raison, ces processus relèvent de la GRC. Il serait inopportun que les enquêtes soient confiées aux représentants élus.

Cela dit, quand on juge que certains types de technologies ou des ressources supplémentaires sont nécessaires, leur acquisition se fait généralement par voie de demandes de crédits budgétaires ou d'un autre type. Les demandes soumises sont examinées au vu de leur bien-fondé, bien entendu.

M. Ryan Williams: Merci, monsieur le ministre.

Savez-vous si le SCRS, le Centre de la sécurité des communications, le CST, ou d'autres organismes utilisent la technologie dont vous avez parlé?

● (1545)

L'hon. Marco Mendicino: Je peux seulement parler de mon propre portefeuille. Comme je l'ai indiqué, la GRC a indiqué qu'elle utilise cette technique.

M. Ryan Williams: D'accord.

Savez-vous si d'autres agences y ont recours?

L'hon. Marco Mendicino: Assurément, quand le gouvernement utilise ce genre de techniques, c'est toujours dans le respect de la Charte, de la législation en matière de protection de la vie privée et de tous les autres mécanismes et principes de transparence associés.

M. Ryan Williams: Merci, monsieur le président.

Le président: Nous entendrons maintenant les questions de Mme Valdez, pour les cinq prochaines minutes.

Mme Rechie Valdez (Mississauga—Streetsville, Lib.): Merci, monsieur le président.

Merci, monsieur le ministre, de vous joindre à nous aujourd'hui.

Monsieur le ministre, le pouvoir d'octroyer un mandat de surveillance électronique à la GRC relève de la partie VI du Code criminel. Comme pour les perquisitions et les saisies, le Code criminel n'autorise pas la surveillance de masse, mais il permet aux forces de l'ordre de recourir à ces outils en cas d'absolue nécessité pour assurer la paix et la sécurité.

Monsieur le ministre, pouvez-vous éclairer le Comité quant aux seuils qui devraient être prévus au Code criminel pour autoriser l'interception de communications privées?

L'hon. Marco Mendicino: C'est un seuil qui est très élevé, madame Valdez, comme vous l'avez mentionné. Les critères ne sont pas faciles à remplir. La Loi permet à un nombre très restreint de personnes de demander une autorisation judiciaire pour faire de l'écoute électronique ou utiliser l'une ou l'autre des techniques d'enquête qui font l'objet de la présente étude. Le demandeur peut invoquer une liste très limitée d'infractions graves prévues au Code criminel pour demander l'autorisation de recourir à la technique en question pour recueillir des éléments d'information ou de preuve.

Comme il a été indiqué précédemment, madame Valdez, l'État doit établir avec force détails que la technique en question, la méthode de surveillance ou les perquisitions et saisies envisagées ne constituent pas un premier recours et ne sont pas un expédient. Il faut faire la démonstration que la demande est soumise après que toutes les autres avenues ont été épuisées. Le Code criminel et la Loi en général comportent de nombreux mécanismes de protection qui assurent l'équilibre entre la capacité de l'État de protéger en même temps les personnes et la vie privée de l'ensemble des Canadiens.

Mme Rechie Valdez: Dans vos remarques liminaires, vous avez insisté sur l'importance de la transparence, de la protection de la vie privée et de la responsabilité. C'est le moins que nous, les Canadiens, puissions attendre de nos services de renseignement. Comment pouvons-nous convaincre les Canadiens que leurs droits à la vie privée et garantis par la Charte des droits et libertés sont respectés, et que faisons-nous pour assurer ce respect?

L'hon. Marco Mendicino: La réponse courte, je crois, est qu'il faut continuer d'exiger l'ouverture, la transparence et la responsabilité. C'est exactement pour cette raison que je suis content de comparaître devant vous et vos collègues du Comité. J'appuie entièrement l'étude en cours. Il est important d'expliquer aux Canadiens pourquoi les forces de l'ordre doivent utiliser cette technologie. N'oublions pas que les criminels et les agents mal intentionnés réussissent de mieux en mieux à échapper à la détection de ces agences en recourant au chiffrement et à d'autres techniques perfectionnées. Ils ne veulent pas être interceptés, et ils font tout pour l'éviter.

Nous savons que les conséquences peuvent être dévastatrices, d'autant plus que notre vie se déroule de plus en plus en ligne. Ces technologies ne sont pas utilisées comme des expédients, à la légère ou de manière frivole. L'État s'en sert pour protéger la sécurité, la paix et la santé des Canadiens. En revanche, j'estime important de lever le voile, dans la mesure du possible, sur l'utilisation de ces techniques et de ces technologies, sans toutefois compromettre l'intégrité opérationnelle. Il faut absolument préserver cet équilibre mais, pour revenir à la prémisse de votre question, c'est l'ouverture qui demeure la clé pour garder la confiance des Canadiens.

Mme Rechie Valdez: Merci.

En mars 2021, notre gouvernement a créé le Programme national d'intégration des technologies afin de rendre la GRC et la façon dont elle collecte, recense et suit les technologies nouvelles et émergentes plus transparentes. Pouvez-vous nous donner un aperçu du fonctionnement de ce programme et de la façon dont la GRC respecte ce droit à la vie privée dans ses enquêtes?

L'hon. Marco Mendicino: En termes simples, le programme vise à centraliser ces processus. Ce faisant, nous pouvons nous assurer d'un plus grand respect des normes professionnelles, de la Loi. Des membres clés de la GRC ont été désignés pour présenter les demandes d'utilisation de ces techniques. Ils sont très au fait des exigences des tribunaux... s'assurant d'être tenus au courant de toute modification législative parce qu'à l'occasion, les tribunaux préciseront l'interprétation de la Loi selon les techniques et la technologie utilisées, et leur interprétation de la façon dont nous pouvons dûment respecter cet équilibre.

À mon avis, la centralisation par l'entremise du PNIT donne davantage confiance dans le fait que la GRC respecte les aspects les plus rigoureux de la Loi, puisque ses membres sont des personnes hautement qualifiées qui adhèrent à des normes professionnelles élevées.

● (1550)

Mme Rechie Valdez: Merci.

Monsieur le président, je crois que mon temps de parole est peut-être écoulé.

Le président: Vous avez le temps de poser une autre question, si vous le souhaitez. Il vous reste environ 35 secondes.

Mme Rechie Valdez: Laissez-moi essayer de glisser celle-ci.

Monsieur le ministre, au bout du compte, les Canadiens veulent savoir que leur vie privée, leurs familles et leurs droits sont protégés. Comment pouvons-nous continuer à garantir que ce sera le cas pour les Canadiens?

L'hon. Marco Mendicino: Nous y parviendrons en nous assurant que nos lois protègent leur vie privée; que nous adhérons aux mécanismes de transparence; que nous coopérons avec l'OSSNR, le CPSNR et le commissaire à la protection de la vie privée; et en continuant à échanger avec tous les parlementaires, y compris ce comité, afin que nous puissions avoir une discussion ouverte et franche sur la façon de protéger les Canadiens face aux nouvelles technologies tout en respectant les droits que la Charte leur confère.

Mme Rechie Valdez: Je vous remercie.

Le président: D'accord. Ce sera tout.

Nous allons maintenant passer à M. Villemure.

[*Français*]

Vous avez la parole pour deux minutes et demie.

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

Monsieur le ministre, est-il possible de fournir au Comité l'ensemble des rapports que vous avez évoqués un peu plus tôt? Ce serait bien aimable de votre part, car cela nous éviterait beaucoup d'heures de recherche.

L'hon. Marco Mendicino: Cela est tout à fait possible.

M. René Villemure: Je vous remercie beaucoup.

Vous avez parlé d'ouverture, de transparence et de reddition de comptes. Ce sont de bonnes choses, nous en convenons. Toutes ces choses sont faites pour obtenir la confiance de la population. Nous sommes d'accord là-dessus.

Le gouvernement a pris un engagement en matière de transparence et de sécurité nationale, tout en soulignant qu'il allait être transparent, mais qu'il ne pourra pas toujours fournir les détails. Nous comprenons cela.

Selon ce que vous avez dit plus tôt, dans vos remarques préliminaires, des efforts sont faits pour assurer la transparence.

Pardonnez-moi de vous le dire, mais nous devons vous croire sur parole. Je me demande si le fait de devoir vous croire suscite la confiance.

Qu'en pensez-vous?

L'hon. Marco Mendicino: Je suis d'accord pour dire que, si nous voulons préserver la confiance des gens, il faut faire preuve d'ouverture et de transparence. C'est la raison pour laquelle le travail de ce comité est essentiel.

Il est aussi essentiel que la GRC et le commissaire travaillent ensemble pour protéger le droit à la vie privée. C'est la raison pour laquelle il faut continuer de travailler avec l'Office de surveillance des activités en matière de sécurité nationale et de renseignement et le Comité des parlementaires sur la sécurité nationale et le renseignement. C'est seulement par la transparence...

M. René Villemure: Je suis désolé de vous interrompre, mais je ne dispose que de peu de temps.

Mes collègues ont mentionné la reconnaissance faciale et la géolocalisation des données. J'ai l'impression que la culture de la GRC est davantage axée sur l'évitement que sur le respect de la vie privée.

Qu'en pensez-vous?

L'hon. Marco Mendicino: J'espère et je pense que la GRC comprend et observe l'engagement selon lequel il faut être transparent et toujours travailler en collaboration avec toutes les institutions qui sont là pour protéger les droits des Canadiens en vertu de la Charte.

La GRC va continuer de travailler de bonne foi avec tous les parlementaires, et elle va continuer de faire beaucoup d'efforts. Elle continuera de travailler avec ce comité pour assurer le respect de la valeur de transparence et pour contribuer à augmenter la confiance.

M. René Villemure: Seriez-vous prêt à interdire le logiciel Pegasus au Canada?

L'hon. Marco Mendicino: Oui.

M. René Villemure: Je vous remercie beaucoup.

[*Traduction*]

Le président: Nous donnons maintenant la parole à M. Green pour deux minutes et demie.

M. Matthew Green: Merci beaucoup.

D'après certaines divulgations dont nous avons pris connaissance en préparation de cette réunion, nous avons constaté qu'il y a eu 32 déploiements de cette technologie en remontant à l'année 2017. Dans vos notes d'information, vous a-t-on déjà appris qu'il y avait eu des cas antérieurs à 2017?

L'hon. Marco Mendicino: Monsieur Green, on m'a informé que l'utilisation la plus ancienne de cette technique remonte à 2017.

M. Matthew Green: Dans le témoignage du commissaire à la protection de la vie privée, lorsque nous avons parlé du recours à la technologie Stingray, qui consiste à installer des tours de téléphonie cellulaire fantômes pour intercepter les données de téléphones cellulaires, nous avons appris qu'il y a eu des cas d'utilisation sans mandat.

Êtes-vous au courant de cas où cette technologie aurait pu être utilisée? Je pense qu'il s'agissait de situations urgentes ou de quelque chose du genre. Êtes-vous au courant de cas où cela aurait pu se produire?

L'hon. Marco Mendicino: Je pense que le critère précis serait de savoir s'il y avait ou non des situations urgentes, mais je sais que tous ces cas ont été soumis à une autorisation judiciaire préalable. Je vous invite à poser aussi la question directement à la GRC.

● (1555)

M. Matthew Green: Sauf votre respect, lorsque j'ai posé cette question, j'ai eu l'impression que vous avez un peu tergiversé. Encore une fois, à mon avis, l'un des moyens de nous éviter une grande partie du travail que nous avons déjà fait, c'est de mettre en place un système qui permette que les évaluations des facteurs relatifs à la vie privée soient une exigence législative par l'entremise du commissaire à la protection de la vie privée. Je vous repose la question: seriez-vous favorable à une telle mesure, étant donné le travail que nous avons fait ici et le témoignage que vous avez déjà donné sur l'importance de la vie privée comme droit fondamental?

L'hon. Marco Mendicino: Monsieur Green, je suppose que ce que je veux dire par ma réponse, c'est que je suis impatient de recevoir cette recommandation. Je pense que...

M. Matthew Green: C'est la même réponse.

Je vais poser la prochaine question de façon directe. Lorsque l'évaluation des facteurs relatifs à la vie privée sera transmise au commissaire à la protection de la vie privée, seriez-vous disposé à nous la transmettre, étant donné le fondement du devoir de franchise et le pouvoir dont jouit notre comité de demander des documents et des éléments de preuve?

L'hon. Marco Mendicino: Oui. Je veux dire, je pense que je peux être aussi transparent que possible sur ces facteurs relatifs à la vie privée. Je veux aussi m'assurer que nous respectons le processus mis en place par le commissaire à la protection de la vie privée en collaboration avec la GRC. L'essentiel pour moi c'est que plus nous serons transparents, mieux ce sera.

Le président: Je vous remercie.

Sur ce, nous allons donner la parole à M. Kurek pour cinq minutes, puis à M. Bains pour cinq minutes. Cela devrait conclure ce groupe.

Allez-y, monsieur Kurek.

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

Monsieur le ministre, je vous remercie d'être venu.

Vous avez évité de répondre à la question auparavant, alors je vais peut-être vous la poser un peu différemment. Savez-vous si d'autres organismes ou ministères relevant de votre compétence ont utilisé cette technologie, oui ou non?

L'hon. Marco Mendicino: Encore une fois, je vous dirais que...

M. Damien Kurek: À part la GRC, monsieur le ministre, savez-vous si d'autres entités relevant de votre compétence, et je ne vous demande même pas de les énumérer, ont utilisé cette technologie? À part la GRC.

L'hon. Marco Mendicino: J'allais vous répondre. J'étais en train de dire que ces techniques, si et quand elles sont utilisées, le sont toujours en conformité avec la Loi et la Charte.

M. Damien Kurek: Nous prendrons cela comme un « oui », bien que vous ayez usé de faux-fuyants.

Monsieur le ministre, comme cela a été le cas, et certainement comme je l'ai vu plusieurs fois devant ce comité, la réponse du gouvernement semble être que nous devons renforcer la confiance, alors faites-nous confiance. Dans bien des cas, notamment dans le témoignage contradictoire que vous avez donné ici aujourd'hui avec ce dont le commissaire à la protection de la vie privée a parlé ce matin... et en voyant comment son bureau a donné son approbation, je crois, votre secrétaire parlementaire de l'époque, Mme Damoff, et la lettre qui a été transmise, il y a une divergence. Il y a une disparité.

Tant dans le Code criminel que dans d'autres cadres législatifs, des dispositions permettent d'invoquer la sécurité nationale pour contourner la partie VI et les processus judiciaires habituels requis pour les opérations de surveillance. Monsieur le ministre, oui ou non: savez-vous si ces dispositions ont déjà été invoquées pendant que vous étiez ministre de la Sécurité publique, oui ou non?

L'hon. Marco Mendicino: Je tiens à être très clair sur le fait que lorsque ces techniques sont utilisées, elles le sont en conformité avec la Loi. J'ai expliqué à plusieurs reprises comment...

M. Damien Kurek: Monsieur le ministre, je pense que ma question était assez directe. Des exemptions au titre de la sécurité nationale peuvent être invoquées pour contourner les processus habituels. Il y a ce processus judiciaire, que vous avez exposé de façon assez détaillée, dans la partie VI du Code criminel. Des exemptions au titre de la sécurité nationale permettent d'utiliser ces techniques de surveillance sans passer par le processus complet décrit dans la partie VI du Code criminel. À votre connaissance, est-ce que cela s'est produit pendant que vous étiez ministre de la Sécurité publique, oui ou non?

L'hon. Marco Mendicino: Je tiens simplement à souligner encore une fois que lorsque cette technique est utilisée, elle l'est en conformité avec la Loi et la Charte. Pour tout détail supplémentaire, je vous invite à poser directement ces questions aux représentants qui sont là pour fournir ces réponses.

M. Damien Kurek: Sauf votre respect, monsieur le ministre, vous êtes le représentant élu, le ministre du Cabinet, qui assure la surveillance que les Canadiens attendent. Le fait que nous obtenions des réponses moins que directes m'apparaît très, très révélateur de cette culture du secret qui semble impliquer... Bien sûr, j'entends souvent des citoyens qui sont frustrés par les interventions de ce gouvernement lorsqu'il s'agit de sa réticence à faire preuve de transparence en répondant à ce que je pense être des questions très, très simples.

Monsieur le ministre, nous observons clairement des éléments de ce que le commissaire à la protection de la vie privée a décrit ce matin, que ce n'est qu'après que les médias ont fait état de l'utilisation des OEE que la GRC... que le Commissariat à la protection de la vie privée travaille maintenant de concert avec la GRC. Ne trouvez-vous pas inquiétant que cela confirme une tendance, que nous avons observée de la part de votre gouvernement, selon laquelle ce n'est qu'après un examen public et, dans bien des cas, des critiques parlementaires et médiatiques, que des mesures sont prises pour, comme vous dites, « renforcer la confiance » des Canadiens?

● (1600)

L'hon. Marco Mendicino: Comme je l'ai déjà dit, je pense qu'il est malheureux que le commissaire à la protection de la vie privée l'ait appris par les médias. C'est pourquoi je me réjouis du travail qui est fait aujourd'hui. Comme je l'ai dit, nous devrions toujours chercher des moyens d'élever la barre de la transparence, surtout lorsque nous utilisons de nouvelles technologies pour protéger les Canadiens.

M. Damien Kurek: Il y a beaucoup de choses malheureuses. Bien sûr, j'ai hâte d'accueillir demain matin l'ancien commissaire à la protection de la vie privée qui a eu, je le signale pour le compte rendu, monsieur le président, des désaccords très médiatisés avec la GRC, entre autres.

Monsieur le ministre, j'espère que vous comprenez que les Canadiens ne sont pas à l'aise avec les messages simples que ce gouvernement semble répéter — nous renforçons la confiance, alors faites-nous simplement confiance — et j'espère que nous pourrons certainement obtenir des réponses à cet égard.

L'hon. Marco Mendicino: Eh bien, je vous dirais simplement qu'il existe de nombreux mécanismes de transparence pour assurer l'ouverture, y compris l'OSSNR et le CPSNR et les critères très rigoureux prévus par le Code criminel. C'est ainsi que nous continuerons à renforcer la transparence, sans négliger le bon travail de ce comité.

Le président: Je vous remercie.

Le dernier intervenant de ce tour sera M. Bains.

Vous disposez de cinq minutes. Allez-y.

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

Merci, monsieur le ministre, de vous joindre à nous. Merci d'avoir été très ouvert et de nous avoir parlé des différents mécanismes de transparence.

Ma première question porte sur la reconnaissance faciale. Des experts nous ont dit que les technologies de reconnaissance faciale contribuent intrinsèquement à des préjugés raciaux, en identifiant mal les personnes racisées dans une proportion beaucoup plus grande. Si la GRC utilise de telles technologies, comment tient-elle compte de ces disparités et comment lutte-t-elle contre ces inégalités systémiques?

L'hon. Marco Mendicino: Merci beaucoup, monsieur Bains, pour cette question. Dans le cadre de mon mandat, je travaille en étroite collaboration avec la GRC et, en fait, avec toutes les directions générales de la Sécurité publique, afin de lutter contre le racisme systémique et d'autres obstacles institutionnels qui, depuis trop longtemps, produisent des résultats disproportionnés, surtout en ce qui concerne les Canadiens racisés et les Autochtones.

J'invite les membres de ce comité à jeter un coup d'œil aux lettres de mandat les plus récentes et actualisées que j'ai envoyées à toutes les directions générales de mon portefeuille, y compris la GRC qui comparaît ici aujourd'hui, car nous devons nous attaquer à cette tâche ensemble. Je tiens à féliciter la commissaire et tous les membres de l'équipe de direction d'avoir compris et reconnu qu'il s'agit d'une priorité absolue pour notre gouvernement. Nous avons évidemment un long chemin à parcourir. Je ne veux pas accorder moins d'attention à cette question qu'elle n'en mérite. Je sais que le Comité se penche sur une question très précise, mais je suis tout à fait d'accord avec vous pour dire que les obstacles institutionnels au racisme systémique sont un véritable problème et qu'ils touchent toutes nos institutions, y compris les forces de l'ordre, depuis bien trop longtemps. Nous cherchons à redresser la barre.

M. Parm Bains: Je vous remercie pour votre réponse.

Vous avez mentionné le Programme national d'intégration des technologies. Pouvez-vous expliquer comment ce programme permettra de mieux surveiller le recours à ces technologies et aux outils d'enquête que la GRC utilise?

L'hon. Marco Mendicino: Merci de cette question, monsieur Bains. Je pense qu'à certains égards, j'en ai déjà parlé en répondant à Mme Valdez.

Essentiellement, la GRC a créé cette direction générale ou ce bureau, si vous voulez, pour centraliser nos efforts à l'égard de l'utilisation de cette technologie. Ce faisant, nous pouvons nous assurer que les attentes sont très claires et très rigoureuses en ce qui concerne les normes professionnelles; que les membres qui ont été désignés pour utiliser cette technologie reçoivent une formation et que, dans le cadre de cette formation, ils sont tenus au courant de l'évolution de la jurisprudence et de la Loi, de sorte que lorsque des améliorations s'imposent, lorsqu'il faut corriger le tir et qu'il faut faire preuve d'une plus grande sensibilité pour nous assurer de protéger la vie privée, nous respectons ces valeurs.

Comme je pense que nous l'avons entendu tout au long de la discussion d'aujourd'hui, l'un des thèmes récurrents est que nous voulons tous renforcer la confiance, mais pour ce faire, la transparence, l'ouverture et la responsabilité sont de mise. Je pense que la création de ce bureau vise à faire exactement cela.

● (1605)

M. Parm Bains: Pour faire suite à votre réponse, quel rôle jouez-vous, le cas échéant, dans le processus décisionnel de la GRC en ce qui concerne la décision d'utiliser les OEE dans une affaire donnée?

L'hon. Marco Mendicino: Aucun, puisqu'il s'agit de techniques opérationnelles. Nous ne voulons pas que les membres élus du gouvernement, ou tout autre politicien élu, d'ailleurs, dirigent ou tentent d'orienter des enquêtes, ce qui, par extension, comprendrait les techniques d'enquête ou les autorisations judiciaires. La Cour suprême a établi des garanties, notamment des principes constitutionnels, pour préserver l'indépendance opérationnelle. C'est quelque chose en quoi je crois, et j'espère qu'il en va de même pour tous les membres de ce comité. Vous ne voudriez pas que moi ou un autre membre élu ordonne le recours à cette technique.

M. Parm Bains: Je vous remercie.

Me reste-t-il du temps, monsieur le président?

Le président: Il vous reste presque une minute. Si vous voulez poser une autre question, allez-y.

M. Parm Bains: D'accord.

Monsieur le ministre, selon vous, quelles avancées de la technologie de chiffrement ont convaincu la GRC que les moyens conventionnels pour surveiller les communications d'éventuels criminels n'étaient plus suffisants?

L'hon. Marco Mendicino: Des criminels et des gens mal intentionnés qui tentent de miner la sécurité publique et la sécurité nationale utilisent des technologies émergentes de contre-surveillance, comme le chiffrement. C'est grâce à la détection de ces techniques et technologies de contre-surveillance que les forces de l'ordre et la GRC ont dû aider et utiliser d'autres techniques pour pouvoir traduire en justice ceux qui tentent de faire du mal aux Canadiens.

C'est très difficile. C'est un travail complexe, mais des garanties sont mises en place, y compris les critères prévus par la Loi et d'autres mécanismes de transparence, afin que nous puissions atteindre cet équilibre.

Le président: Très bien. Avant de suspendre la séance pour passer au groupe suivant, j'aimerais remercier le ministre de son temps et de sa volonté de comparaître devant nous.

Sur ce, la séance est suspendue.

● (1605)

(Pause)

● (1610)

Le président: Bienvenue à nouveau. Je vais convoquer le deuxième groupe de témoins de la séance d'aujourd'hui.

Pour ce deuxième groupe, nous accueillons, de la GRC, Mark Flynn, commissaire adjoint de la Police fédérale, Sécurité nationale et police de protection; Bryan Larkin, sous-ministre des Services de police spécialisés; et le sergent Dave Cobey, du Programme de gestion des dossiers techniques, aux Services d'enquête technique.

Nous allons commencer la discussion avec notre deuxième groupe en écoutant la déclaration liminaire de la GRC.

Allez-y, vous disposez de cinq minutes.

[*Français*]

Chef Bryan Larkin (sous-commissaire, Services de police spécialisés, Gendarmerie royale du Canada): Je vous remercie.

[*Traduction*]

Monsieur le président, mesdames et messieurs du Comité, bonjour. La GRC vous est reconnaissante de l'occasion que vous lui offrez de vous parler aujourd'hui de cette importante question. Nous espérons que nos commentaires éclaireront votre étude sur l'utilisation par la GRC des outils d'enquête embarqués, ou « OEE ».

Le chiffrement est essentiel dans le monde moderne. Il protège les données financières et autres renseignements de nature délicate et permet de garantir la confidentialité des activités en ligne des Canadiens. Malheureusement, le chiffrement et les appareils qui contribuent à protéger la vie privée des Canadiens aident également les criminels à mener des activités illégales et à éviter d'être repérés par la police. Bien que la police soit parfois en mesure de recueillir les données stockées sur ces appareils, le chiffrement rend souvent les données inintelligibles.

Avant de décrire en détail ce qu'est un OEE, je tiens à préciser que la GRC n'a jamais acheté ni utilisé le logiciel Pegasus ou tout autre produit de NSO.

Les OEE sont utilisés dans des cas extrêmement rares et limités. Leur utilisation est toujours ciblée, limitée dans le temps, et ne sert jamais à effectuer une surveillance injustifiée ou de masse. Ces outils ne sont pas utilisés en secret. L'utilisation d'un OEE requiert une autorisation judiciaire préalable, et les éléments de preuve recueillis, y compris la façon dont ils ont été recueillis, peuvent être divulgués et examinés par les tribunaux.

Compte tenu de son mandat et de ses exigences opérationnelles spécifiques, la GRC ne divulgue pas les détails de nature délicate liés aux outils et techniques utilisés dans le cadre de ses enquêtes. Toute divulgation publique allant au-delà de la documentation technique fournie au Comité et décrivant les capacités générales d'un OEE pourrait avoir des répercussions négatives sur nos enquêtes.

Notre utilisation des OEE est entièrement conforme aux lois canadiennes, y compris la Charte des droits et libertés, le Code criminel et la jurisprudence établie.

La technologie OEE peut être utilisée dans le cadre d'enquêtes hautement prioritaires liées à la sécurité nationale, à la criminalité grave et organisée et à d'autres infractions au Code criminel qui ont une incidence sur la sécurité des Canadiens, mais uniquement après l'obtention d'une autorisation judiciaire.

Maintenant, qu'est-ce qu'un OEE? Un OEE est un programme informatique installé secrètement sur le téléphone portable ou l'ordinateur d'un suspect.

Les OEE facilitent les enquêtes en maintenant la capacité des organismes d'application de la loi à recueillir secrètement des communications privées et d'autres données qui ne peuvent plus être obtenues par des écoutes traditionnelles ou d'autres techniques d'enquête moins intrusives. La quantité et le type de données recueillies sont déterminés au cas par cas, conformément aux conditions strictes imposées par le juge qui a autorisé l'utilisation des OEE.

L'approche prudente et mesurée de la GRC est attestée par le fait que depuis 2017, les OEE n'ont été utilisés qu'à l'appui de 32 enquêtes dans lesquelles un total combiné de 49 appareils a été ciblé. J'aimerais insister à nouveau sur ce point: au cours des cinq dernières années et demie, la GRC n'a ciblé que 49 appareils pour le déploiement d'OEE.

La GRC évalue soigneusement les avantages et les inconvénients, y compris l'incidence sur la vie privée et les tiers, avant de demander l'autorisation judiciaire d'utiliser les OEE à l'appui d'une enquête criminelle. Cette évaluation est effectuée en étroite collaboration avec les enquêteurs, les spécialistes techniques et les procureurs de la Couronne fédéraux et provinciaux, et est supervisée par le Programme de gestion des cas techniques de la Direction générale de la GRC. Nous tenons à souligner à nouveau que les OEE ne sont utilisés que pour des infractions criminelles graves et uniquement s'ils sont approuvés par un juge qui autorise explicitement l'utilisation d'OEE sur l'appareil d'un suspect en particulier. Les juges reçoivent des documents d'accompagnement expliquant ce qu'est l'OEE et ses capacités.

Bien que nous ne divulguions pas le nom des organisations avec lesquelles nous travaillons dans ce contexte public, nous tenons à confirmer à nouveau que la GRC n'a jamais acheté ou utilisé Pegasus, ou tout autre produit de NSO. Le fait de partager les détails publiquement expose des informations sensibles qui pourraient avoir un impact négatif sur la capacité de la GRC, et de nos partenaires, à utiliser efficacement les OEE à l'avenir. Des éléments criminels utiliseraient ces informations sensibles afin de rendre les outils inefficaces. Aussi, en plus d'avoir un impact négatif sur les enquêtes de la GRC, l'exposition pourrait compromettre les enquêtes des partenaires étrangers et nos relations avec ces pays.

En avril de cette année, nous avons présenté un exposé détaillé sur l'utilisation des OEE par la GRC à l'Office de surveillance des activités en matière de sécurité nationale et de renseignement du Canada. Le 23 août, des représentants du Commissariat à la protection de la vie privée du Canada recevront une séance d'information similaire.

J'aimerais également attirer l'attention du Comité sur le 4 juillet 2022, date à laquelle le Comité des parlementaires sur la sécurité nationale et le renseignement, le CPSNR, a informé le ministre de la Sécurité publique de sa décision de procéder à un examen de l'interception légale des communications par les organismes de sécurité et de renseignement, auquel nous participerons pleinement. Les objectifs de l'examen comprennent l'étude de l'état actuel de l'accès légal, des préoccupations soulevées par la société civile et les experts de la protection de la vie privée, ainsi que des défis et des lacunes technologiques. Sur la base des résultats de son examen, le CPSNR peut formuler des recommandations relatives à divers aspects des activités et des cadres d'interception légale.

● (1615)

Le président: Je suis vraiment désolé, monsieur Larkin, mais je vous ai laissé dépasser largement le temps alloué pour votre déclaration liminaire. Votre témoignage est important, mais nous allons devoir passer aux questions des membres.

Cependant, avant de le faire, au nom du Comité qui a voté pour obtenir des renseignements très précis de la GRC, je dirai qu'il a été très décevant, voire troublant, de recevoir dans la lettre de la commissaire Lucki ce qui équivaut à un refus catégorique de communiquer l'information.

En tant que grand inquisiteur du Canada, un comité du Parlement a le pouvoir absolu de demander des documents. Nous pouvons discuter de la pertinence de le faire, et vous en avez parlé dans votre déclaration. J'attends avec impatience les discussions que nous aurons avec les différents partis à ce sujet, mais un refus général opposé à un comité est troublant. Nous y reviendrons, j'en suis sûr, lors des questions des membres du Comité.

Sur ce, je vais passer au premier tour de table avec le premier intervenant, M. Bezan.

M. James Bezan: Merci, monsieur le président.

Je tiens à remercier nos témoins de leur présence.

Je remercie la GRC pour son travail.

Le Parti conservateur souhaite que vous disposiez des outils nécessaires pour faire votre travail afin que vous puissiez assurer la sécurité des Canadiens et traiter des questions de sécurité nationale et de sécurité publique en tout temps, mais il faut aussi protéger les droits des Canadiens, leur vie privée et les droits que la Charte leur confère. Le déploiement des OEE suscite des inquiétudes en ce qui concerne leurs conséquences involontaires et la possibilité que ceux qui ne sont pas nécessairement ciblés soient aussi espionnés à l'aide de la technologie dont vous disposez.

Il y a eu aussi une certaine confusion à ce sujet, car lorsque nous avons eu la réponse à la question inscrite au *Feuilleton* que la GRC a déposée par l'intermédiaire de la secrétaire parlementaire du ministre de la Sécurité publique à la Chambre en juin dernier, il a été question de 10 ou 12 cas d'utilisation des OEE. Puis, dans la lettre plutôt décevante de la commissaire Lucki, il est question de 32 enquêtes. Vous dites maintenant que 49 personnes ont été espionnées. Le chiffre ne cesse de changer, monsieur Larkin, et nous sommes tous très soucieux de savoir où se trouve la vérité. Je pense que c'est la raison pour laquelle nous devons obtenir des renseignements plus clairs.

Nous savons déjà que vous n'utilisez pas Pegasus, mais que vous disposez d'une technologie. Est-elle conçue au Canada? Quel est le pays d'origine de cette technologie que vous utilisez dans vos enquêtes?

● (1620)

S.-comm. Bryan Larkin: Merci beaucoup, monsieur Bezan.

J'aimerais simplement préciser que nous avons fait 32 demandes ciblant 49 appareils, et non 49 personnes. C'est une précision que je souhaitais apporter.

Je vais laisser au commissaire adjoint Mark Flynn le soin de parler de la technologie et de son acquisition.

Commissaire adjoint Mark Flynn (commissaire adjoint, Police fédérale, Sécurité national et police de protection, Gendarmerie royale du Canada): Au sein des services d'enquête technique de la GRC, un processus permet d'acquérir toute la technologie. Il y a un processus d'approbation au niveau du directeur général pour l'acquisition des outils et des techniques, ainsi que pour l'approbation des outils et des techniques particuliers que la GRC et nos services de surveillance électronique secrète peuvent utiliser.

M. James Bezan: Vous ne pouvez pas nous dire s'il s'agit d'une technologie canadienne ou le pays d'origine de la technologie? S'il ne s'agit pas de Pegasus, alors d'où vient-elle?

Comm. adj. Mark Flynn: De mon point de vue au sein de la Police fédérale, je ne sais pas d'où vient toute la technologie que nous utilisons, mais je peux dire que j'ai une longue expérience dans ce domaine, et qu'à l'époque, de 2002 à 2015, nous utilisions exclusivement de la technologie canadienne, mais...

M. James Bezan: C'est avant le dossier qui nous occupe. C'était en 2017 pour les OEE, alors vous dites que nous utilisons cette technologie depuis 2012?

Comm. adj. Mark Flynn: Je peux apporter quelques précisions à ce sujet. C'est antérieur à 2012. Je peux apporter des précisions à ce sujet lorsque vous le souhaiterez.

M. James Bezan: Nous utilisons donc cette technologie, en respectant, j'espère, la partie VI du Code criminel qui protège les droits garantis par la Charte.

Combien de fois l'avez-vous utilisée en évoquant les dispositions relatives à la sécurité nationale, qui font qu'il n'est pas nécessaire d'obtenir un mandat, depuis 2012 ou avant? Nous parlons des OEE et nous parlons aussi, je crois que c'est votre groupe des enquêtes spéciales « I », n'est-ce pas?

Comm. adj. Mark Flynn: D'après mon expérience, qui remonte à de nombreuses années, ainsi que dans mon poste actuel à la sécurité nationale, nous n'avons jamais utilisé cet outil sans autorisation judiciaire préalable.

Cela dit, si une situation l'exigeait, des dispositions nous permettent, de même qu'à certaines personnes désignées, d'utiliser ce type d'outil pour intercepter des communications dans des situations d'urgence, mais je n'ai connaissance d'aucune situation où cela s'est produit, et les aspects purement pratiques liés au déploiement de ce type d'outil et de technique dépasseraient la période de validité d'une telle autorisation.

M. James Bezan: Lorsqu'il s'agit d'une question de sécurité nationale, ou de quelqu'un comme l'ancien lieutenant de la Marine canadienne Jeffrey Delisle en 2012, dites-vous que cet outil aurait probablement été utilisé dans cette situation? Sachant qu'il était membre des Forces armées canadiennes, sachant qu'il peut y avoir des personnes d'intérêt au sein de la GRC, devez-vous toujours passer par l'obtention d'un mandat pour protéger leurs droits en vertu de la Charte et de la partie VI du Code criminel, ou en tant que membre du personnel, pouvez-vous les surveiller ou utiliser des logiciels espions à leur insu et sans l'aval du système judiciaire?

Comm. adj. Mark Flynn: Je peux dire sans équivoque que dans ce cas et dans tout autre cas similaire, nous avons obtenu l'autorisation judiciaire préalable pour le faire, et le contraire violerait la partie VI du Code criminel, car celle-ci renferme les dispositions relatives à l'atteinte à la vie privée et nous ne ferions pas cela. Nous sommes une organisation professionnelle qui respecte la loi.

M. James Bezan: En tant qu'organisation professionnelle qui utilise un type de logiciel espion depuis 2012 ou plus tôt, pourquoi a-t-il fallu attendre que cela devienne public? Pourquoi n'avez-vous jamais consulté le Commissariat à la protection de la vie privée au préalable?

Comm. adj. Mark Flynn: Je peux me référer encore une fois à une longue expérience dans le programme spécial « I », et comme nous suivons l'évolution de cette technologie, lorsque des cibles que nous avions l'autorisation judiciaire d'intercepter ont commencé à utiliser le chiffrement, et que nous étions incapables d'entendre l'audio, d'entendre les appels téléphoniques ou de voir les messages qu'elles envoyaient, c'est alors que nous avons conçu l'outil et la technique pour permettre l'interception de ces communications.

Cependant, il est important de souligner que l'atteinte à la vie privée ne vient pas de l'outil utilisé. Elle provient de la capture de l'audio ou du message texte ou de la communication entre deux personnes, et nous avons évolué dans l'utilisation des outils à mesure que les individus ont évolué dans leur façon de communiquer.

● (1625)

M. James Bezan: Alors...

Le président: Je vous remercie. Non, vous avez dépassé un peu le temps imparti, mais je tenais à entendre cette réponse...

M. James Bezan: Merci.

Le président: ... sans interrompre, mais nous devons maintenant donner la parole à Mme Khalid pour au plus six minutes.

Mme Iqra Khalid: Merci, monsieur le président, et par votre entremise, merci à nos témoins de leur présence.

Pour mettre tout cela en contexte, je vais demander d'abord combien d'enquêtes la GRC a menées en général au cours des cinq dernières années?

Sergent Dave Cobey (sergent, conseiller gestion des dossiers techniques, Programme de gestion des dossiers techniques, Gendarmerie royale du Canada): Par votre entremise, monsieur le président, voulez-vous connaître le nombre total d'enquêtes?

Mme Iqra Khalid: Oui, le nombre total d'enquêtes.

Sgt Dave Cobey: Sur le vif, je ne connais pas le nombre, mais ce doit être un très grand nombre.

Mme Iqra Khalid: D'accord, et sur ce très grand nombre, les OEE ont été utilisés dans combien d'enquêtes? J'ai entendu dire que c'était 32 ou 35, et je tenais simplement à le préciser.

Sgt Dave Cobey: Oui, depuis 2017, il n'y a eu que 32 enquêtes dans lesquelles on a eu recours à des OEE.

Mme Iqra Khalid: Et combien de ces enquêtes ont été menées sans mandat?

Sgt Dave Cobey: Monsieur le président, par votre entremise, je précise qu'une autorisation judiciaire pour utiliser les OEE avait été obtenue dans chacune de ces 32 enquêtes.

Mme Iqra Khalid: Et quels types d'activités criminelles étaient en cause lorsque les OEE ont été utilisés dans ces cas précis?

Sgt Dave Cobey: Monsieur le président, je crois que cette information se trouve dans le dossier qui a été fourni.

La liste se ventile en plusieurs types différents. La plupart des enquêtes sont liées au terrorisme ou au trafic de drogue grave. Il y a eu aussi cinq enquêtes pour meurtre et quelques enquêtes pour abus de confiance, l'une d'elles visant les activités d'un policier. Toutefois, au total, toutes catégories confondues, 32 enquêtes comportaient toutes au moins une infraction à l'article 183, comme le ministre l'a souligné lors de la réunion précédente. Ce sont toutes des infractions graves.

Mme Iqra Khalid: Merci.

La GRC est assujettie à la Loi sur la protection des renseignements personnels. Quelles pratiques utilisez-vous en général dans votre service pour vous assurer que vos outils d'enquête embarqués sont conformes à cette loi?

Sgt Dave Cobey: Je peux dire que, tout récemment, lorsque nous avons lancé le Programme national d'intégration des technologies, le rapport du CPVP sur Clearview AI en a été la genèse. Par suite de ce rapport, l'une des recommandations du CPVP, que la GRC a accepté de mettre en oeuvre, était d'avoir un processus plus centralisé pour garantir que tous les facteurs relatifs à la protection de la vie privée étaient pris en compte, y compris l'évaluation, tôt dans le processus, de la nécessité d'une EFVP et, le cas échéant, l'assurance que cette EFVP est rédigée ainsi que d'autres exigences internes de la GRC liées à la sécurité des données, et la détermination de la nécessité d'un mandat. Si un mandat est prescrit, les conditions et le langage nécessaires pour bien décrire les technologies y figurent ainsi que d'autres éléments du genre.

Mme Iqra Khalid: Le CPVP nous a dit plus tôt aujourd'hui que la GRC a mis du temps à le contacter. Pourquoi?

Sgt Dave Cobey: En termes précis, je n'en suis pas sûr en ce qui concerne les OEE en particulier, mais je peux vous dire que par suite de l'examen du CPVP et depuis la formation du CPSNR, nous redoublons d'efforts pour répertorier ces technologies le plus tôt possible et, si les renseignements personnels sont en jeu, nous entamons le processus de consultation du CPVP dès que possible.

Mme Iqra Khalid: Je vous remercie.

En ce qui concerne la portée des OEE dans le cadre d'enquêtes, le risque est-il grand que les OEE saisissent les communications de personnes qui ne sont pas le sujet ou la cible d'une enquête, par exemple? La GRC prend-elle des mesures d'atténuation pour s'assurer que leur portée est très limitée?

Sgt Dave Cobey: L'une des pièces jointes que vous avez reçues est le modèle d'autorisation judiciaire que nous avons communiqué à l'OSSNR aux fins de sa démonstration. Pour répondre brièvement à votre question, l'autorisation préparée dans le cadre d'un recours à des OEE comporte plusieurs conditions imposées par le juge, qui nous obligent à... Si des renseignements sans rapport avec l'enquête ou non pertinents pour les infractions visées par l'enquête sont saisis, alors oui, ils doivent être mis de côté et traités de manière protégée, tout comme d'autres renseignements, par exemple, les renseignements liés au secret professionnel de l'avocat et d'autres choses du genre.

Bon nombre des conditions incluses dans un mandat ordinaire obtenu en vertu de la partie VI ou dans un mandat d'écoute électronique sont incluses et implicites dans nos mandats autorisant l'utilisation d'OEE. À mesure que nous avons utilisé ces nouveaux outils au fil des ans, nous avons essayé d'adopter une approche prudente pour les mettre en oeuvre afin de garantir que ces conditions sont respectées.

● (1630)

Mme Iqra Khalid: Je vais vous poser aussi une question qui a été posée plus tôt au ministre. Elle se rapporte à la discrimination raciale. Comme nous l'a révélé la technologie de reconnaissance faciale, la race est un élément important de la surveillance. La GRC travaille sur cette question, mais son bilan n'est pas reluisant.

Je me demande si vous avez quelque chose à dire à ce sujet et quelles mesures vous prenez lorsque vous utilisez des technologies comme celle-ci, dans leur portée limitée, pour garantir qu'il n'y a pas de profilage racial.

Sgt Dave Cobey: En ce qui concerne les OEE en particulier, je peux vous dire que notre groupe des services d'enquête technique est un groupe de soutien technique qui prête son concours aux enquêteurs. Notre participation se situe au niveau de l'évaluation des technologies qui sont en jeu dans les enquêtes, plutôt que des cibles précises. En réalité, notre groupe n'est pas à même d'exercer une influence sur ce point, car nous examinons les dispositifs et les défis techniques de la collecte ou de l'interception que les enquêteurs tentent de réaliser.

Le président: Très bien.

[*Français*]

Monsieur Villemure, vous avez maintenant la parole.

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

Je remercie aussi les témoins de comparaître devant nous aujourd'hui.

Sans compromettre la sécurité nationale, mais afin que les citoyens de la circonscription de Trois-Rivières puissent bien comprendre certains éléments, j'ai une série de questions à vous poser.

Mes questions sont très simples, et vous pourrez y répondre par oui ou non.

La GRC est-elle en mesure d'installer un logiciel espion sur un téléphone cellulaire à l'insu de son utilisateur?

[*Traduction*]

Sgt Dave Cobey: Oui.

[*Français*]

M. René Villemure: La GRC est-elle capable de capter ou d'écouter une conversation sur un téléphone cellulaire?

[*Traduction*]

Sgt Dave Cobey: Avec une autorisation judiciaire, oui.

[*Français*]

M. René Villemure: J'en conviens, évidemment.

La GRC est-elle capable de capter ou de visionner ce qui est dans le champ du téléphone cellulaire avec la caméra?

[*Traduction*]

Sgt Dave Cobey: Selon le dispositif et nos capacités à ce moment-là, la réponse peut être oui.

[*Français*]

M. René Villemure: La GRC est-elle capable de consulter les informations, le calendrier, les photos ou les messages textes, c'est-à-dire ce qui se trouve dans le téléphone?

[*Traduction*]

Sgt Dave Cobey: Avec la même réserve, oui.

[*Français*]

M. René Villemure: C'est parfait.

Je vous remercie beaucoup.

Nous avons entendu le témoignage du commissaire à la protection de la vie privée ce matin. Tantôt, le ministre a dit que vous étiez pleinement engagés à l'égard du commissaire.

Avant d'utiliser ces logiciels pour la première fois, avez-vous, oui ou non, consulté le commissaire à la protection de la vie privée?

[*Traduction*]

Comm. adj. Mark Flynn: Non.

[*Français*]

M. René Villemure: D'accord.

Je vous remercie beaucoup.

Je poursuis sur un autre sujet.

L'autre jour, la lettre que nous avons reçue de la commissaire Lucki m'a également déçu. Nous avions posé une question assez claire et nous avons eu une réponse très claire. Nous avions demandé si des parlementaires avaient été mis sous écoute et on nous a répondu que cette information ne serait pas fournie par la GRC.

Avez-vous quelque chose à ajouter là-dessus?

[*Traduction*]

Comm. adj. Mark Flynn: J'ajouterais simplement que lorsque nous parlons d'une personne en particulier, il est difficile de poser une question à propos de parlementaires en particulier parce que cela autorise en fait les personnes qui la posent à parler de quelque chose qui leur tient à coeur.

Pour nous, la protection de la vie privée de tous les Canadiens, quelle que soit la position qu'ils occupent, est très importante, et c'est pourquoi nous avons mis en place toutes ces protections. Cependant, j'ajouterais qu'il y a certains secteurs — dont les parlementaires, les journalistes, les institutions religieuses et les établissements d'enseignement — à l'égard desquels nous avons mis en place des mesures de protection supplémentaires dans nos politiques et procédures pour garantir qu'un niveau d'autorisation plus élevé est requis si une demande est soumise ou si un besoin opérationnel existe en raison du comportement criminel des personnes en cause qui font partie de ces secteurs. Cela nécessite un niveau d'approbation plus élevé. Pour les questions de sécurité nationale, c'est ma position en tant que commissaire adjoint chargé de la sécurité nationale.

[*Français*]

M. René Villemure: Je vous remercie beaucoup.

Des partis politiques ont-ils déjà fait l'objet de surveillance?

● (1635)

[*Traduction*]

Comm. adj. Mark Flynn: Encore une fois, cela revient à parler de cibles d'enquêtes précises. Je peux dire que les partis eux-mêmes... Je suis fermement convaincu, sans avoir passé en revue toutes les autorisations judiciaires — et j'émets ici une forte réserve à ce sujet —, que la GRC ne cible pas les partis politiques.

[*Français*]

M. René Villemure: Je vous remercie beaucoup. Je suis très heureux de l'entendre.

Considérant le fait que les technologies évoluent rapidement, croyez-vous qu'il devrait y avoir une forme de moratoire sur leur utilisation afin que les gens comprennent ce qui est en jeu?

Force est d'admettre que c'est complexe. Croyez-vous qu'un moratoire est une bonne idée afin de permettre à plus de gens de s'exprimer et de comprendre ce qui se passe?

[*Traduction*]

Comm. adj. Mark Flynn: Je ne crois pas qu'un moratoire s'impose.

Encore une fois, pour revenir au point que j'ai soulevé plus tôt sur ce qui a conduit à l'évolution du recours à cette technologie, nous parlons des techniques les plus intrusives que nous pouvons utiliser lorsque nous parlons d'interception de communications, qu'il s'agisse d'une conversation téléphonique analogique ou d'une conversation chiffrée. Nous devons protéger la vie privée, sans égard à la difficulté ou à la complexité de la technologie utilisée. La GRC a protégé cette technologie. Les lois du Canada ont protégé ce droit à la vie privée, sans égard au degré de sophistication requis. Je pense que ces protections sont valables aujourd'hui, comme elles l'étaient dans les années 1960.

[*Français*]

M. René Villemure: Je vous remercie beaucoup.

Monsieur Larkin, tantôt, vous avez évoqué des partenaires étrangers. Vous avez dit que vous ne vouliez pas compromettre des enquêtes de l'extérieur.

Pouvez-vous nous dire si des Canadiens peuvent faire l'objet d'une surveillance par des entités étrangères?

[*Traduction*]

S.-comm. Bryan Larkin: Merci beaucoup, monsieur Villemure.

Je vais demander au commissaire adjoint Mark Flynn, qui s'occupe de nos services de sécurité nationale et de protection, de répondre à cette question.

Cependant, en ce qui concerne votre point précédent, j'aimerais souligner à nouveau que la GRC reconnaît que le cadre législatif actuel comporte des lacunes. Nous pensons que votre travail est très important pour renforcer les protections et atténuer ces risques, pour combler ces lacunes, et nous sommes très ouverts à travailler dans ce processus de transparence. Je pense qu'il est très important que nous reconnaissions que l'évolution de la technologie dépasse notre capacité à la suivre et qu'il faut améliorer le cadre législatif pour atténuer ces risques afin que nous puissions garantir l'accessibilité et la responsabilisation, mais aussi la protection de la vie privée des Canadiens.

Je cède la parole à Mark Flynn pour qu'il réponde à votre question précise, monsieur Villemure.

[*Français*]

M. René Villemure: Je vous remercie.

[*Traduction*]

Comm. adj. Mark Flynn: Si possible, pourriez-vous répéter le point clé de la question? Je veux simplement être certain...

[*Français*]

M. René Villemure: Un peu plus tôt, j'ai entendu M. Larkin évoquer des partenaires étrangers. Je me demande si des partenaires étrangers — il pourrait s'agir de pays — surveillent actuellement des Canadiens.

[*Traduction*]

Comm. adj. Mark Flynn: La distinction clé dont j'avais besoin était « partenaires étrangers ».

Comme vous le savez, des accords internationaux conclus avec certains partenaires prévoient qu'il n'y aura pas de surveillance de nos citoyens, en particulier parmi les membres du Groupe des cinq.

Cependant, en raison de ma position dans le domaine de la sécurité nationale, je dirais que vous devez vous préoccuper, que vous devez être conscients que des États étrangers qui ne sont pas des partenaires utilisent sans aucun doute ces types d'outils et de techniques. Je vois ici même de nombreux dispositifs électroniques. Vous les utilisez tous autant que tout le monde dans la société d'aujourd'hui, et vous devez être inquiets et conscients que vous êtes ciblés. Je n'ai que très peu de doutes à ce sujet.

[*Français*]

M. René Villemure: Je vous remercie beaucoup.

[*Traduction*]

C'est une réponse claire.

Le président: Merci pour cette réponse franche. Nous avons dépassé le temps imparti pour ce tour, mais nous avons obtenu des renseignements importants.

Nous passons maintenant à M. Green.

M. Matthew Green: Merci.

Qui est le plus haut gradé de vous trois?

S.-comm. Bryan Larkin: Monsieur Green, c'est moi, le sous-commissaire aux services de police spécialisés. Je suis récemment passé d'un service de police municipal où j'étais chef de police...

M. Matthew Green: Je sais bien que vous avez fait beaucoup de travail dans la région de Waterloo.

S.-comm. Bryan Larkin: ... au poste de commissaire adjoint des services de police spécialisés. L'un de mes mandats a été de veiller à ce que le travail soit...

M. Matthew Green: J'ai simplement besoin de cette confirmation. Je vous en remercie. Vous comprendrez aussi qu'en raison de nos tours minutés, nous devons être expéditifs.

Vous m'avez probablement entendu demander au ministre responsable que la GRC nous fournisse l'évaluation des facteurs relatifs à la vie privée en voie d'élaboration à l'intention du commissaire à la protection de la vie privée. En tant que plus haut gradé, pourriez-vous vous engager à le faire, à nous transmettre cette étude au moment opportun, lorsqu'elle sera prête?

S.-comm. Bryan Larkin: Je le répète, monsieur Green, nous sommes tout à fait disposés à promouvoir la transparence au sein de la GRC. Nous attendons avec impatience notre rencontre du 23 août. Nous envisagerions assurément de vous communiquer ce document, tandis que nous nous employons à augmenter la transparence et à renforcer la confiance au sein de la population canadienne, alors oui.

● (1640)

M. Matthew Green: Pour que les choses soient claires, nous avons le pouvoir de demander des documents sans restriction. Je préférerais ne pas avoir à présenter une motion pour demander ce document. Si je pouvais simplement obtenir officiellement votre engagement aujourd'hui, inscrit dans les témoignages du Comité, que nous pourrons le faire... S'il y a des éléments dans l'évaluation des facteurs relatifs à la vie privée qui... je vous ferai remarquer que nous avons la possibilité de travailler à huis clos, comme le CPSNR, comme d'autres comités.

Cela dit, monsieur le président, on a évoqué à quelques reprises un certain malaise à l'idée d'avoir des discussions à propos des partenaires et des lieux d'origine de cette technologie.

Étant donné que vous vous êtes engagé, monsieur Larkin, à nous fournir l'évaluation des facteurs relatifs à la vie privée au moment opportun, lorsqu'elle sera prête, seriez-vous prêt à comparaître à huis clos devant nous pour approfondir peut-être le recours à cette technologie afin que nous disposions des mêmes renseignements dont le gouvernement dispose?

S.-comm. Bryan Larkin: Monsieur le président, simplement pour préciser une réserve, monsieur Green, ce serait oui en ce qui concerne l'évaluation des facteurs relatifs à la vie privée, mais en reconnaissant qu'elle peut renfermer des renseignements de nature délicate qu'il serait préférable de communiquer à huis clos.

M. Matthew Green: D'accord.

S.-comm. Bryan Larkin: Encore une fois, nous nous réjouissons de l'occasion de vous rencontrer à huis clos pour communiquer plus de détails, comme nous le faisons avec le CPSNR. Nous sommes certainement disposés à le faire. Nous nous réjouissons de cette possibilité.

M. Matthew Green: Bien.

Comme vous le savez certainement, l'un des principes de l'arrêt Peel est que la capacité de la police à s'acquitter de ses fonctions dépend de l'approbation des interventions de la police par le public. Je pense que vous étiez présents lorsqu'on a fait état de problèmes de confiance dans des témoignages précédents.

Des membres de votre service ont refusé de nous fournir des renseignements fondamentaux, ce qui me semble en contradiction avec votre devoir de franchise. J'espère que, le moment venu, nous aurons l'occasion de vous inviter à nouveau à huis clos pour approfondir ce que nous avons appris en tant que comité. Encore une fois, nous avons quatre réunions. Je pense que nous aurons probablement l'occasion de revenir sur une partie de ces questions lorsque l'évaluation des facteurs relatifs à la vie privée sera prête.

Monsieur le président, le ministre responsable nous a répété qu'il attendait avec impatience nos recommandations et, malgré certaines protestations de la part de membres du gouvernement faisant partie de notre comité, qu'il était en fait très heureux que nous nous penchions sur ce sujet.

S'il y a un point qui m'agace dans notre débat, c'est celui des processus de surveillance. On y fait référence dans une lettre type. Avez-vous eu connaissance de la lettre type que la GRC nous a fournie? Elle concernait un mandat. J'y ai fait référence ce matin. Il y est question des interceptions réalisées à l'aide d'outils d'enquête embarqués. C'est à la page 6, au point d, où l'on dit que:

> d. Lorsque des communications orales ont été interceptées à l'aide d'un OEE, le moniteur 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.

Seriez-vous prêt à dire officiellement que ce paramètre est une pratique courante dans le cadre de ces mandats?

Sgt Dave Cobey: Oui.

M. Matthew Green: D'accord, je vous vois hocher de la tête. C'est inscrit au procès-verbal, oui.

Qui serait chargé d'exercer la surveillance nécessaire pour que cela soit le cas?

Sgt Dave Cobey: Je vois que vous avez un exemple. Les mandats sont délivrés par un juge. Les services d'enquête technique auraient un rôle à jouer pour veiller d'un point de vue technique à ce que le mandat soit exécuté conformément aux conditions. Puis, en ce qui concerne les renseignements recueillis ou, comme vous le dites, leur examen concret, cela relèverait de l'équipe d'enquête. Un petit nombre de personnes — vous avez mentionné les contrôleurs — et les analystes affectés au premier examen seraient chargés de veiller au respect des conditions.

Puis, bien sûr, le...

M. Matthew Green: Pour que je comprenne bien, encore une fois, comme nous essayons de recueillir des renseignements pour notre propre processus de preuve et la possibilité de demander des documents et ainsi de suite, sur ces 32 mandats, y aurait-il ensuite une vérification ou un rapport qui confirmerait que cette protection juridique contre l'atteinte à la vie privée de simples citoyens non liés à l'enquête serait assurée?

Sgt Dave Cobey: Je ne suis pas au courant qu'un rapport soit produit pour chaque cas, mais la responsabilité ultime entrerait en jeu lorsque les pratiques, les méthodes de collecte d'éléments de preuve, seraient contestées en cour lorsque ces accusés...

M. Matthew Green: Ce n'est pas proactif. Assurément, ce n'est pas la meilleure option de politique interne pour protéger la vie privée des citoyens canadiens. Face à cette technologie émergente, avez-vous envisagé des moyens proactifs de mettre en place vos propres contrôles internes? Bien franchement, nous entendons sans cesse de la part du gouvernement et des organismes d'application de la loi que nous devons les croire sur parole. Je vous demande maintenant, comme vous êtes responsable de l'examen de la légalité et des protections garanties par la Charte, et bien franchement, si je comprends bien, la seule personne qui a accès à la question de savoir si oui ou non vous faites ce qui est prévu dans les mandats, y a-t-il des mécanismes de rapport au sein de vos services pour illustrer le respect continu des mandats tels qu'ils sont libellés?

● (1645)

Sgt Dave Cobey: Je ne sais pas si une description de ces mesures vous intéresserait, mais je peux vous dire que nous avons mis en oeuvre plusieurs mesures proactives pour garantir que les mandats ou les OEE sont mis en oeuvre de façon efficace. Au début du processus, nous n'avons pas explicitement envisagé la production d'un tel rapport.

M. Matthew Green: D'accord, je vous remercie.

Le président: Très bien, merci.

Sur ce, nous passons au deuxième tour.

Le premier intervenant est M. Kurek.

Allez-y.

M. Damien Kurek: Merci beaucoup, monsieur le président, et merci aux membres de la GRC qui sont ici. Je vous remercie aussi pour le travail que vous faites pour protéger les Canadiens.

J'ai quelques questions auxquelles j'espère obtenir une réponse aussi directe que possible. Premièrement, nous avons beaucoup entendu parler du nombre d'autorisations, du nombre de personnes et du nombre de dispositifs touchés, bien qu'il y ait quelques divergences à ce sujet. Ce n'est pas explicitement le chiffre qui m'intéresse, mais plutôt le nombre de demandes d'autorisations judiciaires qui ont été présentées et qui ont été refusées. Connaissez-vous ce chiffre?

Sgt Dave Cobey: Voulez-vous dire les autorisations judiciaires, ou les demandes internes de recours à des OEE?

M. Damien Kurek: Les deux, si vous pouvez. J'aimerais obtenir le nombre de demandes d'utilisation d'OEE en interne et les autorisations judiciaires qui ont été refusées, donc je suppose que ce sont deux chiffres différents.

Sgt Dave Cobey: Le nombre d'autorisations refusées au titre de la partie VI est suivi dans le rapport annuel sur la surveillance électronique présenté au gouvernement fédéral, donc ces chiffres s'y trouvent. Voulez-vous l'autre chiffre également?

M. Damien Kurek: S'il vous plaît.

Sgt Dave Cobey: En passant, en ce qui concerne le nombre d'enquêteurs qui demandent des OEE par rapport au nombre d'enquêtes dans lesquelles des OEE sont déployés, je dirais que parmi les enquêtes dans lesquelles on demande ou on souhaite recourir à des OEE, une sur dix passe effectivement par notre processus et donne lieu au déploiement d'OEE. Comme notre processus est assez rigoureux et que la mise en oeuvre de ces outils est très difficile, très peu d'enquêteurs qui les demandent finissent par pouvoir les utiliser.

M. Damien Kurek: En ce qui concerne les recours à des OEE — et c'est évidemment une pratique très compliquée et nous avons beaucoup parlé des aspects techniques — le secret professionnel est l'un des défis qui ont été soulevés à l'égard du recours à ce type de technologie. Existe-t-il des exemples de recours à des OEE où les enquêteurs ont été confrontés au secret professionnel de l'avocat dans le cadre de l'utilisation de cette technologie de surveillance? Des protocoles ont-ils été mis en place pour garantir que les droits des Canadiens sont protégés à cet égard?

Sgt Dave Cobey: En un mot, oui; il y a des protocoles en place. L'exemple de mandat que vous avez reçu, qui est l'exemple d'autorisation au titre de la partie VI, comprend des conditions précises relatives au secret professionnel de l'avocat, et qu'il s'agisse de renseignements recueillis par OEE ou lors d'un appel téléphonique traditionnel, ces conditions doivent être respectées.

M. Damien Kurek: J'aimerais poser quelques autres questions concernant le témoignage...

J'ai siégé à ce comité au cours de deux législatures et il y a eu des désaccords très publics entre la direction de la GRC et le Commissariat à la protection de la vie privée et, comme on l'a dit aujourd'hui, il y a une certaine frustration du fait que la GRC semble hésiter à divulguer des documents au Parlement. Êtes-vous au courant du témoignage que le commissaire à la protection de la vie privée a présenté ce matin? Seriez-vous d'accord pour dire que ce n'est qu'après que cette information a été rendue publique à la fin du mois de juin que la GRC a communiqué avec le Commissariat à la protection de la vie privée concernant précisément l'utilisation des OEE dans vos enquêtes?

Comm. adj. Mark Flynn: Je suppose, encore une fois, que cela revient à l'évolution de la technologie, parce que, depuis 20 ans que je participe au débat sur l'accès légal, l'utilisation de ce type de technologie et les défis que présente le cryptage pour la GRC et les services de police en général ont été un sujet de discussion auquel ont participé le commissaire à la protection de la vie privée, la politique de droit pénal du ministère de la Justice et la section des droits de la personne pendant de nombreuses années.

Pour en revenir à une période plus récente et à la date de juin, je ne me souviens pas de l'ordre exact, mais je sais que les opérations techniques ont invité le bureau du commissaire à la protection de la vie privée à la présentation qui aura lieu en août.

En outre, vous remarquerez que des articles publics ont été publiés par des personnes comme le sergent Dave Cobey, ici présent, dans le but d'offrir une plus grande visibilité publique sur ce que nous faisons. Nous levons le voile. Nous essayons de le faire d'une manière professionnelle, qui respecte à la fois la loi sur la protection des outils et des techniques...

● (1650)

M. Damien Kurek: Si je peux me permettre, parce que mon temps de parole est presque écoulé, une des préoccupations qui, je pense, a été soulignée par ce comité est qu'il semble que ce n'est qu'après que des détails ont été révélés — et cela ne se limite pas à cette circonstance — que la GRC est franche au sujet de certains des détails liés à son enquête.

J'aimerais simplement ajouter une chose pour le compte rendu, et il s'agit d'une distinction importante. Le CPSNR est un comité de parlementaires, et non un comité permanent du Parlement, et je pense que c'est une distinction importante qui doit être faite.

Le président: Je vous remercie.

Sur ce, votre temps est écoulé.

Nous passons maintenant à Mme Hepfner pour cinq minutes.

Mme Lisa Hepfner: Merci beaucoup, monsieur le président.

Je remercie les membres de la GRC qui sont avec nous aujourd'hui.

J'aimerais commencer par demander pourquoi ne pas faire une évaluation des facteurs relatifs à la vie privée chaque fois que la GRC commence à utiliser une nouvelle technologie? Pourquoi une EFVP ne serait-elle pas l'une des premières choses que vous faites?

Comm. adj. Mark Flynn: Pour revenir au point que j'ai soulevé plus tôt, c'est un débat que nous avons et, parfois, il inclut aussi une discussion avec le groupe consultatif du gouvernement et avec le bureau du commissaire à la protection de la vie privée également, mais nous examinons ce que nous faisons.

Comme je l'ai dit, qu'il s'agisse de l'interception d'une communication analogique ou d'une communication cryptée, la vie privée se trouve dans le contenu, et non dans la méthode d'obtention. Au fur et à mesure que nous avançons dans le temps, nous nous demandons si nous envahissons effectivement la vie privée des gens. Lorsque nous en arrivons au point de penser qu'il y a des soucis... J'ai personnellement participé à des réunions où l'on nous a dit qu'aucune EFVP n'était requise parce que nous n'atteignions pas les seuils de déclenchement. En tant qu'organisation, nous changeons notre position sur ces questions, et je dirais même que dans un cas particulier, nous allons de l'avant avec l'évaluation des facteurs relatifs à la vie privée même si tous les conseils que nous avons reçus disent qu'elle n'est pas nécessaire.

Nous essayons d'avancer. Nous allons de l'avant. Vous avez trois personnes à cette table aujourd'hui qui croient fermement qu'il faut pécher par excès dans la révélation de détails et permettre aux gens d'évaluer correctement s'il y a effectivement une atteinte supplémentaire à la vie privée ou si nous ne faisons pas simplement les choses en utilisant une nouvelle méthode, mais au même degré essentiellement d'intrusion de la vie privée qu'auparavant, lorsque cela était autorisé par le pouvoir judiciaire.

Mme Lisa Hepfner: D'après vos renseignements de base ici, il semble qu'il vous faut... deux mandats, un mandat d'enregistreur de données de transmission et un mandat général, pour intercepter les fonctions informatiques et utiliser les OEE. Faut-il deux mandats?

Selon vous, les juges s'intéressent-ils vraiment à la vie privée des personnes non apparentées? Les juges se préoccupent-ils de la vie privée des Canadiens lorsqu'ils évaluent ces mandats?

Sgt Dave Cobey: Pour répondre à votre question, il y a plus de deux mandats. Principalement, l'ordonnance omnibus que nous demandons exige, en plus des exigences de la partie VI, qui est le mandat d'interception des communications privées, un mandat général qui est requis pour le déploiement et l'utilisation de l'OEE, la technologie en arrière-plan. Il y a un mandat d'enregistrement des données de transmission, qui est nécessaire pour recueillir les données de transmission requises pour leur exploitation, puis, si l'OEE est utilisé pour recueillir des renseignements liés à l'emplacement du dispositif, nous demandons également un mandat de localisation. Tous ces mandats sont principalement inclus dans les autorisations que nous demandons.

À l'occasion, nous demandons un mandat général si l'objectif est de rechercher à distance des renseignements historiques dans un appareil, mais la plupart du temps, nous utilisons ces outils pour des enquêtes en cours et nous cherchons des communications prospectives, des communications privées. Donc, tous les mandats que j'ai énumérés, y compris une ordonnance de mise sous scellés et une ordonnance d'assistance, sont demandés en même temps.

Mme Lisa Hepfner: Je pense que c'est M. Flynn qui a parlé de l'utilisation d'une technologie semblable dès 2012. Je ne pense pas que nous ayons entendu beaucoup de détails sur cette technologie et sur ce qui se faisait en 2012, alors je me demande si je peux vous donner la chance de développer ces commentaires.

● (1655)

Comm. adj. Mark Flynn: J'ajouterai un élément. Je crois que les juges tiennent absolument compte du facteur protection de la vie privée. C'est leur principale responsabilité lorsqu'ils évaluent la mesure dans laquelle les forces policières ont besoin d'utiliser ces techniques.

Pour revenir en arrière, l'affaire Delisle a été évoquée dans l'une des questions précédentes. Si l'on prend l'affaire Delisle, on peut voir dans la couverture médiatique que la GRC, dans le cadre de son dossier de divulgation, a présenté certains des documents recueillis à l'aide de l'OEE. Il s'agissait notamment de captures d'écran de certaines communications entre l'accusé dans cette affaire et ce que l'on pense être des acteurs étrangers avec lesquels il était en relation.

Lorsqu'il est question de cette technologie, on l'entend qualifiée de « logiciel espion » et de « logiciel malveillant ». Je vais être franc. Je crois que ce n'est ni l'un ni l'autre. Nous utilisons des outils et des techniques qui sont conçus pour nous permettre de faire le travail que l'on attend de nous pour ce qui est de recueillir des preuves sur les comportements criminels. Vous pouvez constater, d'après les statistiques fournies uniquement à partir de 2017, qu'il s'agit de cas graves et d'un degré de criminalité grave.

Mme Lisa Hepfner: Merci beaucoup.

Je crois que c'est tout le temps qui m'est alloué, monsieur le président, ou est-ce qu'il me reste du temps?

Le président: Non, nous l'avons dépassé un peu; vous avez donc terminé.

[*Français*]

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

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

Selon des documents qui ont été fournis, il y a eu une évaluation de la pertinence de lancer un débat public sur l'utilisation des technologies en 2016. Cela n'a pas été fait. Il y a peut-être des raisons à cela, que vous pourrez nous expliquer.

Y a-t-il une ouverture à l'idée de lancer un débat public sur l'utilisation des technologies intrusives?

[*Traduction*]

Comm. adj. Mark Flynn: Y a-t-il une ouverture à l'idée de parler de l'utilisation de techniques intrusives...? Je crois qu'un point important a peut-être échappé à la traduction.

Je dirais qu'il y a absolument une ouverture à l'idée de parler publiquement de l'utilisation des technologies invasives. Nous sommes là. Nous sommes heureux d'avoir cette discussion. Encore une fois, vous verrez les articles de presse qui en parlent, alors je ne vais pas vous faire perdre votre temps.

[*Français*]

M. René Villemure: Vous exercez vos fonctions depuis 2017.

Est-ce bien cela?

[*Traduction*]

Comm. adj. Mark Flynn: Je travaille dans le domaine de ces technologies depuis 2002. J'ai changé de poste en 2015, et maintenant j'occupe mon poste en sécurité nationale et en police de protection depuis décembre, il y a un an et demi.

[*Français*]

M. René Villemure: D'accord.

Je fais toujours allusion au désir de la GRC de lancer un débat public en 2016.

Est-ce que quelqu'un est en mesure de me dire pourquoi cela n'a pas été fait?

[*Traduction*]

S.-comm. Bryan Larkin: Je ne suis pas sûr que qui que ce soit parmi nous puisse donner la raison pour laquelle cela ne s'est pas produit en 2016. En toute franchise, monsieur Villemure, aucun d'entre nous ne participait réellement à ce processus à l'époque, alors...

[*Français*]

M. René Villemure: Si jamais vous trouvez la réponse, vous pouvez nous l'envoyer par écrit. Ce sont des documents de la GRC que je cite.

Comme M. Green l'a mentionné, nous parlons de confiance. Nous ne tentons pas de faire une chasse aux sorcières. L'idée est de vous aider à accomplir vos tâches dans les meilleures conditions possible.

Seriez-vous ouvert à l'idée qu'il y ait une vérification par une tierce partie ou qu'une tierce partie vous assiste afin que nous n'ayons pas l'obligation de vous croire?

[*Traduction*]

Sgt Dave Cobey: En un mot, oui. Notre participation avec des procureurs fédéraux et provinciaux chevronnés pour nous assurer de bien faire les choses en ce qui concerne la communication de suffisamment de détails aux juges est un exemple de cas où nous avons fait appel à des tiers pour essayer de bien faire les choses.

[*Français*]

M. René Villemure: D'accord.

Je vous remercie beaucoup.

[*Traduction*]

Le président: Merci.

Pour deux minutes et demie, nous avons M. Green.

M. Matthew Green: Je vous remercie.

Dans la dernière étude du Comité sur la technologie de reconnaissance faciale, les représentants de la GRC ont parlé au Comité d'une nouvelle stratégie nationale, le Programme national d'intégration des technologies, le PNIT. Ce programme est censé garantir que les nouvelles technologies sont évaluées avant d'être utilisées.

Pourquoi ne pas faire intervenir le commissaire à la protection de la vie privée de manière officielle?

S.-comm. Bryan Larkin: Merci beaucoup, monsieur Green.

Je pense que l'un de nos processus lorsque nous nous réunirons le 23 août sera de discuter de la façon dont nous modernisons et faisons évoluer le PNIT. Cela concerne toute la technologie, la technologie centralisée, afin que nous ayons une réglementation, une surveillance et de bons audits, et cela intègre également l'ACS+ et les évaluations juridiques, etc.

C'est une recommandation à laquelle nous sommes très ouverts et que nous attendons avec impatience.

M. Matthew Green: Étant donné que la GRC est actuellement assujettie à la Loi sur la protection des renseignements personnels, quelles pratiques sont actuellement en place, peut-être avec ce nouveau programme d'intégration, pour s'assurer que l'utilisation par la GRC d'outils d'enquête sur les appareils est conforme à cette loi?

Sgt Dave Cobey: Si vous le permettez, puis-je répondre brièvement à votre question précédente?

● (1700)

M. Matthew Green: Bien sûr.

Sgt Dave Cobey: En ce qui concerne le Programme national d'intégration des technologies et la participation du commissaire à la protection de la vie privée, je ne sais pas exactement où en est la situation, mais nous avons effectivement demandé si le commissaire verrait un avantage à intégrer quelqu'un dans notre programme.

M. Matthew Green: Quand cela se serait-il produit?

Sgt Dave Cobey: Cela se serait produit peu de temps après la publication du rapport.

M. Matthew Green: Encore une fois, cela témoigne, très franchement, de la manière réactive de la GRC et de sa culture d'après coup que j'ai observées.

Cela étant dit, j'ai toujours un peu de mal à comprendre ce qui se passe lorsque la surveillance se produit et qu'elle risque d'aller à l'encontre de notre objectif, et notre objectif concerne maintenant les personnes qui ne font pas l'objet d'une enquête. Ce processus serait-il également ouvert à une révision? Vous savez, avec 32 occurrences dont nous avons connaissance depuis 2017, il semble que le commissaire à la protection de la vie privée pourrait avoir un rôle important à jouer afin que nous, au Comité, n'ayons pas à découvrir les choses après coup dans les médias, ce qui est, très franchement, un peu problématique.

Sgt Dave Cobey: Je peux vous dire qu'en tant que personne au niveau opérationnel qui travaille tous les jours avec des enquêteurs et des spécialistes de la technologie pour que tout se passe bien, oui, nous serions heureux d'avoir plus d'engagement de la part de tiers comme le commissaire à la protection de la vie privée.

M. Matthew Green: Merci.

Le président: Je vous remercie.

Nous passons à M. Williams pour cinq minutes.

M. Ryan Williams: Merci beaucoup, monsieur le président.

Merci encore, messieurs, d'être venus aujourd'hui.

Je pense que l'équilibre le plus important que nous recherchons ici est l'équilibre entre la sécurité nationale ou votre travail d'enquête, qui est très important, puis l'assurance que nous avons la divulgation publique et la protection des lois sur la vie privée dans son ensemble. Nous savons que c'est parfois très difficile. Je pense que, comme l'ont indiqué nos collègues, si nous sommes ici, c'est en partie en raison d'un travail parlementaire qui consistait simplement à poser certaines questions au Parlement. Ce fut un choc ou une surprise pour les parlementaires de découvrir que quelque chose était utilisé et que personne n'en savait rien — y compris le commissaire à la protection de la vie privée auquel nous ferions confiance. Apprendre aujourd'hui que la technologie est utilisée depuis 10 ans...

Comme mes collègues l'ont dit, nous avons mené des enquêtes sur d'autres technologies, comme la technologie de reconnaissance faciale, et nous avons constaté que la GRC n'était pas totalement engagée dans le processus. Nous avons constaté l'absence de communication. Sachant cela, et sachant que l'outil demandé par le commissaire à la protection de la vie privée, qui sera mis en œuvre ici, en août, n'est pas encore disponible...

Je suppose que d'un point de vue général, pour que je puisse comprendre, pourquoi le commissaire à la protection de la vie privée n'a pas été invité à participer, même il y a trois ans, alors que cet outil était vraiment utilisé dans le système judiciaire pour différents processus? Quelle est la meilleure réponse à la question de savoir pourquoi le commissaire à la protection de la vie privée, qui dispose, comme il nous l'a expliqué ce matin, de systèmes complets et hermétiques permettant de garder tout confidentiel mieux que nous ne pouvons le faire dans un comité ouvert au public aujourd'hui...? Pourquoi cela n'a-t-il pas été la première mesure prise avec la GRC?

Comm. adj. Mark Flynn: Je peux remonter encore plus loin que les 10, voire 20 dernières années. Encore une fois, pour ce qui est de l'atteinte réelle de la vie privée, nous nous concentrons beaucoup sur l'outil et la méthodologie, mais l'atteinte de la vie privée consiste à écouter la conversation et à voir ce que les gens font physiquement. Nous le faisons depuis des années; j'ai suivi le programme complet de formation de la Sous-direction des affaires spéciales, qui porte sur l'installation de dispositifs d'écoute, de matériel et de caméras dissimulés discrètement dans un endroit particulier où se déroule un comportement criminel. Ceci est une nouvelle méthode d'atteinte à la vie privée, mais une atteinte à la vie privée au même degré que précédemment, que ce soit en utilisant ces autres techniques ou en s'infiltrant dans un ordinateur pour en extraire toutes les données — là encore, en respectant les conditions de l'ordonnance du tribunal.

Alors, lorsque vous nous demandez quand nous arrivons au point où nous constatons un degré d'atteinte à la vie privée autre qu'auparavant, c'est vraiment là que les déclencheurs interviennent pour nous. Pour ceux d'entre nous qui vivent et font ce travail depuis 20 ans, l'évolution semble lente. Il y a des moments où nous avons besoin de mécanismes de contrôle qui nous signalent qu'il est temps de réfléchir et de faire appel à de nouvelles personnes. Des personnes comme le sergent Dave Cobey sont arrivées. Il est un fervent partisan d'une plus grande publicité de ce que nous faisons. Il écrit des articles pour les différents journaux et revues pour essayer de donner de la visibilité à tout cela. C'est vraiment cela le déclencheur.

M. Ryan Williams: Je conviens tout à fait de tout cela, mais en même temps, nous sommes ici aujourd'hui, et ce dont nous parlons s'articule sur le mot « confiance ». Nous essayons de créer et de maintenir une confiance totale dans les institutions gouvernementales et la GRC. N'aurait-il pas été logique — pour contrer votre argument — que le commissaire à la protection de la vie privée soit le premier à s'engager dans ce processus pour assurer un degré maximal de confiance et de responsabilité?

● (1705)

Comm. adj. Mark Flynn: Comme je l'ai déjà dit, je sais que le bureau du commissaire à la protection de la vie privée, les commissaires précédents, la politique de droit pénal du ministère de la Justice, la section du droit de la personne, ont participé au débat sur l'accès légal qui explique la raison de l'utilisation de cette technologie et d'autres depuis deux décennies. Je sais que vous êtes tous bien conscients du débat sur l'accès légal et de ses aspects multigénérationnels.

Je sais que ces conversations ont eu lieu à certains niveaux. Je ne sais pas ce qui est parvenu jusqu'aux commissaires à la protection de la vie privée eux-mêmes. Je sais que nous avons eu des discussions. Je peux vous en mentionner une en particulier où nous avons eu une conversation très fructueuse avec le bureau du commissaire à la protection de la vie privée au sujet de l'accès légal. Nous avions le sentiment d'être bien compris, mais nous avons reçu par la suite des messages contraires. Nous avons participé à ce débat. Nous nous réjouissons de la transparence. Nous sommes ouverts à la transparence. Nous aimons le travail qui se fait.

M. Ryan Williams: Je pense qu'une partie ou l'ensemble du travail de ce comité consiste à formuler des recommandations, parce que nous modernisons également notre Loi sur la protection des renseignements personnels dans son ensemble, non seulement pour rattraper l'Europe et les Américains, mais aussi peut-être pour tenter de les devancer.

Ce que je vais demander, ce sont des recommandations écrites de votre part, pas seulement de la nôtre, sur ce qui pourrait se faire pour plus de transparence et moderniser de notre mieux la Loi sur la protection des renseignements personnels, y compris la protection de la confidentialité qui est nécessaire pour éviter que ce genre de chose se reproduise. Je pense que la partie la plus importante de notre dialogue est que nous avons confiance, confiance dans nos institutions gouvernementales. Nous l'avons dit et répété. Je pense que c'est de là que nous partons. C'est ce que nous voulons voir. Que nous recommanderiez-vous pour que cela soit maximisé?

Le président: Je vous remercie.

Je ne suis pas sûr que c'était vraiment une question, mais même si c'était le cas, nous n'avons pas le temps d'entendre une réponse.

M. Ryan Williams: J'aimerais la recevoir par écrit, si possible, par votre intermédiaire, monsieur le président.

Le président: Je pense qu'il s'agissait plutôt d'une demande de réponse écrite. Nous allons considérer qu'il s'agit d'une demande en ce sens et passer maintenant à Mme Valdez pour cinq minutes.

Mme Rechie Valdez: Merci à la GRC de se joindre à nous pour cette étude.

Monsieur le président, par votre intermédiaire, je vais adresser mes questions au sergent Cobey. Toute autre personne peut intervenir pour ajouter des remarques, au besoin.

Sergent Cobey, pouvez-vous nous donner quelques détails sur les critères utilisés par la GRC pour déterminer si ces outils d'enquête sur appareil sont utilisés?

Sgt Dave Cobey: Certainement.

La façon la plus utile pour moi d'expliquer les critères utilisés est de vous présenter brièvement notre processus.

Au départ, nous organisons une consultation avec les enquêteurs qui envisagent d'utiliser ces outils. Au cours de cette consultation, nous leur expliquons — nous démystifions ces outils et expliquons — à quel point ils sont compliqués et le fait qu'ils ne vont pas forcément être en mesure de fournir les preuves qu'ils souhaitent, et nous les encourageons vraiment à envisager d'autres outils moins invasifs si possible.

Tout d'abord, nous nous assurons qu'ils comprennent vraiment dans quoi ils s'engagent et qu'ils ont les ressources nécessaires pour le faire. À la suite de cette consultation, ils doivent soumettre une demande officielle de leur chaîne de commandement à nos services d'enquête technique afin que la direction soit informée et supervise leur demande pour s'assurer qu'elle a été correctement contrôlée.

Ensuite, si cette demande est approuvée de notre côté, nous procédons à une deuxième consultation avec le procureur de la Couronne. Ou, s'ils n'ont pas de procureur de la Couronne, nous insistons pour qu'un procureur de la Couronne soit désigné afin qu'il comprenne les risques et les avantages potentiels de l'utilisation de ces outils.

Nous précisons clairement au cours de cette consultation qu'il s'agit de nouvelles technologies et que nous nous attendons à ce qu'elles fassent l'objet de litiges. Nous nous assurons qu'ils comprennent le risque de litige et le genre de renseignements délicats que nous ne pouvons pas partager et que nous chercherions à protéger en vertu de l'article 37 ou de l'article 38 de la Loi sur la preuve au Canada.

Tout ce processus jusqu'à présent vise vraiment à s'assurer qu'ils comprennent que s'il y a un autre outil qui fonctionne, ils devraient l'utiliser, parce que ces outils sont compliqués. Encore une fois, rien ne garantit qu'ils fonctionneront.

Après toutes ces consultations, nous rédigeons une note d'engagement entre notre unité et l'unité requérante afin de consigner toutes les conversations et d'établir la nécessité de protéger les outils. Ce n'est qu'après l'accusé de réception de cette note d'engagement par l'agent responsable de l'enquête que l'assistance est fournie. Bien entendu, tout cela n'a aucune importance à moins qu'une autorisation judiciaire n'ait été accordée par le biais du processus que nous avons décrit précédemment en ce qui concerne un représentant de la Couronne, une autorisation en bonne et due forme avec toutes les conditions que nous avons précisées.

J'espère que cela répond à votre question.

● (1710)

Mme Rechie Valdez: Oui.

Quel genre de renseignements peut être obtenu au moyen des OEE, mais ne peut pas être obtenu par un simple mandat de perquisition?

Sgt Dave Cobey: Eh bien, en général, les OEE sont demandés pendant l'enquête, donc l'objectif des OEE, bien sûr, est de recueillir les renseignements pendant que la cible utilise encore l'appareil. Pour obtenir un mandat de perquisition, il faut retirer l'appareil à la personne concernée, et celle-ci cesse donc de l'utiliser. Les renseignements qui peuvent être recueillis sont ceux que le suspect utilise ou enregistre encore sur cet appareil avant que nous ne le saisissions, ou avant qu'il ne sache qu'il est la cible d'une enquête policière.

Mme Rechie Valdez: Merci.

L'ancien premier ministre Stephen Harper s'est beaucoup impliqué dans l'entreprise israélienne Corsight AI, dont la technologie permet d'identifier les traits de reconnaissance faciale dans des situations où ils sont difficiles à identifier.

Savez-vous si la GRC utilise une partie de cette technologie?

Sgt Dave Cobey: Personnellement, je ne suis pas au courant de cet outil particulier.

Mme Rechie Valdez: Je crois comprendre que des membres de l'opposition ont indiqué que la GRC a effectué une surveillance à grande échelle de la population et, en fait, de députés. Avez-vous des observations à faire à ce sujet?

Sgt Dave Cobey: Je reviens sur ce que j'ai dit précédemment, à savoir que ces outils ne sont jamais utilisés pour effectuer une surveillance à grande échelle. Encore une fois, l'autorisation judiciaire n'est accordée par un juge que si elle est nécessaire et si le juge est convaincu qu'une infraction particulière impliquant une personne particulière et des dispositifs particuliers ont été exposés, ainsi que la façon dont ces dispositifs seront interceptés. C'est très ciblé. Il ne s'agit jamais de surveillance générale.

Mme Rechie Valdez: Pouvez-vous décrire les obstacles que vous rencontrez dans l'exécution des mandats de perquisition et comment cette technologie peut-elle mieux aider la GRC à recueillir des preuves clés?

Sgt Dave Cobey: Je vais commencer par la deuxième partie de la question.

Je pense que cette technologie peut aider à recueillir des preuves précieuses parce que, comme chacun d'entre nous dans cette salle, les suspects criminels portent des appareils. Je soupçonne que chacun d'entre nous dans cette salle utilise un appareil d'une manière plus complexe pour les forces de l'ordre, avec les applications que nous utilisons et la façon dont nous utilisons nos appareils. Rien de tout cela n'est propice aux activités d'écoute électronique à l'ancienne qui nous permettaient simplement d'envoyer notre commande à une société de télécommunications et que celle-ci nous envoie les communications.

Compte tenu de tous les appareils et du fait que les utilisateurs ont entièrement le choix de l'appareil qu'ils achètent, des applications qu'ils utilisent et de la façon dont ils utilisent ces applications, les OEE sont essentiels, car ils nous aident à gérer toute cette complexité.

Le président: Très bien. Je vous remercie.

Mme Rechie Valdez: Merci.

Le président: Cela nous amène à la fin des deux premiers tours complets, selon la motion adoptée par le Comité. Je vais m'en écarter pour la simple raison que le temps devient un facteur.

Pour le troisième tour, nous passerons à quatre minutes chacun pour M. Bezan et M. Bains, deux minutes chacun pour M. Villemure et M. Green, puis quatre minutes chacun pour M. Kurek et Mme Khalid. Cela nous permettra de terminer à peu près à l'heure, ou peut-être une minute ou deux plus tard.

Sur ce, allez-y, monsieur Bezan, pour quatre minutes.

M. James Bezan: Merci. La discussion a été intéressante.

Lorsque vous demandez un mandat, la GRC doit-elle informer le fournisseur de services que quelqu'un qui a un de ses appareils — Rogers, Telus, Bell — a un système piraté par un logiciel espion de la GRC? Y a-t-il une obligation de divulgation?

Sgt Dave Cobey: Je ne caractériserais pas nos activités comme vous l'avez fait, mais je dirais que les fournisseurs de services ne sont pas impliqués lorsque nous utilisons les OEE.

M. James Bezan: D'accord, alors encore une fois, lorsque vous surveillez les conversations, que vous utilisez le microphone et que vous piratez les conversations et les courriels, qu'en est-il des autres parties, des tiers qui sont des spectateurs innocents, comme les amis, les parents et les conjoints, par exemple? Comment protégez-vous leur vie privée?

Sgt Dave Cobey: C'est une excellente question. La protection de la vie privée des tiers innocents et des communications non pertinentes est un problème depuis le début des écoutes téléphoniques. Si vous prenez l'exemple d'ordonnance que nous avons fourni, vous verrez qu'il y a des conditions. En mettant de côté les OEE pour un moment, il y a des modalités et conditions pour les écoutes normales. Encore une fois, nous allons revenir sur les communications privilégiées. Le secret de la communication entre un avocat et son client doit être protégé et traité de manière très spéciale. Il en va de même pour le données recueillies par OEE, et certaines des conditions de cet exemple d'ordonnance, qui est représentatif des ordonnances que nous demandons, incluent le fait que les renseignements non pertinents relatifs à des tiers et à d'autres personnes doivent être mis de côté, protégés et traités uniquement selon les directives du tribunal.

Un autre exemple précis, qui est également inclus dans cette ordonnance, est l'exigence que la fonction de « micro bavard » décrite dans le document technique ne peut être activée que s'il y a des motifs de croire que l'une des principales personnes connues, comme nous les appelons, les...

● (1715)

M. James Bezan: Dans le cas où vous avez le privilège du secret professionnel de l'avocat et que vous surveillez une personne qui rencontre son avocat et dit: « Au fait, non seulement nous blanchissons de l'argent, mais nous avons aussi une cargaison de drogue qui arrive par le port », vous ne donneriez pas suite à cette information?

Sgt Dave Cobey: Si une personne est en communication avec son avocat, les modalités et conditions sont claires. Les renseignements doivent être scellés, et nous ne pouvons pas les consulter sans une nouvelle ordonnance du tribunal.

M. James Bezan: Monsieur Flynn, rapidement, vous disiez que vous êtes là depuis longtemps dans ce dossier. Pouvez-vous nous parler du protocole d'entente que la GRC a avec le SCRS et avec le CST en particulier? Le Centre de la sécurité des télécommunications possède de nombreux logiciels espions qu'il utilise à l'échelle internationale sur des non-Canadiens. Quel genre de relation la GRC a-t-elle avec le CST?

Comm. adj. Mark Flynn: De façon générale, selon votre question, la GRC, du point de vue de la sécurité nationale, travaille en partenariat avec tous les organismes de sécurité nationale, qui comprennent évidemment le SCRS, le CST et l'ASFC. Je pourrais poursuivre avec une longue liste de partenaires en matière de sécurité nationale.

Plus précisément, en ce qui concerne notre relation avec le CST, celui-ci a un mandat qui lui permet de nous fournir un soutien technique par l'intermédiaire des opérations techniques qui gèrent cette relation avec le CST, mais je peux dire que cette relation n'étend pas les pouvoirs de la GRC.

M. James Bezan: Merci.

Monsieur le président, comme nous avons demandé des renseignements et que nous ne les avons jamais obtenus, j'aimerais proposer la motion suivante:

> 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.

Je vais parler de cette motion, monsieur le président, car je veux assurer aux membres du Comité et à la GRC que nous ne voulons pas nuire aux enquêtes qu'ils mènent actuellement sur la criminalité ou la sécurité nationale.

Ce que nous voulons voir, c'est la portée générale de ces mandats et les documents qui y sont associés. Grâce au processus d'examen que nous avons utilisé par le passé dans un certain nombre de comités parlementaires, le légiste et le conseiller parlementaire s'assureraient que les documents sont expurgés et que l'information qui nous est cachée en tant que membres du Comité est conforme à la protection de ces enquêtes, de la sécurité nationale et de la vie privée des personnes qui sont mises en cause.

J'ai transmis le texte de cette motion au greffier et j'ai demandé qu'il soit distribué. Tous les membres du Comité devraient avoir la motion devant eux maintenant. Je viens moi-même de la recevoir. Elle est dans les deux langues officielles.

Le président: Elle est recevable.

Avant de faire quoi que ce soit d'autre ou de revenir, avec le peu de temps qu'il nous reste, à des tours de questions, nous passons au débat.

Je donne la parole à Mme Khalid.

Mme Iqra Khalid: Merci, monsieur le président.

Je voudrais respectueusement soumettre aux membres... Évidemment, je n'ai pas eu l'occasion de l'examiner, mais la GRC est ici pour 11 minutes de plus. Je propose que nous revenions à nos témoins et que, après avoir examiné cette motion, nous l'abordions comme premier point à l'ordre du jour de la réunion de demain.

● (1720)

Le président: Je suppose que c'est une idée. Je peux sonder la salle.

Y a-t-il un intérêt dans...

M. James Bezan: Monsieur le président, je voudrais simplement dire ceci.

Je crois que nous devrions... Compte tenu du manque de renseignements fournis par la GRC... J'apprécie ce qu'ils nous ont donné. Ils nous ont donné des renseignements généraux, mais ils ne traitent pas de la portée plus large de la motion que nous avons présentée. En ce qui concerne le processus parlementaire...

Le président: Je ne faisais que...

M. James Bezan: Je vais simplement dire ceci. Nous devrions nous occuper de cette motion parce que demain nous avons un programme complet, et j'aimerais pouvoir entendre des témoins demain plutôt que de passer la journée à débattre de cette motion.

Le président: En effet.

M. Fergus a également levé la main. Est-ce que je vois quelqu'un d'autre dans la salle?

M. Fergus est le seul que je vois pour l'instant.

Allez-y, monsieur Fergus.

[*Français*]

L'hon. Greg Fergus (Hull—Aylmer, Lib.): Je voulais dire exactement la même chose que Mme Khalid. Pour moi, il est très tard. J'aimerais savoir si on peut lire la motion et continuer avec les témoins qui sont présents. Cela peut être la première chose que nous aborderons demain.

[*Traduction*]

Le président: Très bien. Sur le plan de la procédure, je ne suis pas...

Je vais avoir un mot rapide avec le greffier.

Bon, nous manquons vraiment de temps pour faire les deux — poser des questions supplémentaires à nos témoins et donner aux membres le temps d'examiner cette motion —, alors je suppose qu'à moins qu'il y ait une véritable motion d'ajournement ou de suspension du débat, il n'y a vraiment aucun moyen pour moi de traiter cette question.

Je vois que Mme Khalid a de nouveau la main levée, tout comme M. Fergus.

Allez-y, madame Khalid.

Mme Iqra Khalid: Merci, monsieur le président.

Je veux simplement réitérer parce que, d'après ce que nous avons entendu aujourd'hui de la GRC, du CPVP et du ministre, je pense qu'il y a peut-être d'autres documents que nous pourrions vouloir ajouter à cette liste. Par exemple, nous avons entendu dire qu'il y avait une certaine activité en 2012 que nous pourrions vouloir poursuivre. C'est pourquoi j'espérais que nous aurions le temps de revenir en arrière, d'examiner les témoignages et de voir comment nous pourrions renforcer cette motion — quels autres documents —, plutôt que de continuer à le faire de manière fragmentaire. Nous pourrions le faire de manière plus substantielle et plus complète.

Je suis, pour ma part, très intéressée par la mention de 2012 qui a été faite. Je sais que certains membres pourraient être intéressés par d'autres éléments que nous pourrions peut-être inclure dans le texte de cette motion. Je me demande simplement s'il y a des membres qui seraient prêts à donner un peu de temps pour voir si nous pouvons vraiment l'élargir.

Le président: Je vous remercie.

Monsieur Fergus, vous avez la parole.

[*Français*]

L'hon. Greg Fergus: Je vous remercie, monsieur le président.

Si vous voulez que je présente une motion pour ajourner le débat, c'est avec plaisir que je le ferai.

Je voulais savoir si nous pouvons conclure une entente entre collègues. Comme je l'ai dit, j'aimerais que nous abordions ce sujet demain matin dès le début de la rencontre, à 11 heures. Cela nous permettrait d'avoir le temps de lire les documents et de prendre en considération ce que Mme Khalid a suggéré.

Il y a peut-être un moyen de bonifier la motion. Accordez-nous quelques heures pour lire ces documents de manière à ce que nous puissions proposer des modifications. Nous pourrons ensuite avoir un excellent débat. Je pense que cela serait la meilleure façon de procéder, mais j'aimerais savoir si nous pouvons…

● (1725)

[*Traduction*]

Le président: Je vais devoir vous interrompre, monsieur Fergus. Si vous proposez en fait d'ajourner le débat, c'est une motion dilatoire et non discutable qui devrait faire l'objet d'un vote. Pour ce qui est de faire cela sans vote, je vois des sourcils froncés et des têtes secouées dans la salle, alors je ne sais pas si cela peut se faire autrement que par un vote.

Si vous avez proposé, monsieur Fergus, d'ajourner le débat, je vais devoir procéder à un vote.

[*Français*]

L'hon. Greg Fergus: M'entendez-vous bien?

[*Traduction*]

Le président: Je vous entends en traduction, mais vous n'êtes pas très fort dans la salle.

L'hon. Greg Fergus: Oh, donc, vous ne pouvez pas m'entendre en anglais?

Le président: Je peux vous entendre en anglais maintenant. C'est bon maintenant.

L'hon. Greg Fergus: Très bien.

Monsieur le président, je n'ai pas le plaisir d'être dans la salle. En fait, j'ai le grand plaisir de ne pas être dans la salle, étant donné l'endroit où je me trouve. N'avons-nous pas envie de tenir ce débat à la première heure demain matin?

Le président: Est-ce que je sens dans la salle un désir d'ajourner le débat?

M. James Bezan: Il propose l'ajournement. Faites ce qu'il faut.

Le président: Non, il n'y a pas de consensus, de toute façon, pour laisser cela jusqu'au matin. Il y a des membres qui tiennent beaucoup aux témoins. Nous avons une liste complète de témoins.

J'offre l'occasion... Nous avons fait deux heures. Pour ce qui est de demain, je pense que nous avons prévu du temps pour les travaux du Comité si nous prolongeons l'une des réunions de demain. Est-ce une possibilité?

L'hon. Greg Fergus: Cela me convient.

Le président: D'accord. Voici ma proposition. Après le temps accordé aux témoins demain — je le ferai peut-être après le premier groupe de témoins, juste au cas où les gens voyageraient après le deuxième groupe —, nous aurons du temps pour les travaux du Comité au cours duquel nous pourrons examiner à la fois la motion de M. Bezan et tout amendement éventuel qui pourrait élargir la motion, ce que Mme Khalid avait en tête.

Est-ce raisonnable? Je cherche simplement une solution qui satisferait tout le monde.

M. James Bezan: Je pense que, du point de vue de la procédure, vous avez une motion à l'étude, et vous devez avoir un débat ou une motion d'ajournement du débat.

Le président: Effectivement, vous avez raison. Nous avons une motion à l'étude qui pourrait être mise aux voix dès maintenant s'il n'y a pas de débat. Je vois que Mme Khalid a levé la main. Nous en sommes à 17 h 20 environ. Je ne peux pas laisser les choses se prolonger au-delà de 17 h 30 avec les ressources de la Chambre.

Allez-y, madame Khalid.

Mme Iqra Khalid: Merci, monsieur le président.

Pour parler de la motion elle-même, je suis sûre que M. Bezan a pris du temps pour la rédiger. Je suis sûre qu'il s'est entretenu avec ses collègues qui sont dans la salle.

Encore une fois, je l'ai dit plus tôt aujourd'hui également. Je répète que si vous aviez fait circuler le texte de la motion, à moi ainsi qu'aux autres députés libéraux, avec un petit préavis, nous aurions pu examiner le document. Nous aurions pu avoir une conversation de fond.

Il nous reste deux minutes dans une réunion de comité, et nous sommes maintenant forcés de voter sur quelque chose que nous n'avons même pas examiné. Nous n'avons pas eu l'occasion d'avoir une conversation à ce sujet. Les membres présents dans cette salle n'ont pas eu la courtoisie de nous dire: « Hé, écoutez, voici ce que nous proposons. Faisons-le. »

Nous sommes présents et disposés à agir. Nous posons des questions. Nous nous intéressons à cette étude très importante. Nous aimerions simplement qu'il y ait un peu plus de coopération.

Je suis tout à fait d'accord avec le président. J'ai l'impression qu'avec un simple clic sur un bouton, vous auriez pu m'envoyer un courriel. Vous auriez pu m'envoyer un texte ou autre chose. Nous aurions pu avoir une conversation en parallèle ou simultanément durant l'audience du Comité. Maintenant, tout d'un coup, nous nous retrouvons dans une situation où je n'ai pas lu le texte complet de la motion. Oui, il est sur mon téléphone, devant moi. Je ne l'ai pas lu. Je n'ai pas envisagé quoi d'autre ou quelle portée. Je n'ai pas eu le temps de digérer ce que j'ai entendu de la GRC aujourd'hui pour voir ce qui manque.

J'aimerais qu'il y ait un peu plus de coopération, monsieur le président. Il est regrettable que nous devions nous plaindre auprès de vous de ce manque de coopération. Je comprends que vous avez tous les votes. Vous pouvez adopter votre motion de la manière que vous voulez.

Je vous demanderais simplement de respecter un peu le temps du Comité, le temps de tout le monde ici, de coopérer davantage et de faire en sorte que les choses se fassent ensemble sans être toujours aussi conflictuels. Nous sommes ici pour travailler tous ensemble.

● (1730)

Le président: Merci.

Monsieur Fergus, vous avez la parole.

L'hon. Greg Fergus: Merci, monsieur le président.

Cela se résume vraiment à cela. Chers collègues, c'est une occasion à saisir. Je pense que nous sommes tous sur la même longueur d'onde. Je crois que nous sommes tous vivement intéressés par cette question. Nous voulons tous avoir un débat approfondi. Il y a là une occasion pour nous de le faire.

Soyons francs. Nous n'avons pas une liste complète de témoins demain. À mon avis, la suggestion du président est très logique, et je crois que tout le monde peut l'appuyer. Nous avons le temps demain de le faire sans réduire le nombre de témoins, alors pourquoi pas? Ce n'est que dans quelques heures, les amis.

Le président: Très bien, j'ai M. Villemure.

[*Français*]

M. René Villemure: Serait-il possible de s'assurer que tout le monde aura le bon équipement demain? Nous devons être en mesure de bien entendre les propos des participants. Malheureusement, il y a des moments où je n'entends pas M. Fergus, ce qui est malheureux, parce que j'aime bien entendre ses propos.

Je vous remercie.

[*Traduction*]

Le président: Vous avez raison, monsieur Villemure, nous avons eu un petit problème de son de temps en temps. M. Fergus coupait un peu et il était difficile de l'entendre à certains moments. Je ne sais pas ce que nous pouvons faire à ce sujet, si ce n'est veiller à ce qu'on en soit conscients.

J'ai les deux... Je ne sais pas qui est la première. Je pense que c'est Mme Khalid. Nous venons d'entendre M. Fergus, alors allez-y, madame.

Mme Iqra Khalid: Merci, monsieur le président.

Dans l'intérêt du plan que vous avez présenté, que je trouve raisonnable, je propose que le débat soit ajourné jusqu'à demain sur cette motion.

Le président: La motion avec la condition ajoutée ici devient discutable, alors y a-t-il quelqu'un qui souhaite s'exprimer sur la motion?

Madame Khalid, vous pourriez supprimer la condition et dire simplement que le débat est ajourné sur la motion. Bien, ajourné jusqu'à demain.

Il n'y a pas de débat, alors si vous êtes d'accord dans un sens ou dans l'autre, nous allons passer au vote.

Mme Iqra Khalid: Désolée, monsieur le président, je crois que M. Fergus a levé la main.

Le président: D'accord, je pense que sa caméra s'est débranchée, et quand cela se produit, je ne vois plus sa main.

Allez-y, monsieur Fergus.

L'hon. Greg Fergus: Toutes mes excuses; je retournais à la lecture de la motion sur mon compte de messagerie P9.

[*Français*]

J'aimerais présenter mes excuses à tous les députés, en particulier à mon collègue du Bloc québécois. La raison pour laquelle je n'ai pas le casque d'écoute, c'est parce que la rencontre a été convoquée pendant que j'étais à l'extérieur du pays et je n'avais pas mon casque d'écoute ou mon ordinateur avec moi. J'en suis désolé.

Encore une fois, je présente mes excuses à tous mes collègues et aux interprètes.

[*Traduction*]

Le président: Très bien, voilà où nous en sommes... S'il n'y a pas d'autre débat, nous pouvons voter sur la motion de Mme Khalid, qui vise à ajourner le débat.

(La motion est adoptée.)

Le président: Sur ce, nous avons dépassé le temps imparti. La séance est levée.