CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

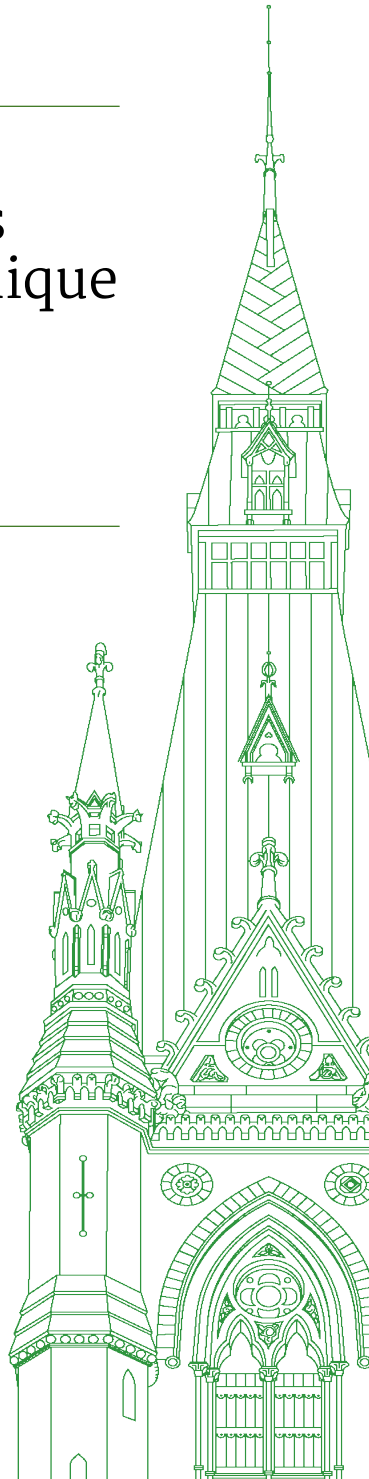
44e LÉGISLATURE, 1re SESSION

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

TÉMOIGNAGES

NUMÉRO 101

Le mardi 6 février 2024



Président : M. John Brassard

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

Le mardi 6 février 2024

● (1100)

[*Traduction*]

Le président (M. John Brassard (Barrie—Innisfil, PCC)): Bonjour à tous.

La séance est ouverte.

[*Français*]

Bienvenue à la 101e réunion du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes.

Conformément à l'article 108(3)h) du Règlement et à la motion adoptée par le Comité le mercredi 6 décembre 2023, le Comité reprend aujourd'hui son étude sur l'utilisation par le gouvernement fédéral d'outils technologiques permettant d'extraire des données sur des appareils mobiles et des ordinateurs.

La réunion d'aujourd'hui se déroule sous forme hybride, conformément au Règlement de la Chambre. Les députés peuvent y participer en personne ou au moyen de l'application Zoom.

[*Traduction*]

Je veux simplement rappeler à tout le monde — je sais que les témoins le savent — qu'il ne faut pas approcher les écouteurs des microphones parce que cela provoque des réactions acoustiques pour nos interprètes et pourrait aussi causer des blessures.

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

Nous accueillons Francis Brisson, sous-ministre adjoint et dirigeant principal des finances, et Pierre Pelletier, dirigeant principal de l'information, du ministère des Ressources naturelles. Nous accueillons également Dave Yarker, directeur général, Cyberopérations et systèmes d'information de commandement et de contrôle, et Sophie Martel, dirigeante principale de l'information par intérim, du ministère de la Défense nationale.

Nous disposons de cinq minutes pour les déclarations préliminaires.

Je suppose, monsieur Yarker, que c'est à vous que nous allons donner la parole, ou est-ce à Mme Martel?

Mme Sophie Martel (dirigeante principale de l'information par intérim, ministère de la Défense nationale): Ce sera moi, monsieur le président.

[*Français*]

Le président: Vous avez la parole, madame Martel.

Mme Sophie Martel: Monsieur le président et chers membres du Comité, au nom du ministère de la Défense nationale et des Forces armées canadiennes, je vous remercie de nous avoir invités au Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique.

Je suis Sophie Martel, dirigeante principale de l'information par intérim. Dans le cadre de mes fonctions, je représente l'autorité fonctionnelle responsable de l'ensemble du programme ministériel des technologies de l'information et de la communication. Je m'assure que le ministère de la Défense nationale et les Forces armées canadiennes disposent d'un environnement numérique fiable, sécurisé et intégré, et capable de répondre aux besoins opérationnels.

Les technologies de l'information et de la communication fournies par mon équipe soutiennent les fonctions de base de la Défense nationale que sont les renseignements, la surveillance, la reconnaissance, les communications, la guerre cybernétique, le commandement, la gestion ainsi que la sécurité cybernétique. La dirigeante principale de l'information du ministère est également responsable du développement et de la disponibilité opérationnelle de la force cybernétique au sein du commandement cybernétique des Forces armées canadiennes.

[*Traduction*]

Le brigadier-général Yarker, directeur général, Cyberopérations et systèmes d'information de commandement et de contrôle, m'accompagne aujourd'hui.

Il est responsable de l'organisation et de l'exécution des cyberopérations et des exercices au sein des Forces armées canadiennes, y compris la fonction d'investigation informatique et la maintenance des principales infrastructures nationales de commandement et de contrôle.

Je tiens à souligner que la protection des renseignements personnels est une priorité absolue et que le ministère de la Défense nationale s'engage à faire tout ce qui est en son pouvoir pour protéger ces renseignements. Cependant, il doit y avoir un équilibre. Il n'y a qu'une attente limitée en matière de protection de la vie privée lors de l'utilisation de nos systèmes de TI et de nos appareils mobiles, car ils font l'objet d'une surveillance aux fins de l'administration, de la maintenance et de la sécurité du système, ainsi que pour assurer le respect des politiques.

Notre surveillance est conforme aux politiques et normes gouvernementales applicables.

[*Français*]

En conclusion, j'aimerais répéter que le ministère de la Défense nationale et les Forces armées canadiennes continuent de s'acquitter de leur mandat tout en garantissant la protection des renseignements personnels.

[*Traduction*]

Mon collègue et moi serons heureux de répondre à vos questions. Par principe et pour assurer la sécurité opérationnelle, nous ne pouvons pas divulguer de renseignements sur l'utilisation d'un équipement particulier ou sur les systèmes utilisés de façon opérationnelle.

Merci.

● (1105)

[*Français*]

Le président: Merci, madame Martel. Vous n'avez pas utilisé tout votre temps de parole. C'est bien pour le Comité, qui pourra poser plus de questions.

Monsieur Brisson, vous avez la parole cinq minutes pour faire votre allocution.

M. Francis Brisson (sous-ministre adjoint et dirigeant principal des finances, ministère des Ressources naturelles): Bonjour et merci beaucoup.

Je vous remercie de me donner l'occasion de vous parler de l'utilisation que fait Ressources naturelles Canada d'outils technologiques pour protéger nos actifs technologiques et nos données et pour assurer l'évolution et la croissance constantes de nos activités scientifiques.

J'aimerais également souligner que je m'adresse à vous depuis le territoire traditionnel non cédé du peuple anishinabe algonquin. Nous reconnaissons ce peuple comme le gardien et le défenseur coutumier du bassin versant de la rivière des Outaouais et de ses affluents. Nous honorons sa longue histoire d'accueil de nombreuses nations sur ce magnifique territoire et nous défendons la voix et les valeurs de nos hôtes.

[*Traduction*]

Comme on l'a mentionné, je suis Francis Brisson, le dirigeant principal des finances et sous-ministre adjoint responsable de la gestion des services intégrés à Ressources naturelles Canada. Mes principales responsabilités comprennent les services intégrés, les ressources humaines, les technologies de l'information et la sécurité. Le dirigeant principal de l'information et DPI de notre ministère, Pierre Pelletier, qui m'accompagne aujourd'hui, est responsable de la gestion, de la mise en œuvre et de l'utilisation des technologies de l'information et de l'informatique à RNCan.

RNCan est une organisation à la fois scientifique, politique et économique. Il est crucial qu'elle veille à ce que ses fonctions essentielles demeurent résilientes et réactives face aux menaces internes et externes. Les menaces planent non seulement sur nos données numériques, mais aussi sur nos systèmes physiques et nos appareils. Plus notre environnement numérique est complexe, plus le risque de compromettre nos systèmes et nos actifs augmente. Ces risques comprennent les atteintes à la protection des données, le vol de propriété intellectuelle, les perturbations des services, les revers financiers et les menaces à la sécurité.

Pour se protéger contre les risques et y réagir, il faut déployer des efforts réguliers et soutenus. Notre ministère, comme d'autres, dispose d'un grand nombre de systèmes, de politiques et d'outils différents pour gérer les risques et y réagir. Pour contrer les menaces et y réagir, on peut avoir besoin d'outils logiciels d'investigation. RNCan a acheté une licence de Magnet Forensics pour avoir cet outil dans sa boîte à outils, mais ne l'a jamais utilisé.

Je soulignerais également que, advenant que le ministère ait des besoins opérationnels qui l'amènent à utiliser ce logiciel ou un logiciel semblable, RNCan suivra les protocoles et les exigences applicables pour les utiliser de façon appropriée et effectuer les évaluations des facteurs relatifs à la vie privée, ou des EFVP.

[*Français*]

Je vous remercie de votre attention et c'est avec plaisir que M. Pierre Pelletier et moi répondrons à vos questions concernant notre travail.

Le président: Merci, monsieur Brisson. Vous aussi avez pris moins de temps que prévu. C'est bien. Les membres du Comité auront plus de temps de parole pour poser leurs questions.

Nous allons justement commencer notre premier tour de questions.

Vous avez la parole pour six minutes, monsieur Kurek.

[*Traduction*]

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

Je remercie nos témoins de s'être joints à nous aujourd'hui.

À l'instar des membres du Comité et de nombreux Canadiens, j'ai été préoccupé lors de la parution dans les médias des reportages faisant état de l'utilisation de ce qui, à mon avis, pourrait être interprété à juste titre comme une technologie très invasive. Ils ont certes suscité des préoccupations, qui nous ont menés là où nous en sommes aujourd'hui, à la lumière de l'érosion de la confiance à l'égard des institutions gouvernementales qui a eu lieu au cours des dernières années en particulier.

J'ai deux ou trois questions à poser. Je vais commencer par l'évaluation des facteurs relatifs à la vie privée. Ma question s'adresse aux représentants des deux ministères.

La semaine dernière, le commissaire nous a dit qu'aucun de vos ministères n'avait présenté d'évaluation des facteurs relatifs à la vie privée. Peut-être pourriez-vous, en 30 secondes environ — et je vais commencer par le MDN, puis passer à RNCan — me dire où vous en êtes, si vous avez soumis les évaluations des facteurs relatifs à la vie privée et si vous avez l'intention de le faire?

Je vais commencer par vous, les représentants du MDN.

Mme Sophie Martel: Je vous remercie de la question.

Un certain nombre d'évaluations des facteurs relatifs à la vie privée sont en cours. Du point de vue des DPI, comme nous sommes responsables de la sécurité de notre réseau, nous respectons la Loi sur la gestion des finances publiques — ou la LGFP —, les normes du Conseil du Trésor et toutes les lois. À part cela, si on a besoin d'une EFVP, nous y travaillons. Par exemple, actuellement, nous examinons Microsoft 365, parce que nous commençons à consigner des renseignements et à produire des transcriptions, et nous commençons à nous pencher sur les conséquences qu'entraîneront ces activités du point de vue de l'EFVP.

● (1110)

M. Damien Kurek: Si je comprends bien, le processus est en cours, mais vous n'avez pas présenté à la commissaire à l'information une EFVP concernant l'observation d'appareils?

Mme Sophie Martel: À l'heure actuelle, un certain nombre d'entre elles sont en cours au ministère.

M. Damien Kurek: D'accord.

Messieurs les représentants de RNCan...?

M. Francis Brisson: Bonjour.

En ce qui nous concerne, comme nous l'avons dit au début dans notre déclaration préliminaire, nous avons acheté l'outil, et ce, afin de l'avoir dans notre boîte à outils, mais nous ne l'avons pas utilisé, pour notre part. Une chose que je voulais répéter et dont je voudrais assurer le Comité, c'est que, si nous prévoyions utiliser l'outil, nous procéderions uniquement au titre d'un mandat de sécurité, et nous suivrions des protocoles clairs. Advenant que nous utilisions l'outil, pour notre part, nous procéderons à une EFVP, le cas échéant.

Pour l'instant, nous ne l'avons pas utilisé. Si nous devions l'utiliser pour nous acquitter d'un mandat approuvé par notre dirigeant principal de la sécurité, ce faisant, nous envisagerions d'effectuer une EFVP.

M. Damien Kurek: Je vous remercie de cette explication. Je pense que l'une des préoccupations que nous avons entendues concerne un certain fossé. La semaine dernière, le commissaire nous a parlé du fait qu'il était heureux de travailler avec les ministères et les organismes, mais qu'il n'avait pas reçu d'EFVP. Surtout compte tenu du fait que nous avons entendu dire que RNCan a acheté un logiciel qui lui donne la capacité d'extraire des données sur des appareils mobiles et ordinateurs, j'espère certainement que le processus d'EFVP soit en cours et qu'il puisse même être réalisé avant l'achat d'un tel logiciel.

En ce qui concerne les outils permettant d'extraire des renseignements personnels — je vais commencer par les représentants de RNCan —, votre ministère a-t-il déjà utilisé un outil de ce genre?

M. Francis Brisson: En ce qui nous concerne, à RNCan, nous possédons des outils, et nous devons surveiller notre système et tout le reste. Nous nous assurons d'être respectueux, et nous appuyons les politiques à cet égard. Pour notre part, nous utilisons des outils pour nous assurer de recueillir des renseignements, mais c'est fait dans le contexte des politiques du SCT, entre autres.

M. Damien Kurek: A-t-on déjà recueilli des renseignements auprès de personnes qui ne font pas partie de l'organisation? Je parle non pas d'employés, mais de personnes de l'extérieur de l'organisation de RNCan. Votre ministère a-t-il déjà recueilli des renseignements au moyen de ce genre d'outils?

M. Francis Brisson: L'outil d'investigation dont nous avons parlé n'a jamais été utilisé, et, s'il devait l'être, il ne le serait qu'à l'interne. En ce qui nous concerne, tous les systèmes de surveillance dont nous sommes dotés dans ce domaine sont utilisés pour nos besoins internes, au sein de l'organisation, et à des fins administratives, conformément aux exigences en matière de sécurité découlant d'un mandat de sécurité clair pour l'avenir.

M. Damien Kurek: Je vais poser la même question aux représentants du MDN, et puis-je l'obtenir en 30 secondes environ?

Mme Sophie Martel: Oui. En 30 secondes, nous enquêtons sur des réseaux, pas sur des gens. Pour enquêter sur les réseaux, nous devons utiliser des outils afin d'assurer la confidentialité, l'intégrité et l'accessibilité des données. C'est conforme à la LGFP, à la norme du Conseil du Trésor et à la Loi sur la protection des renseignements personnels.

M. Damien Kurek: A-t-on déjà utilisé l'outil à l'extérieur du MDN ou des Forces armées canadiennes?

Mme Sophie Martel: Il sert à surveiller notre réseau, seulement notre réseau.

M. Damien Kurek: Merci.

Je suppose qu'il s'agit de conseils non sollicités, mais surtout, compte tenu de certains reportages publiés dans les médias à ce sujet, j'espère qu'on adopte une approche proactive dans tous les ministères et les gouvernements. La commissaire à l'information veut travailler avec les ministères. Le rétablissement d'une partie de la confiance qui a été perdue est certainement une chose que j'encouragerais tous ceux qui... et je vais probablement le répéter: travaillons d'arrache-pied pour rétablir la confiance que doivent avoir les Canadiens.

Merci.

Le président: Je vous remercie, monsieur Kurek.

Tout le monde me facilite la tâche aujourd'hui. C'était juste à temps.

Madame Khalid, vous avez exactement six minutes, espérons-le. Allez-y.

Mme Iqra Khalid (Mississauga—Erin Mills, Lib.): Ha, ha! Nous prenons tous nos désirs pour des réalités, monsieur le président.

Merci beaucoup à nos témoins de leur présence aujourd'hui.

Ce que j'espère faire, c'est parler aux représentants de chaque ministère individuellement, alors mes questions seront semblables pour les deux.

D'abord et avant tout, je m'adresse aux représentants de la Défense nationale. À vos yeux, quel est le but d'une évaluation des facteurs relatifs à la vie privée?

● (1115)

Mme Sophie Martel: L'évaluation des facteurs relatifs à la vie privée vise à garantir que nous protégeons les renseignements des citoyens.

Mme Iqra Khalid: Pensez-vous qu'il soit nécessaire qu'une évaluation des facteurs relatifs à la vie privée soit effectuée au sein de votre ministère pour assurer la confiance dont dépend le fonctionnement de la démocratie?

Mme Sophie Martel: Je pense que la protection des renseignements personnels est absolument essentielle. Nous devons absolument nous assurer que la confidentialité, l'intégrité et l'accessibilité des données sont protégées. C'est pourquoi nous protégeons également notre réseau afin de protéger les renseignements et de nous assurer qu'ils sont utilisés comme il se doit.

Mme Iqra Khalid: Pourquoi lisons-nous des reportages selon lesquels vous n'avez pas effectué d'évaluation des facteurs relatifs à la vie privée?

Mme Sophie Martel: Au ministère, un certain nombre d'évaluations des facteurs relatifs à la vie privée sont en cours. Actuellement, nous, au sein du groupe du DPI plus précisément, travaillons sur une telle évaluation avec Microsoft 365. Nous en avons quelques-unes en cours.

Mme Iqra Khalid: Communiquez-vous avec notre commissaire à la protection de la vie privée pour qu'il vous aide dans ce processus?

Mme Sophie Martel: À la Défense nationale, nous avons une équipe qui communique avec lui.

Mme Iqra Khalid: Quels sont certains des défis que votre ministère et vous devez relever pour vous assurer qu'une EFVP est menée efficacement?

Mme Sophie Martel: Je ne suis pas en mesure de répondre à cette question. Je suis la DPI, alors je ne suis pas bien placée pour parler de la relation entre cette organisation et la Défense nationale. D'autres personnes peuvent en parler.

Mme Iqra Khalid: Surveillez-vous les Canadiens?

Mme Sophie Martel: Nous ne surveillons pas les Canadiens.

Comme je l'ai dit, nous sommes là pour appuyer les Canadiens. Nous sommes là pour assurer leur sécurité. Nous surveillons les réseaux. Nous ne surveillons pas les gens.

Mme Iqra Khalid: Si vous deviez surveiller un Canadien, le feriez-vous en suivant un certain processus juridique?

Mme Sophie Martel: Ce n'est pas du tout notre mandat, mais, si un autre ministère ou un autre organisme avait besoin de notre aide, il faudrait que l'on procède en suivant des processus précis.

Monsieur Yarker, voulez-vous ajouter quelque chose?

Bgén Dave Yarker (directeur général, Cybersécurité et commandement et contrôle des opérations des systèmes d'information, ministère de la Défense nationale): Nous ne serions pas appelés à surveiller les Canadiens. Cela ne fait pas partie de notre mandat ni n'est de notre ressort.

Mme Iqra Khalid: Merci beaucoup.

Je passe aux représentants de RNCan avec les mêmes questions.

À vos yeux, quel est le but des évaluations des facteurs relatifs à la vie privée?

M. Francis Brisson: Pour notre part, comme dans le cas de nos collègues du MDN, les évaluations des facteurs relatifs à la vie privée visent à protéger les renseignements et à nous assurer que, en ce qui nous concerne, les renseignements que nous détenons sont recueillis de la bonne façon, que nous les utilisons de la bonne façon, que nous en protégeons l'intégrité et, comme nous l'avons déjà dit, que nous renforçons la confiance entre les ministères et les gouvernements.

Mme Iqra Khalid: Dans quelle mesure la protection de la vie privée se classe-t-elle parmi les priorités de votre ministère dans le cadre de ses activités?

M. Francis Brisson: C'est assurément d'une extrême importance, en ce qui nous concerne.

Du fait que je suis nouveau à ce poste, à l'instar de M. Pelletier qui l'est aussi... c'est extrêmement important pour nous. Nous voulons continuer de surveiller les progrès réalisés dans ce domaine.

Mme Iqra Khalid: Pourquoi n'avez-vous pas effectué une évaluation des facteurs relatifs à la vie privée?

M. Francis Brisson: En ce qui nous concerne, l'outil n'a jamais été utilisé. Si nous devions l'utiliser, nous aurions des EFVP prêtes à être mises en œuvre et accessibles, si c'était le cas.

Nous n'utiliserions cet outil que dans le cadre de notre mandat de sécurité et en nous assurant de suivre les bons protocoles, que nous avons mis en place. Si cet outil était nécessaire pour mener une enquête, nous procéderions à une évaluation de la vie privée avant de l'utiliser.

Mme Iqra Khalid: Avez-vous communiqué avec le commissaire à la protection de la vie privée au sujet de ce problème lié à l'évaluation des facteurs relatifs à la vie privée?

M. Francis Brisson: Nous ne l'avons pas fait dans ce cas à proprement parler. Nous sommes dotés au sein du ministère d'une équipe qui est responsable de ces communications.

Je peux vous assurer que nous sommes constamment en communication et discutons constamment avec les gens du Commissariat. M. Pelletier et moi, qui sommes nouveaux au ministère, voulons poursuivre l'excellent travail qui se fait dans ce domaine. Nous continuerons à nous assurer d'organiser les choses dans cette optique.

● (1120)

Mme Iqra Khalid: Surveillez-vous les Canadiens?

M. Francis Brisson: Non.

Mme Iqra Khalid: Quels sont les défis que doit relever votre ministère pour protéger la vie privée des Canadiens tout en remplissant ses rôles?

M. Francis Brisson: Je peux peut-être céder la parole à M. Pelletier.

M. Pierre Pelletier (dirigeant principal de l'information, ministère des Ressources naturelles): Bien sûr.

En ce qui concerne les défis, ce pourrait être la lourdeur de la bureaucratie si, disons, le commissaire à la protection de la vie privée exigeait une EFVP précise et complète aux fins d'une enquête. On s'attend à ce que les ministères exercent un certain contrôle sur ce qu'on appelle le fichier de renseignements personnels. Dans un milieu de travail, on s'attend à ce que certaines données soient communiquées à l'employeur. La plupart des enquêtes se situent dans le cadre de ce qui est accepté dans un fichier de renseignements personnels. Si quoi que ce soit allait au-delà de ce mandat et de cette portée, une EFVP serait requise. Les EFVP doivent être très précises, et, habituellement, les ministères respectent bien le protocole de sécurité pour travailler et appuyer ces activités.

Le président: Merci.

M. Pierre Pelletier: L'acquisition d'une bonne compréhension de ce que supposent ces défis à mesure que nous peaufinerons la politique appuiera cette orientation.

Le président: Merci, monsieur Pelletier.

[*Français*]

Monsieur Villemure, vous avez la parole pour six minutes.

M. René Villemure (Trois-Rivières, BQ): Merci beaucoup, monsieur le président.

Je remercie tous les témoins de leur présence. Je vais poser les mêmes questions aux deux ministères, en commençant par celui de la Défense nationale.

Madame Martel, votre ministère a-t-il acheté des outils capables de capter les données sur les appareils mobiles ou les ordinateurs?

Mme Sophie Martel: Comme je l'ai mentionné plus tôt, nous avons acheté des outils permettant de protéger nos réseaux.

Notre mandat est de nous assurer que la confidentialité, l'intégrité et la disponibilité de l'information sur nos réseaux sont protégées et sécurisées. Les outils que nous avons achetés nous aident à mener des enquêtes en lien avec nos réseaux, et non des personnes.

M. René Villemure: Quels sont ces outils?

Mme Sophie Martel: Je vais demander à M. Yarker de répondre à cette question.

Bgén Dave Yarker: Nous avons plusieurs outils de ce type, mais je ne vais pas tous les expliquer aujourd'hui. Comme nous l'avons dit plus tôt, nous avons des préoccupations de nature opérationnelle liées à la sécurité et aux outils que nous utilisons.

M. René Villemure: En résumé, à quelles fins les outils ont-ils été achetés?

Mme Sophie Martel: Nous les avons achetés pour mener des enquêtes sur les réseaux et pour les réseaux.

M. René Villemure: Sur les réseaux, il y a des gens.

Mme Sophie Martel: Oui, nous sommes d'accord sur le fait qu'en recueillant de l'information sur le réseau, on recueille des paquets de données et de l'information personnelle. Cela dit, les procédures en place s'appliquant à cette information sont très strictes. Des gens ont été formés, ont obtenu la cote de sécurité requise et suivent ces procédures très strictes.

M. René Villemure: L'évaluation des facteurs relatifs à la vie privée n'a pas été faite dans ce cas précis, n'est-ce pas?

Mme Sophie Martel: En ce qui a trait au travail visant à protéger nos réseaux, nous nous conformons à la Loi sur la protection des renseignements personnels, à la Loi sur la gestion des finances publiques et à toutes les normes pertinentes du Conseil du Trésor.

Au-delà de ça, nous étudions le besoin d'une évaluation des facteurs relatifs à la vie privée. D'ailleurs, nous avons entamé une telle évaluation dans le cas de Microsoft 365.

M. René Villemure: Êtes-vous d'accord avec le commissaire à la vie privée du Canada lorsqu'il dit que certains ministères et organismes, dont le vôtre, enfreignent certaines dispositions administratives de la Loi sur la protection des renseignements personnels?

Mme Sophie Martel: En ce moment, nous utilisons ces outils en nous conformant à la Loi sur la gestion des finances publiques, à la Loi sur la protection des renseignements personnels et à toutes les normes du Conseil du Trésor.

M. René Villemure: Croyez-vous que le fait de suivre la lettre de la loi est suffisant pour susciter la confiance?

Mme Sophie Martel: Nous sommes capables de nous assurer que les gens ont confiance en nous. Notre rôle est de protéger les réseaux dans le but de protéger les Canadiens.

M. René Villemure: Tout à l'heure, vous avez dit quelque chose qui m'a étonné: en matière de vie privée, l'expectative est moindre.

Mme Sophie Martel: Pardon, pouvez-vous répéter?

M. René Villemure: Vous avez parlé de l'expectative du respect de la vie privée, qui est moindre dans le cas d'un appareil gouvernemental, par exemple, que…

Mme Sophie Martel: Ce que je voulais probablement dire, c'est que, pour utiliser un appareil gouvernemental et avoir un compte sur le réseau, un employé est obligé de remplir un questionnaire et il sait qu'il va être surveillé pour des raisons de sécurité du réseau.

M. René Villemure: D'accord, merci.

Monsieur Brisson, représentant du ministère des Ressources naturelles, je vais maintenant m'adresser à vous.

Comme vous l'avez mentionné plus tôt, votre ministère a acheté des outils, mais ne les a pas utilisés. Pourquoi les avoir achetés et pourquoi ne pas les avoir utilisés?

● (1125)

M. Francis Brisson: Je vous remercie de la question.

De notre côté, notre ministère utilise différents outils, mécanismes et protocoles. Il est important de souligner que nous n'avons pas toujours besoin d'utiliser ces outils pour mener des enquêtes. Les enquêtes internes faites par le ministère sont liées aux agissements des fonctionnaires, entre autres.

Parmi les différents outils utilisés, nous avons parlé de notre outil d'investigation informatique, qui est disponible au besoin. Cet outil peut nous aider à accélérer les recherches et à recueillir l'information, entre autres. Par contre, nous n'avons pas eu besoin de l'utiliser pour les requêtes. Cela dit, il fait partie de notre boîte à outils.

M. René Villemure: Vous êtes donc prêts.

M. Francis Brisson: Si nous devions l'utiliser, nous aurions le protocole de sécurité et le mandat nécessaire pour le faire.

Avant d'utiliser l'outil, par contre, nous nous assurerions d'effectuer une évaluation des facteurs relatifs à la vie privée.

M. René Villemure: Quel est le niveau d'autorité requis pour acheter un tel outil? Est-ce que c'est vous, en tant que sous-ministre, qui autorisez cela, ou est-ce une personne placée plus bas ou plus haut dans la hiérarchie?

M. Francis Brisson: À ma connaissance, à l'époque, cet outil a été autorisé par le dirigeant principal de l'information, poste qu'occupe maintenant M. Pelletier, après une discussion avec le chef de la sécurité du ministère.

M. René Villemure: Il y a donc quand même certaines exigences.

M. Francis Brisson: Oui, absolument. Nous respectons les protocoles en place avant d'aller de l'avant. Nous nous sommes procuré l'outil en question par l'entremise de Services partagés Canada, à la suite de discussions, en suivant les protocoles et en nous basant sur l'information que nous avions.

M. René Villemure: Qu'est-ce que vous cherchez à déceler? S'agit-il d'inconduites de la part d'employés?

M. Francis Brisson: C'est un système de surveillance qui vise à s'assurer que tout est en place. De tels outils sont utilisés si nous avons un mandat relatif à la sécurité qui dit que nous devrions étudier un cas d'un peu plus près.

M. René Villemure: Qu'est-ce que vous cherchez?

M. Francis Brisson: Il s'agit de déterminer si quelqu'un divulgue de l'information correspondant à ce qui est défini dans notre mandat de sécurité. Nous recueillerions alors les renseignements nécessaires pour répondre à ces besoins.

M. René Villemure: En fin de compte, il s'agit de déceler des inconduites.

M. Francis Brisson: Oui, il peut certainement s'agir de cela. Il peut y avoir différentes raisons.

M. René Villemure: Merci beaucoup.

[*Traduction*]

Le président: Je vous remercie, messieurs Villemure et Brisson.

Monsieur Green, vous disposez de six minutes. Allez-y, s'il vous plaît.

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

Je vais commencer par M. Yarker. Êtes-vous d'accord pour dire que l'esprit de cette conversation est au sujet de la confiance?

Bgén Dave Yarker: Oui. Il est certain que, en ce qui nous concerne, les outils et les questions que nous utilisons et les processus que nous appliquons visent délibérément à accroître la confiance à l'égard de notre réseau et à faire en sorte qu'il ne soit pas compromis.

M. Matthew Green: Je pense qu'on peut dire sans risquer de se tromper... Je vais peut-être poser ma question autrement. Les gens qui sont enrôlés dans les forces armées ne sont pas exactement des citoyens. Je ne comparerais pas nécessairement vos membres à ceux du ministère de l'Agriculture, par exemple. Est-ce exact?

Bgén Dave Yarker: D'accord. Je comprends très bien ce que vous voulez dire. Je vous remercie de la question.

Ce que je dirais, c'est que tous les membres du ministère conservent leur droit à la protection de la vie privée, et il est certain que nous en tenons compte dans toutes nos activités.

M. Matthew Green: Vous avez dit tout à l'heure que vous n'aviez pas pour mandat de surveiller les Canadiens.

Bgén Dave Yarker: C'est exact.

M. Matthew Green: Dans votre rôle, êtes-vous un officier du renseignement militaire?

Bgén Dave Yarker: Non. Mon rôle est celui d'agent des cyberopérations, principalement axé sur les opérations cyberdéfensives.

M. Matthew Green: Avez-vous déjà eu affaire avec le Commandement des opérations interarmées du Canada?

Bgén Dave Yarker: Oui, je travaille régulièrement avec le Commandement des opérations interarmées du Canada.

● (1130)

M. Matthew Green: Dans quelle mesure votre collaboration est-elle étroite?

Bgén Dave Yarker: Très étroite.

M. Matthew Green: Auriez-vous travaillé avec lui à l'époque où il surveillait le mouvement Black Lives Matter, en 2021?

Bgén Dave Yarker: Non, je ne suis pas au courant de cette surveillance.

M. Matthew Green: Encore une fois, quand je parle de confiance et de l'importance pour les Canadiens qui nous regardent de savoir qui a le mandat de faire quoi, je trouve franchement choquant que l'armée canadienne ait un dossier sur le mouvement Black Lives Matter, qu'elle ait affirmé qu'elle surveillait le contexte local des activités au Canada et que, dans le dossier, elle considérait les membres de ce mouvement comme des acteurs étrangers hostiles.

Ayant moi-même assisté à bon nombre de ces rassemblements et participé à ce travail, je ne peux m'empêcher de penser qu'à un moment donné, j'ai été surveillé de cette façon. Si vous connaissez les activités du mouvement, quelle technologie aurait-on utilisée pour suivre les déplacements d'une organisation de protestation ou ses manifestations dans tout le pays?

Bgén Dave Yarker: Je crains que cette surveillance aille au-delà de ma compétence. Je ne connais pas la réponse à votre question.

M. Matthew Green: À votre connaissance, utilise-t-on la technologie de l'intelligence artificielle pour surveiller les activités en ligne dans les médias sociaux, ou bien le fait-on manuellement par l'intermédiaire du Commandement des opérations interarmées?

Bgén Dave Yarker: Je crains de ne pas connaître la réponse à cette question.

M. Matthew Green: Y a-t-il un contexte dans lequel votre ministère — et, madame Martel, n'hésitez pas à intervenir — utiliserait la collecte de renseignements de source ouverte pour surveiller l'utilisation des médias sociaux par des membres du ministère de la Défense nationale?

Bgén Dave Yarker: Certainement, je dirais que, dans le contexte de la cyberdéfense, nous ne le ferions pas. Encore une fois, en ce qui concerne la cyberdéfense et les types d'outils dont il est question aujourd'hui, ces outils et leur utilisation visent à assurer notre sécurité.

M. Matthew Green: La question ne relève pas de votre compétence. J'accepterai cette réponse.

Comme je l'ai mentionné lorsque vous êtes arrivé, une partie de notre travail consiste à être les derniers à transmettre les questions et à revenir sur des choses qui ont été dites. Je m'assure simplement que l'échange correspond aux situations que j'ai vécues dans le passé. Je suis encore un peu surpris par l'utilisation que font les militaires de cette application. Si vous voulez en faire rapport à vos supérieurs afin qu'ils sachent que c'est toujours une question que je me pose ici, au comité de la protection des renseignements personnels et de l'éthique, j'aimerais bien obtenir une réponse.

Dans le cadre de ce travail, je sais que nous avons tenté de faire une distinction entre un outil de collecte de renseignements sur appareil, un logiciel espion et ce genre d'utilisation en investigation. Utilisez-vous aussi des applications sur appareil au ministère de la Défense nationale?

Bgén Dave Yarker: Certains de ces outils visent des particuliers et identifient des appareils. C'est un peu le but de l'outil. Cependant, si j'ai bien compris le sens de votre question, ce sont des choses que l'on utilise pour enquêter sur des incidents de sécurité. Nous ne les utilisons pas à d'autres fins.

M. Matthew Green: D'accord, il n'y a donc pas de surveillance continue.

Bgén Dave Yarker: Non. Certes, dans l'ensemble de l'infrastructure de sécurité du réseau, des outils de surveillance surveillent les activités malveillantes et d'autres activités du genre.

M. Matthew Green: Je vais être plus précis.

Connaissez-vous la technologie appelée Pegasus?

Bgén Dave Yarker: Oui.

M. Matthew Green: Y a-t-il quelque chose comme Pegasus… pas le nom de marque, mais son application?

Bgén Dave Yarker: Dans le domaine de la cybersécurité et de la cyberdéfense, nous n'utilisons pas ce genre de technologies, je crois, dans le sens de la question que vous posez.

M. Matthew Green: Savez-vous si elle est utilisée au ministère de la Défense nationale?

Bgén Dave Yarker: Je ne sais pas si elle est utilisée au ministère de la Défense nationale.

M. Matthew Green: Très bien. Merci beaucoup.

Je m'adresse aux représentants des deux ministères. Encore une fois, nous faisons la distinction — et je crois que c'est une distinction importante à faire — entre un appareil utilisé à des fins d'investigation, qui nécessite un dispositif physique en main dans le cadre d'une enquête, et ce qui est considéré comme un logiciel espion. J'ai parlé de Pegasus, mais il s'agit de choses qui permettraient de recueillir subrepticement des données en temps réel en tout temps.

À votre connaissance, utilisez-vous parfois ce genre d'applications dans le cadre de l'utilisation des appareils fédéraux?

M. Francis Brisson: Non.

M. Matthew Green: Dans ce cas, qu'est-ce qui justifie — une fois de plus, pour le Comité — l'achat de ce type d'appareil d'investigation?

M. Pierre Pelletier: C'est pour être efficace en cas de problème de sécurité.

M. Matthew Green: À quelle fréquence ces problèmes de sécurité surviennent-ils? Avez-vous un rapport de votre ministère faisant état de l'occurrence de 36 de ces incidents?

M. Pierre Pelletier: Ce n'est pas quelque chose à quoi j'ai facilement accès. Pour des raisons de sécurité et pour que nous soyons capables, en tant qu'organisation, de résister à toute menace potentielle, je ne divulguerais pas cette information aisément sur une tribune publique. Oui, nous avons des données internes à ce sujet.

● (1135)

M. Matthew Green: D'accord. À une date ultérieure, si nous siégeons à huis clos, s'agit-il de quelque chose dont nous pourrions discuter sans la présence des médias et du public?

M. Pierre Pelletier: C'est exact.

M. Matthew Green: D'accord. Merci beaucoup.

Le président: Merci, messieurs Green et Pelletier.

Voilà qui met fin à notre première série de questions.

Nous allons passer à deux questions de cinq minutes et à deux de deux et demi, en commençant par M. Brock.

Allez-y, monsieur.

M. Larry Brock (Brantford—Brant, PCC): Merci, monsieur le président.

Je remercie les témoins de leur présence aujourd'hui.

Je voudrais commencer par examiner les premiers principes. La présente étude fait essentiellement suite à un reportage de la SRC publié à la fin de l'automne dernier sur la façon dont le gouvernement du Canada et divers ministères — dont deux comparaissent devant le Comité aujourd'hui — ont utilisé des logiciels et du matériel pour espionner non seulement la fonction publique fédérale, mais aussi les Canadiens.

Nous avons découvert cet incident probablement des années après les faits, et l'information a été obtenue grâce à une demande d'accès à l'information présentée par un professeur de l'Université York, un expert en protection de la vie privée, qui avait des préoccupations au sujet de la capacité des fonctionnaires d'espionner les employés et les Canadiens. Il a reçu de l'information concernant les contrats — il y en avait deux avec les ministères — qu'il examinait. Radio-Canada a reçu ces contrats, et la Société a communiqué avec les deux ministères pour obtenir une explication concernant leur utilisation de ce logiciel espion.

Je voulais établir les règles de base, parce que je pense qu'il est important de le faire en vue de la première question que je vais poser, qui s'adressera aux représentants de Ressources naturelles Canada. Il semble y avoir un certain manque de cohérence, et je voudrais que vous m'expliquiez ce problème particulier. Radio-Canada a communiqué avec votre ministère. Je ne sais pas qui c'était en particulier, mais un représentant de votre ministère a confirmé que vous possédiez le logiciel, le matériel, mais que vous n'aviez pas fourni les EFVP à cet égard. C'est un problème.

Ensuite, j'ai vu dans un reportage de la SRC, à la suite de la comparution du commissaire à la protection de la vie privée — c'était dans un reportage daté du 2 février —, que des représentants de Ressources naturelles Canada avaient dit au commissaire, après sa comparution, j'imagine, qu'ils avaient acheté les outils d'extraction de données, mais qu'ils ne les avaient jamais utilisés.

Dans ce cas, pourquoi auriez-vous dit à Radio-Canada que vous l'avez fait, mais que vous n'avez jamais utilisé d'EFVP, puis, par ailleurs, dit au commissaire que vous aviez les outils, mais que vous ne les aviez jamais utilisés? Voyez-vous un certain manque de cohérence à cet égard?

M. Francis Brisson: Je vous remercie de la question. J'espère l'avoir comprise.

De notre point de vue, je vais énoncer les faits tels que je les connais, et j'espère que cette réponse améliorera votre compréhension.

Nous avons acheté l'outil, et nous le possédons, et je crois savoir que nous l'avons depuis 2018. L'outil est à notre disposition, mais il n'a jamais été utilisé. À l'heure actuelle, il n'y a personne au ministère qui puisse l'utiliser, et, si nous avions l'impression que, en raison d'une situation de sécurité, nous devrions utiliser un outil comme celui-là, au titre d'un mandat clair, nous remplirions automatiquement une EFVP pour nous assurer de faire les choses correctement.

Pour notre part, nous ne l'avons jamais utilisé, et, si nous devions le faire, en cas de besoin du point de vue de la sécurité, nous effectuerions automatiquement une EFVP.

M. Larry Brock: Au fil des ans, votre ministère a probablement connu des cas d'inconduite d'employés. Serait-il juste de l'affirmer?

M. Francis Brisson: Je ne peux pas parler au nom de…

M. Larry Brock: Est-ce que l'un de vous deux peut aborder cette question?

M. Pierre Pelletier: Je pense qu'il est juste de l'affirmer, oui.

M. Larry Brock: Dans le cadre de ces enquêtes, avez-vous déjà utilisé des logiciels et du matériel semblables à ceux dont il est question aujourd'hui?

M. Pierre Pelletier: C'est possible, mais on n'aurait pas nécessairement besoin d'avoir les outils. Ils contribuent à améliorer nos capacités, mais on pourrait le faire manuellement.

● (1140)

M. Larry Brock: Lorsque vous avez utilisé d'autres outils, avez-vous présenté une EFVP?

M. Pierre Pelletier: Pas à ma connaissance, mais, dans le cadre de l'évaluation des facteurs relatifs à la vie privée, les ministères peuvent travailler dans ce qu'on appelle les fichiers de renseignements personnels. Ces documents contiennent des types de renseignements prédéterminés auxquels notre ministère voudrait avoir accès au sujet de ses employés. Je crois savoir que, lorsque nous travaillons avec cet ensemble de renseignements, nous respectons notre mandat.

M. Larry Brock: Savez-vous qu'une directive du Conseil du Trésor…?

M. Pierre Pelletier: C'est exact.

M. Larry Brock: … prévoit que les EFVP doivent être adoptées de façon générale?

M. Pierre Pelletier: Sur les programmes, c'est exact.

M. Larry Brock: Oui, vous le savez.

M. Pierre Pelletier: RNCan a cette directive.

M. Larry Brock: Merci. Mon temps de parole est écoulé.

Merci, monsieur le président.

Le président: Je vous remercie, monsieur Brock.

C'est au tour de M. Bains, pour cinq minutes.

Allez-y, s'il vous plaît.

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

Je remercie nos invités de s'être joints à nous aujourd'hui. Vous avez tous des rôles très importants à jouer.

Ma première question s'adresse aux représentants du ministère des Ressources naturelles. Croyez-vous que les données, les biens et les systèmes de laboratoire exploités par RNCan sont protégés et sécurisés?

M. Francis Brisson: Oui. En ce qui nous concerne, c'est notre mandat, et nous faisons ce que nous pouvons pour les surveiller et nous assurer qu'ils sont protégés.

M. Parm Bains: Que faites-vous pour vous assurer qu'ils sont protégés? Comment les surveillez-vous et les protégez-vous?

M. Francis Brisson: Je peux céder la parole à M. Pelletier.

M. Pierre Pelletier: Nous travaillons avec notre fournisseur de services. Nous travaillons en étroite collaboration avec Services partagés Canada pour nous assurer que le réseau est surveillé et protégé. De la même façon, nous travaillons avec nos organismes centraux afin de l'appuyer du point de vue des menaces à la cybersécurité, et nous entretenons cet équipement. Nous le tenons à jour. Nous donnons des directives sur l'utilisation du réseau. Nous tenons et maintenons nos systèmes et leur appliquons des correctifs pour assurer la sécurité. Nous formons également le personnel à l'interne pour veiller à ce qu'il suive les directives de sécurité appropriées.

M. Parm Bains: Vous avez mentionné que RNCan s'adapte à une attention accrue accordée à la sécurité. Pouvez-vous nous en dire plus sur certaines des menaces qui pèsent sur le Canada?

M. Pierre Pelletier: Il y a beaucoup de menaces. Une grande partie de ce sur quoi RNCan travaille a une valeur commerciale, alors il y a assurément une menace externe. C'est toujours le cas.

M. Parm Bains: S'agit-il d'une menace pour nos ressources naturelles en général?

M. Pierre Pelletier: Il y a de nombreux secteurs d'activité, comme celui de l'énergie, où RNCan est intéressant pour des entités étrangères ou pour des raisons intérieures. C'est toujours la nature des activités. Le défi intéressant à RNCan tient à la nature ouverte de la culture scientifique. Il est certainement difficile pour nous de maintenir un juste équilibre entre l'échange de renseignements avec les principaux intervenants et la protection de biens importants.

M. Parm Bains: Vous avez parlé de considérations intérieures. Pouvez-vous nous parler de la menace intérieure?

M. Pierre Pelletier: Du point de vue du commerce, on s'intéresse à certaines technologies, aux percées ou à l'information scientifique qui pourraient receler un potentiel…

M. Parm Bains: Voulez-vous parler de la propriété intellectuelle, de choses de ce genre?

M. Pierre Pelletier: C'est exact.

M. Parm Bains: Quelles circonstances ont justifié l'acquisition de cette offre?

M. Pierre Pelletier: C'était surtout du point de vue de la disponibilité opérationnelle. Comme nous sommes une organisation de TI, je pense qu'il est tout à fait normal que nous nous tenions au courant des progrès technologiques. La technologie évolue constamment. Les vecteurs de menace évoluent également, et les gens se perfectionnent, alors je pense qu'il est normal qu'une organisation s'assure de maintenir un certain degré de savoir-faire technologique.

M. Parm Bains: À quelle fréquence effectuez-vous des examens? Est-ce tout simplement constant?

M. Pierre Pelletier: C'est exact.

M. Parm Bains: Les fonctionnaires sont-ils mis au courant lorsque les outils d'investigation sont utilisés dans le cadre d'enquêtes? Je pense que cette question a peut-être été posée un peu différemment.

M. Pierre Pelletier: La sécurité des TI serait assurée au moyen d'un protocole bien établi. Alors, notre chef de la sécurité lancerait une enquête. C'est là que les TI interviennent. Pour ma part, en tant que DPI, mon mandat consiste à fournir des outils et de l'équipement pour mieux appuyer une enquête de sécurité. Absolument, il y a un protocole établi, et plus précisément pour…

● (1145)

M. Parm Bains: Pourriez-vous nous donner un exemple?

M. Pierre Pelletier: Certainement. Si nous devions enquêter sur un appareil physique, on le ferait, tout d'abord, dans le cadre d'un engagement à l'égard de la sécurité du personnel. À ce stade, on procéderait à un examen des répercussions sur la sécurité, et on amorcerait l'enquête en soi. Les TI interviendraient. On procède dans un environnement sécurisé où l'accès est consigné et géré. Les renseignements fournis par les TI sont renvoyés à l'organisation du chef de la sécurité, et c'est là qu'ils sont traités à l'interne.

M. Parm Bains: Combien de temps me reste-t-il?

Le président: Il vous reste 15 secondes.

M. Parm Bains: D'accord. Merci beaucoup pour votre temps.

Le président: Merci, monsieur Bains.

Merci, monsieur Pelletier.

[*Français*]

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

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

Madame Martel, un peu plus tôt, M. Pelletier a mentionné qu'il y avait d'autres moyens d'obtenir les mêmes résultats. Est-ce le cas pour vous également?

Mme Sophie Martel: Vous parlez d'autres moyens d'obtenir quoi, exactement?

M. René Villemure: Je parle d'autres moyens d'obtenir les mêmes résultats.

Mme Sophie Martel: Pouvez-vous me donner un peu plus d'information?

M. René Villemure: Existe-t-il d'autres moyens, moins invasifs, d'obtenir les mêmes résultats?

Mme Sophie Martel: En ce moment, nous utilisons les outils dont nous avons besoin pour assurer la sécurité de nos réseaux et la plupart de ces outils sont les moins invasifs possible.

M. René Villemure: Pouvez-vous m'en dire plus?

Mme Sophie Martel: Je vais demander à M. Yarker de vous fournir une explication supplémentaire.

[*Traduction*]

Bgén Dave Yarker: Nous n'adopterions des outils plus invasifs que si la nature de l'enquête nous y obligeait. Oui, nous avons toujours recours aux outils les moins invasifs possible.

[*Français*]

M. René Villemure: D'accord. Merci beaucoup.

Monsieur Pelletier, un peu plus tôt, mon collègue vous demandait si l'employé est au courant qu'il est sous le coup d'une investigation recourant aux outils en question. J'imagine que quelqu'un qui commence à travailler chez vous remplit toutes sortes de formulaires qui autorisent certaines choses, mais est-ce l'équivalent de cliquer « j'accepte » quand on va sur un site Web, mais qu'on ne lit pas les conditions d'utilisation?

M. Pierre Pelletier: Le gouvernement n'est pas différent des autres organisations. Quand vous utilisez les réseaux d'une institution gouvernementale, vous avez certaines obligations en tant qu'employé de vous assurer que votre utilisation du matériel est conforme aux politiques gouvernementales. Dans le cas particulier d'une analyse judiciaire, il est clair qu'elle ne peut pas être faite sans que la partie prenante soit au courant. En aucun cas ne pourrions-nous la faire sans d'abord en informer les gens en cause.

M. René Villemure: Comme vous, je trouve que cela tombe sous le sens, mais des rappels de sécurité sont-ils faits régulièrement aux employés?

M. Pierre Pelletier: Absolument. Un rappel est fait automatiquement chaque fois que quelqu'un se branche au réseau privé virtuel. Le ministère remet régulièrement en évidence les obligations des employés et nous sommes d'ailleurs en plein dans le mois de la cybersécurité. Notre ministère prend donc des mesures pour sensibiliser ses employés à cette réalité.

M. René Villemure: Donc, si vous en veniez à utiliser l'outil en question, les gens ne pourraient pas dire qu'ils avaient oublié ou ignoraient que cet outil pouvait être utilisé. Autrement dit, ils auraient été prévenus.

M. Pierre Pelletier: Si on utilisait l'outil en question, ça se ferait avec beaucoup de transparence pour l'organisation et pour l'employé impliqué.

M. René Villemure: D'accord. Merci beaucoup.

Le président: Merci, monsieur Villemure.

[*Traduction*]

Monsieur Green, vous disposez de deux minutes et demie.

M. Matthew Green: Merci.

Je vais revenir à mon ami, M. Yarker. Par souci d'équité, je veux que le public ait l'occasion de se faire une idée du risque auquel le Canada est exposé en matière de cybersécurité et de cybermenaces.

Brièvement, pouvez-vous nous parler de l'importance du travail que vous faites pour protéger notre pays contre les attaques étrangères et les perturbations possibles, y compris les manquements militaires très graves?

Bgén Dave Yarker: Certainement. Je vous remercie de poser la question.

On sait très bien que le cyberespace n'est pas un espace amical. C'est un endroit où nous faisons face à de nombreuses menaces provenant de diverses directions, d'États-nations et d'acteurs criminels. Nous prenons ces menaces très au sérieux.

Au ministère de la Défense nationale, nous sommes dotés d'un solide programme de cybersécurité. De plus, nous avons des cyberforces capables de défendre nos réseaux, au besoin.

M. Matthew Green: D'une certaine façon, c'est comme une quatrième dimension des opérations militaires traditionnelles. C'est un monde complètement nouveau avec des technologies qui dépassent l'imagination de la plupart des gens.

Est-il juste de l'affirmer?

● (1150)

Bgén Dave Yarker: Oui. Je vous remercie de la question.

Je dirais que nous le traitons certainement comme un autre domaine. Il y a l'air, la terre, la mer et l'espace. La cybernétique compte parmi ces domaines.

M. Matthew Green: Vous sentez-vous bien préparé pour ce qui plane?

Bgén Dave Yarker: Comme je l'ai mentionné, le cyberespace est un peu un endroit hostile. C'est aussi un endroit où nous apprenons, et il y a encore beaucoup à faire.

Même si, oui, nous avons des forces bien entraînées et bien préparées, c'est aussi un espace où il reste toujours du travail à faire.

M. Matthew Green: Je vous remercie, Mme Martel et vous, des services que vous rendez au pays.

Je vais m'adresser à vous, au bout de la table, au sujet de l'évaluation des facteurs relatifs à la vie privée, étant donné que vous n'avez pas eu à l'utiliser. Ce que j'essaie de tirer de la présente étude, en ce qui concerne sa valeur législative réelle, c'est quels sont le processus, les systèmes et les mesures qu'il faut prendre.

Vous avez dit que vous aviez acheté la technologie et que vous êtes prêts à l'utiliser si vous en avez besoin. Vous avez affirmé que vous feriez une évaluation des facteurs relatifs à la vie privée, ou EFVP, si vous deviez utiliser la technologie. Pourquoi ne pas la faire à l'avance?

M. Francis Brisson: Assurément. En ce qui nous concerne, comme je l'ai déjà dit, M. Pelletier et moi sommes nouveaux à notre poste, et c'est certainement quelque chose que nous voulons continuer d'étudier et d'examiner de plus près.

M. Matthew Green: Êtes-vous capables, avez-vous la capacité décisionnelle, de simplement commencer une EFVP en sortant de la réunion, ou bien est-ce quelque chose que vous devez...?

M. Francis Brisson: Non. Pour notre part, nous le pouvons assurément.

M. Matthew Green: Vous engagez-vous à le faire après que vous aurez quitté le Comité?

M. Francis Brisson: En ce qui nous concerne, je n'aurai aucun problème à le faire parce que nous nous penchons de façon proactive sur ce que nous pouvons faire dans ce domaine. Je me sens à l'aise de le faire étant donné que nous avons les…

M. Matthew Green: Je vais considérer cette réponse comme un engagement. Je vous en suis reconnaissant.

Le président: Je vous remercie, messieurs Green et Brisson.

Il nous reste du temps pour deux questions de quatre minutes. Nous allons passer à M. Barrett. Nous arriverons ainsi assez haut dans la liste, puis nous passerons à notre prochain groupe de témoins.

Allez-y, monsieur Barrett.

M. Michael Barrett (Leeds—Grenville—Thousand Islands et Rideau Lakes, PCC): Clarifions les choses. Il y a eu l'article de la SRC dont mon collègue a parlé tout à l'heure. L'histoire remonte au 29 novembre 2023. L'article était intitulé « *Tools capable of extracting personal data from phones being used by 13 federal departments, documents show* », ce qui signifie en français « des documents montrent que des outils permettent d'extraire des données personnelles des téléphones utilisés par 13 ministères fédéraux ». Vos ministères comptent parmi ceux qui sont nommés.

Général et madame Martel, votre ministère a-t-il cette capacité, oui ou non?

Mme Sophie Martel: Oui. Nous avons la…

M. Michael Barrett: D'accord. Vous en avez la capacité.

Vous avez dit que vous ne surveilliez pas les gens. Vous ne surveillez que des réseaux.

Mme Sophie Martel: C'est exact.

M. Michael Barrett: Les outils qui permettent d'extraire des données personnelles des téléphones… en quoi s'agit-il de surveiller un réseau et non pas de surveiller une personne?

Mme Sophie Martel: Je vais laisser M. Yarker répondre à cette question.

Bgén Dave Yarker: Dans le cas d'un incident de cyberdéfense typique, et c'est de cela qu'il est question en réalité, les outils dont nous parlons sont ceux dont on aurait besoin pour déterminer comment et pourquoi un appareil comme un téléphone cellulaire a été compromis.

M. Michael Barrett: D'accord.

Bgén Dave Yarker: Je pense que, ce que nous voulons dire, c'est que nous abordons le problème du point de vue de la compromission de l'appareil et du réseau.

M. Michael Barrett: Je vois. Dans le cadre de votre enquête, l'un de vos outils d'enquête vous donne accès au téléphone d'une personne. Vous utiliseriez ce logiciel comme outil, et une partie de votre processus consiste à accéder au téléphone de la personne.

Répondez brièvement par oui ou par non. Mon temps de parole est limité.

Bgén Dave Yarker: Seuls les appareils de la Défense nationale sont utilisés, mais, évidemment, ces appareils sont utilisés par des personnes.

M. Michael Barrett: D'accord. Je ne pense pas que c'était clair dans vos réponses initiales.

Les membres ont-ils droit à la vie privée?

Mme Sophie Martel: Tout à fait. Oui.

M. Michael Barrett: Avez-vous utilisé cette capacité sur le téléphone de membres?

Bgén Dave Yarker: Leurs téléphones personnels...? Non.

M. Michael Barrett: Sur des téléphones attribués à des membres...?

Bgén Dave Yarker: Oui.

M. Michael Barrett: Les membres sont-ils autorisés à ouvrir une session dans des comptes infonuagiques personnels sur des téléphones attribués?

Mme Sophie Martel: Ils ne sont pas censés le faire, mais certains le font.

Bgén Dave Yarker: Oui.

M. Michael Barrett: S'agit-il d'un non-respect de leurs conditions d'emploi?

Mme Sophie Martel: Le gouvernement…

M. Michael Barrett: Le général a dit oui, et vous avez dit non, alors il y a manifestement un désaccord, même à la table. Je m'attendrais à ce que, si on sondait les membres, ils aient des idées différentes puisqu'on n'est même pas certain à ce niveau-ci.

Mme Sophie Martel: Je vais m'expliquer.

Comme je l'ai dit plus tôt, lorsque nous obtenons un compte sur le réseau, pour accéder au compte, on doit signer pour dire qu'on n'utilisera l'appareil en question que pour faire du travail gouvernemental.

M. Michael Barrett: Bien sûr.

Mme Sophie Martel: Or, les gens…

M. Michael Barrett: Pour faire du travail gouvernemental sur ces téléphones, les gens utilisent des applications de messagerie. Ces applications de messagerie sont habituellement les mêmes que celles qu'ils utilisent sur leur appareil personnel, ce qui vous donne accès aux renseignements personnels sur leur appareil.

Avez-vous obtenu une EFVP avant d'utiliser cette technologie?

● (1155)

Mme Sophie Martel: Avant la première fois que nous l'avons utilisée... Ce que nous faisons grâce à une EFVP, c'est nous assurer que nous respectons la Loi sur la gestion des finances publiques, ou LGFP et les normes du Conseil du Trésor.

M. Michael Barrett: Avez-vous terminé le processus avant de l'utiliser?

Mme Sophie Martel: Nous avons terminé le processus qui devait être suivi, selon les politiques et les normes du gouvernement, c'est-à-dire la sécurité du réseau.

M. Michael Barrett: Vous ne croyez pas qu'il soit nécessaire de faire une EFVP avant d'utiliser cette technologie.

Mme Sophie Martel: Non, ce que je dis, c'est que…

M. Michael Barrett: La question est très claire, madame.

Avez-vous ou non rempli une EFVP avant d'utiliser cet outil? Vous l'avez fait, ou vous ne l'avez pas fait.

Mme Sophie Martel: Pour être honnête avec vous, je n'en suis pas certaine.

Bgén Dave Yarker: Nous ne l'avons pas fait.

M. Michael Barrett: D'accord. Ma question est la suivante: pourquoi pensez-vous que vous n'avez pas besoin de le faire? Mais je n'ai plus de temps.

Vos membres sont des citoyens canadiens. Les Canadiens, vous en avez convenu, ont le droit à la vie privée, et votre défaut de procéder à une EFVP est un défaut de protéger et de respecter la vie privée de vos membres.

Je me désole de ne pas avoir plus de temps pour poursuivre.

Le président: Merci, monsieur Barrett.

Monsieur Kelloway, vous avez quatre minutes. Allez-y, s'il vous plaît.

M. Mike Kelloway (Cape Breton—Canso, Lib.): Merci, monsieur le président.

Mes questions s'adressent aux représentants de la Défense nationale.

Durant votre témoignage, vous avez affirmé que l'utilisation par le MDN d'outils d'investigation informatique est conforme aux politiques et aux normes du gouvernement et que ces outils ne sont utilisés qu'à l'interne. Dans ce cas, après avoir reçu un appareil officiel du ministère, les employés du MDN sont-ils clairement informés du fait que leurs appareils sont assujettis à des outils d'investigation informatique?

Mme Sophie Martel: Oui, tout à fait. Nous envoyons également un rappel chaque fois qu'une personne ouvre une session dans le système pour qu'elle en soit informée. Oui.

M. Mike Kelloway: Je vous remercie de cette réponse.

Étant donné que les fonctionnaires de la Défense nationale s'occupent d'affaires liées à la plus haute sécurité nationale sur leurs appareils officiels, considérez-vous que le fait de soumettre les employés du MDN à une surveillance informatique lorsqu'ils utilisent leurs appareils officiels soit une mesure de sécurité essentielle?

Bgén Dave Yarker: Je dirais que, en ce qui concerne de la sécurité, nous surveillons le réseau, comme je l'ai mentionné, pour déceler les menaces à la sécurité, les compromissions et les problèmes du genre. Nous sommes tout à fait conscients que certains hauts dirigeants sont plus susceptibles d'être pris pour cibles par les auteurs de menaces.

M. Mike Kelloway: Merci de cette réponse. Je vous en suis reconnaissant.

Ma question s'adresse aux représentants de l'un ou l'autre des ministères. Connaissez-vous une autre entité de défense nationale ou de sécurité nationale au pays, ou même dans tout pays allié, qui assure la protection totale de la vie privée des employés qui traitent des renseignements touchant la sécurité nationale?

Mme Sophie Martel: Nous assurons la protection totale de la vie privée des employés qui utilisent notre système. J'ai mentionné qu'une des raisons pour lesquelles nous assurons la sécurité du réseau, c'est pour garantir la confidentialité, l'intégrité et l'accessibilité des données. Nous travaillons avec nos alliés pour nous assurer que les normes que nous respectons au pays sont aussi des normes qui sont respectées dans d'autres pays.

M. Mike Kelloway: Je vous remercie de cette réponse.

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

Le président: Il vous reste une minute et 45 secondes, mais je vais vous accorder 30 secondes supplémentaires parce que M. Barrett a pris 30 secondes de plus.

M. Mike Kelloway: C'est très gentil de votre part. Je vous en suis reconnaissant.

Je vais passer aux représentants de Ressources naturelles, si vous me le permettez.

J'entends dire aujourd'hui que vos outils numériques ont été achetés par l'intermédiaire de Services partagés Canada et qu'ils n'ont jamais été utilisés. Je me demande à quel moment le ministère a décidé qu'il était nécessaire d'obtenir ces services par l'intermédiaire de Services partagés Canada.

M. Francis Brisson: Si vous me le permettez, de notre point de vue, comme on l'a dit plus tôt, et pour insister sur ce point, d'après ce que nous croyons comprendre, le ministère a décidé d'acheter ce système afin de s'assurer que nous disposions des outils nécessaires si nous en avions besoin à un moment donné. En ce qui nous concerne, c'est ce que nous avons fait.

Depuis, chaque année, nous renouvelons notre licence au cas où nous en aurions besoin. Comme je l'ai déjà dit, si jamais nous décidions de l'utiliser conformément à une exigence de sécurité, nous nous assurerions d'envisager de procéder à une EFVP. Toutefois, comme nous nous y sommes engagés plus tôt, c'est quelque chose que nous envisagerons de faire dans l'avenir, même si l'outil n'est pas utilisé.

M. Mike Kelloway: J'ai une dernière question à poser, si j'en ai le temps.

Au cours de votre témoignage, monsieur Brisson, vous avez mentionné que Ressources naturelles Canada utilise des outils d'investigation informatiques pour atténuer les menaces. Ces menaces concernent-elles uniquement les systèmes internes du ministère, ou s'agit-il de menaces touchant les ressources naturelles du Canada?

● (1200)

M. Pierre Pelletier: C'est une très bonne question. J'affirmerais qu'elles touchent surtout les données qui transitent dans le cadre des activités de RNCan… la science et la recherche qui y sont associées. Pour ce qui est des ressources naturelles, je ne suis pas en mesure de répondre. Je ne sais pas.

M. Mike Kelloway: Merci, monsieur le président.

Le président: Merci, monsieur Kelloway.

[*Français*]

De la part du Comité, je tiens à remercier les témoins de notre premier groupe: M. Yarker, Mme Martel, M. Brisson et M. Pelletier.

Nous allons suspendre la séance pendant quelques minutes pour que le prochain groupe de témoins s'installe.

● (1200)

(Pause)

● (1205)

[*Traduction*]

Le président: Bon retour à tous.

Nous allons accueillir notre deuxième groupe de témoins.

Je rappelle à tous nos témoins qu'ils doivent porter des écouteurs. Tenez-les loin des microphones lorsque vous parlez afin de protéger nos interprètes de toute lésion auditive.

[*Français*]

J'aimerais maintenant souhaiter la bienvenue aux témoins qui comparaissent pendant la deuxième heure de notre réunion d'aujourd'hui.

[*Traduction*]

Nous accueillons M. Aaron McCrorie, vice-président, Renseignement et exécution de la loi, de l'Agence des services frontaliers du Canada. Nous accueillons également, du Service correctionnel du Canada, France Gratton, commissaire adjointe, Opérations et programmes correctionnels, ainsi que Tony Matson, commissaire adjoint et dirigeant principal des finances, Services corporatifs.

Nous accueillons à titre de représentants de la Gendarmerie royale du Canada M. Bryan Larkin, sous-commissaire, Services de police spécialisés, et Nicolas Gagné, surintendant, Gendarmerie royale du Canada.

Nous allons commencer par les déclarations préliminaires de cinq minutes.

Monsieur McCrorie, je crois comprendre que vous êtes le premier à prendre la parole. Vous disposez de cinq minutes. Veuillez commencer.

Merci.

M. Aaron McCrorie (vice-président, Renseignement et exécution de la loi, Agence des services frontaliers du Canada): Merci, monsieur le président.

Comme on l'a dit, je m'appelle Aaron McCrorie. Je suis vice-président du Renseignement et de l'exécution de la loi à l'ASFC. Je suis heureux de comparaître aujourd'hui.

Comme on l'a dit, je m'appelle Aaron McCrorie. Je suis vice-président du Renseignement et de l'exécution de la loi à l'ASFC. Je suis heureux de comparaître aujourd'hui.

Cette responsabilité comprend la conduite d'enquêtes criminelles sur des infractions présumées au titre des lois frontalières. C'est dans le cadre de cette enquête que l'ASFC utilise du matériel et des logiciels judiciaires pour déverrouiller et déchiffrer les appareils numériques saisis et, par la suite, rechercher des preuves d'infractions. Je considère que c'est comme recourir à un serrurier afin qu'il ouvre une boîte verrouillée qui contient des éléments de preuve.

Les appareils examinés par les équipes d'informatique judiciaire de l'ASFC ont été saisis en vertu d'ordonnances judiciaires précises, comme des mandats de perquisition ou des autorisations judiciaires, délivrées aux enquêteurs de l'Agence. Les données extraites des appareils numériques saisis sont traitées uniquement dans les laboratoires judiciaires numériques de l'ASFC et ne sont fournies qu'aux personnes légalement autorisées à y accéder.

Actuellement, nous gérons notre utilisation de ces outils à l'aide du fichier de renseignements personnels, qui décrit clairement les types de renseignements que nous recueillons et les usages que nous en faisons.

Nous travaillons également avec nos partenaires internes à une évaluation des facteurs relatifs à la vie privée. Nous avons commencé ce travail en 2020. Malheureusement, il a été retardé pour plusieurs raisons. Nous poursuivons ce travail, et nous collaborerons avec le Commissariat à la protection de la vie privée pour parachever l'évaluation des facteurs relatifs à la vie privée.

J'aimerais également préciser qu'on définit généralement les logiciels espions comme des logiciels installés sur un appareil dans le but d'intercepter, de surveiller ou de recueillir secrètement les activités ou les données d'un utilisateur. Je tiens à assurer au Comité et à la population canadienne que les outils judiciaires numériques utilisés par les enquêteurs de l'ASFC ne sont pas des logiciels espions. Nous utilisons du matériel et des logiciels judiciaires pour déverrouiller et décrypter les appareils numériques saisis, et ce sont des outils importants dans nos efforts visant à faire respecter la législation frontalière et à protéger les Canadiens.

Encore une fois, je tiens à assurer aux membres du Comité que seuls les enquêteurs dûment formés et détenant une autorisation judiciaire utilisent cette technologie.

Je vous remercie de me donner l'occasion de comparaître devant vous. Je serai heureux de répondre à vos questions.

● (1210)

Le président: Merci, monsieur McCrorie.

Nous passons maintenant à Mme Gratton.

Vous avez cinq minutes.

[*Français*]

Mme France Gratton (commissaire adjointe, Opérations et programmes correctionnels, Service correctionnel du Canada): Bonjour à tous.

Monsieur le président et chers membres du Comité, je vous remercie de nous donner l'occasion de comparaître devant vous aujourd'hui dans le cadre de votre étude.

Je suis France Gratton et je suis la commissaire adjointe aux Opérations et programmes correctionnels au Service correctionnel du Canada. Je suis accompagnée aujourd'hui de Tony Matson, commissaire adjoint aux Services corporatifs et dirigeant principal des finances.

Assurer la protection de nos établissements et des collectivités tout en favorisant la réhabilitation en toute sécurité des délinquants demeure notre plus grande priorité.

De par sa nature, la gestion des délinquants pose divers défis. Cela comprend les menaces permanentes que représentent l'introduction et la circulation d'objets interdits. On entend par « objet interdit » tout objet dont la possession n'a pas été autorisée et qui pourrait compromettre la sécurité de l'établissement ou celle des personnes.

[*Traduction*]

Conformément aux pouvoirs qui nous sont conférés par la loi, nous saisissons les objets interdits comme les appareils électroniques. Pour faire face au risque posé par la présence de téléphones cellulaires interdits et de drogues illicites, le SCC doit faire usage de technologies facilitant la détection et la collecte de renseignements.

Dans ce contexte, le SCC s'est doté d'outils pour extraire de l'information numérique à des fins de renseignement. Nous n'utilisons pas ces outils pour mener des enquêtes sur des appareils appartenant au personnel, aux visiteurs ou aux bénévoles. L'accès à ces outils est limité et contrôlé. Ils sont utilisés uniquement sur des ordinateurs autonomes qui ne sont pas connectés à un quelconque réseau organisationnel. Des mesures de protection strictes sont en place pour limiter l'accès aux données extraites.

Par le passé, le SCC a rempli la liste de vérification de l'évaluation des facteurs relatifs à la vie privée, ou EFVP, concernant les activités de criminalistique numérique du SCC. L'utilisation d'outils améliorés pour lutter contre les activités criminelles s'étant accrue au cours des dernières années, le SCC s'est engagé à renouveler l'évaluation initiale et à remplir une liste de vérification actualisée.

Nous demeurons déterminés à respecter nos obligations en matière de protection de la vie privée au moyen des mesures de protection éprouvées et appropriées qui sont en place.

Merci. Je serai heureuse de répondre à vos questions.

[*Français*]

Le président: Je vous remercie de ce discours d'ouverture, madame Gratton.

[*Traduction*]

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

[*Français*]

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

[*Traduction*]

Bonjour, monsieur le président et honorables membres du Comité.

J'ai le plaisir d'être accompagné du surintendant Nicolas Gagné, directeur des services d'enquêtes techniques de la Direction des Opérations techniques de la GRC.

Nous vous sommes également très reconnaissants de nous donner l'occasion de vous parler aujourd'hui de l'utilisation par la GRC d'outils servant à extraire de l'information d'appareils numériques et à l'analyser. Ces outils sont essentiels aux services policiers d'aujourd'hui.

Tout d'abord, je tiens à reconnaître et à confirmer que la GRC utilise certains des outils de criminalistique numérique mentionnés dans l'article de décembre 2023 de la CBC, y compris Cellebrite et Graykey, maintenant connu sous le nom de Magnet Forensics.

Cependant, les informations diffusées dans les médias selon lesquelles ces outils de criminalistique numérique sont assimilables à des logiciels espions sont inexactes, et je vous fournirai des éclaircissements à ce sujet en répondant à vos questions.

Ces outils sont utilisés sur des appareils numériques saisis légalement dans le cadre d'enquêtes criminelles. Ils permettent d'extraire des données d'un appareil qui est en la possession de la GRC et de les analyser. Nous utilisons les autorisations judiciaires, les mandats de perquisition et les mandats généraux exigés des tribunaux, qui précisent comment des enquêteurs formés et qualifiés peuvent recueillir l'information, de quels appareils ils peuvent l'extraire et de quel délai ils disposent pour le faire. Ces outils ne sont utilisés d'aucune façon à des fins de surveillance ou de surveillance de masse.

Lors d'enquêtes criminelles, la GRC utilise ces outils uniquement pour extraire et récupérer des données à l'appui d'activités liées à son mandat dans les circonstances suivantes: avec l'autorisation judiciaire préalable des tribunaux canadiens et dans le respect des limites prescrites par le mandat de perquisition; avec le consentement volontaire du propriétaire de l'appareil, par exemple un témoin d'un crime ou la victime du crime; et dans les cas urgents où il n'est pas possible d'obtenir un mandat, conformément au Code criminel du Canada.

Lors d'enquêtes administratives, l'utilisation qu'en fait la GRC est régie par des dispositions législatives et des politiques. La capacité légale de recourir à l'aide de notre programme de criminalistique numérique existe au sein de notre organisation. La collecte d'éléments de preuves au moyen de ces outils est fondée sur la nécessité et la proportionnalité par rapport aux allégations à l'origine de l'enquête déontologique interne. Nous n'effectuerions un examen que sur des appareils appartenant à la GRC, et un mandat judiciaire serait requis en ce qui concerne tout appareil personnel.

Ces outils peuvent procurer un accès complet à l'intégralité des renseignements contenus dans l'appareil, mais seuls les renseignements expressément visés par le mandat ou pertinents par rapport à l'enquête administrative sont fournis aux enquêteurs.

Malgré les mesures de protection de la vie privée qui sont en place, la GRC reconnaît les problèmes en matière de protection de la vie privée inhérents à ces outils ainsi que le besoin de transparence et de reddition de comptes. En janvier 2021, nous avons offert une séance d'information technique au Commissariat à la protection de la vie privée au sujet des outils de criminalistique numérique, et l'évaluation des facteurs relatifs à la vie privée qui est en cours devrait être terminée d'ici la mi-2024.

Je vous remercie de nouveau de m'avoir donné l'occasion d'être ici. Nous serons heureux de répondre à vos questions.

● (1215)

Le président: Merci, sous-commissaire Larkin.

Nous allons commencer notre premier tour de six minutes.

Monsieur Brock, vous avez six minutes. Allez-y, s'il vous plaît.

M. Larry Brock: Merci, monsieur le président.

Je remercie les témoins de leur présence aujourd'hui. Je vais commencer par quelques observations préliminaires.

Cette histoire a éclaté par suite d'une demande d'accès à l'information d'un professeur de l'Université York, un expert en matière de protection de la vie privée. Les données ont été transmises à Radio-Canada, qui a communiqué avec vos organismes respectifs pour savoir s'ils utilisaient le logiciel, s'ils pouvaient confirmer son utilisation et s'ils avaient d'abord effectué des évaluations des facteurs relatifs à la vie privée. Selon leurs réponses écrites adressées à Radio-Canada, il n'y en a pas eu.

Ma première question s'adresse à l'Agence des services frontaliers du Canada, ou ASFC.

Monsieur, quand avez-vous acheté le logiciel auprès de Services partagés Canada?

M. Aaron McCrorie: Graykey a été acquis pour la première fois en mars 2019. Le premier achat d'exemplaires de Cellebrite Premium a eu lieu en mars 2021.

M. Larry Brock: Combien de fois avez-vous utilisé ce logiciel en particulier?

M. Aaron McCrorie: Je ne pourrais pas vous dire exactement combien de fois nous avons utilisé le logiciel. Ce que je peux vous dire, c'est qu'en 2023, par exemple, nous avons mené 119 enquêtes criminelles dans le cadre desquelles nous avons saisi 712 dispositifs. Lorsque nous disons « 712 dispositifs », cela comprend, par exemple, la carte mémoire ou la carte SIM qui se trouvent dans un téléphone cellulaire, de sorte qu'un téléphone cellulaire pourrait compter comme trois dispositifs.

M. Larry Brock: Pourriez-vous communiquer au Comité le nombre de fois que vous avez utilisé ce logiciel depuis la date d'achat?

M. Aaron McCrorie: Nous ferons de notre mieux. Je ne peux pas vous assurer que nous pouvons compter chaque cas d'utilisation, mais nous pouvons certainement vous fournir des statistiques.

M. Larry Brock: Nous parlons de centaines.

M. Aaron McCrorie: Je dirais que oui.

En 2021, nous avons saisi…

M. Larry Brock: Nous parlons de centaines d'enquêtes menées à l'aide de ce logiciel, et votre ministère n'a jamais demandé d'évaluation des facteurs relatifs à la vie privée. Est-ce exact?

M. Aaron McCrorie: Nous avons le FRP, qui signifie fichier… Excusez-moi, j'oublie la signification de l'acronyme.

M. Larry Brock: Vous parlez de l'EFVP?

M. Aaron McCrorie: C'est un FRP.

Nous affichons en ligne les types de renseignements que nous recueillons, les circonstances dans lesquelles nous les recueillons et la façon dont nous les utilisons.

Nous avons lancé notre processus interne en vue de la tenue d'une EFVP à l'échelle du programme, car nous voulons le faire à l'échelle du programme et non au niveau des appareils.

M. Larry Brock: Vous comprenez, monsieur, que l'EFVP n'est pas facultative.

M. Aaron McCrorie: Oui.

M. Larry Brock: C'est une directive du Conseil du Trésor.

M. Aaron McCrorie: Oui.

M. Larry Brock: Selon son témoignage de la semaine dernière, le commissaire a communiqué avec votre organisme pour savoir précisément quand vous alliez commencer à mener des EFVP. Vous avez répondu que vous étiez en train d'examiner la question, ou que vous étiez sur le point de le faire.

Quelle a été votre véritable réponse? Êtes-vous toujours en train d'envisager d'exécuter ce processus obligatoire, ou l'avez-vous effectivement lancé par suite de cette controverse?

● (1220)

M. Aaron McCrorie: Comme je l'ai dit dans ma déclaration préliminaire, nous avons lancé le processus en vue d'effectuer une évaluation des facteurs relatifs à la vie privée visant l'ensemble du Programme des enquêtes criminelles en 2022. Ce faisant, nous suivons nos procédures internes.

Par conséquent, nous allons maintenant de l'avant avec l'EFVP, dans le cadre de laquelle nous allons collaborer avec le commissaire à la protection de la vie privée.

M. Larry Brock: Il y a une crise des vols de voitures au Canada. Elle est en train de prendre des proportions alarmantes, à tel point que le gouvernement organise un sommet. Il aura lieu jeudi, je crois.

L'ASFC est chargée de protéger nos frontières. Est-ce exact?

M. Aaron McCrorie: Entre autres… oui.

M. Larry Brock: À cause de la mauvaise gestion qu'en font Justin Trudeau et le gouvernement actuel, nos ports fédéraux sont devenus des parcs de stationnement pour voitures volées, qui disparaissent ensuite à l'étranger. Par exemple, au port de Montréal — d'où la majorité des voitures volées quittent le Canada — il n'y a que cinq agents de l'ASFC pour inspecter l'énorme quantité de conteneurs expédiés chaque année, selon *Le Journal de Montréal*. Il y a aussi un appareil à rayon X qui se brise constamment. Les ports fédéraux de Vancouver, de Prince Rupert et de Halifax sont aux prises avec une situation semblable.

Selon Mark Haywood, détective de la police de Peel, l'ASFC vérifie moins de 1 % des conteneurs qui quittent le pays. Nous parlons de milliers de conteneurs par semaine. Pourquoi?

Compte tenu de tout l'argent que le gouvernement verse à l'ASFC, pourquoi contribuez-vous à cette crise...

Mme Pam Damoff (Oakville-Nord—Burlington, Lib.): J'invoque le Règlement, monsieur le président.

Quel est le rapport avec notre étude?

Le président: Merci de votre rappel au Règlement. Je crois avoir déjà mentionné, madame Damoff, que j'accorde généralement beaucoup de latitude aux députés. Je m'attends à ce que M. Brock revienne au sujet qui nous occupe.

Nous allons voir. Il lui reste une minute et 31 secondes.

Monsieur Brock, allez-y, s'il vous plaît. Vous avez la parole.

M. Larry Brock: Son titre est « Renseignement et exécution de la loi ». Il est tout à fait apte à répondre à la question que je lui pose.

Compte tenu des centaines de millions de dollars que le gouvernement transfère à l'ASFC pour vous aider à appliquer la loi et à mener des inspections, pourquoi néglige-t-elle à un tel point ses responsabilités quant à l'inspection de ces conteneurs? De toute évidence, le message que cela envoie au monde interlope et aux groupes du crime organisé, c'est que le Canada est un refuge pour ce genre d'activité.

Nous avons ici des représentants des forces de l'ordre qui, j'en suis sûr, sont très frustrés par le peu d'attention que vous accordez à cette question. Je vous prie d'expliquer aux forces de l'ordre pourquoi nous n'avons que cinq agents.

M. Aaron McCrorie: Ce que je dirais, c'est que, en fait, nous sommes un partenaire clé des forces de l'ordre partout au pays.

Au cours de la dernière année, nous avons participé à 14 opérations conjointes avec la police locale dans la région de Toronto, par exemple. Nous travaillons en étroite collaboration avec la police en Ontario et au Québec dans le cadre d'une approche fondée sur le risque en matière d'examen des conteneurs.

Je crois que vous pouvez comprendre qu'il est tout à fait impossible de fouiller chaque conteneur qui entre dans un port ou qui en sort…

M. Larry Brock: Pourquoi?

M. Aaron McCrorie: À cause du volume et du nombre considérables de conteneurs, qui se comptent par milliers…

M. Larry Brock: Demandez des ressources.

M. Aaron McCrorie: Ce que nous faisons, c'est que nous adoptons une approche fondée sur le risque en utilisant les renseignements que nous obtenons de nos partenaires des forces de l'ordre…

M. Larry Brock: Le message que nous envoyons au monde entier, c'est que nous n'inspectons pas les conteneurs qui partent et que nous n'inspectons pas les conteneurs qui arrivent. C'est pourquoi nous avons une crise du fentanyl. Il y a les drogues illicites et mortelles en provenance de l'Asie qui ne sont pas inspectées dans les ports de Vancouver.

Mme Iqra Khalid: J'invoque le Règlement, monsieur le président.

Le président: Monsieur Brock, les six minutes sont écoulées.

Merci, monsieur.

M. Larry Brock: Merci.

Le président: Allez-y avec votre rappel au Règlement, madame Khalid.

Mme Iqra Khalid: Je voulais simplement mentionner que, à moins qu'il s'agisse de vols d'automobile commis au moyen de dispositifs de surveillance, je ne vois pas en quoi cela est pertinent, monsieur le président.

Le président: Je comprends. Merci.

Allez-y, madame Damoff.

Mme Pam Damoff: Merci, monsieur le président.

Merci à tous les témoins d'être ici.

Je vais commencer par une question de pure forme. Je me demande si M. Brock est en train de suggérer que ce logiciel soit utilisé pour lutter contre le vol d'automobiles. Je n'ai pas entendu cela dans sa question.

Le commerce serait paralysé si nous inspections chaque conteneur qui quitte le Canada. N'est-ce pas exact?

M. Aaron McCrorie: Si nous inspections chaque conteneur qui entre au pays et qui en sort, cela paralyserait le commerce.

Mme Pam Damoff: Merci.

Pour ce qui est de notre étude proprement dite, j'ai une brève question.

M. Michael Barrett: Monsieur le président, j'invoque le Règlement.

Deux députés libéraux ont interrompu M. Brock à cause de la nature de ses questions, puis Mme Damoff a poursuivi exactement dans la même veine.

Monsieur le président, il ne s'agit pas d'une question concernant le Règlement ou la pertinence. Il s'agit d'essayer d'interrompre un député qui a légitimement la parole, dont le temps n'est pas écoulé, qui pose des questions au témoin et qui lui donne l'occasion de répondre.

Nous avons déjà vu cela. Si nous voulons que les réunions se déroulent dans le chaos le plus total, cette invitation peut être acceptée, mais maintenant que nous voyons qu'il y a des jeux qui se jouent, je pense que les interruptions de la part des députés libéraux doivent cesser.

● (1225)

Le président: Merci, monsieur Barrett.

Là encore, vous siégez tous avec moi à ce comité depuis assez longtemps pour savoir que je donne généralement beaucoup de latitude aux membres pour qu'ils utilisent leur temps comme bon leur semble. Des experts sont parmi nous. Oui, nous avons un sujet à traiter, et je m'attends à ce que nous y revenions.

Franchement, je n'aime pas ces constantes interruptions et invocations du Règlement fondées sur le simple fait que les propos d'une personne ou la nature de ses questions déplaisent. Cela vaut pour tous les partis.

Madame Damoff, il vous reste cinq minutes et 22 secondes. Veuillez poursuivre vos questions.

Vous avez la parole. Allez-y, s'il vous plaît.

Mme Pam Damoff: Merci.

J'aimerais que vous répondiez tous les trois très rapidement. Nous pourrions peut-être commencer par la GRC et poursuivre dans cet ordre.

Ce logiciel est-il utilisé sur les téléphones de vos employés?

S.-comm. Bryan Larkin: Nous n'utilisons pas le logiciel sur les téléphones des employés. Nous avons la capacité de l'utiliser parce que nos téléphones sont déployés de façon opérationnelle. Chaque membre signe un formulaire de consentement quant à l'utilisation de l'appareil, etc. Toutefois, nous ne les surveillons pas activement. Cela se produirait par suite d'une allégation particulière relative à un code de déontologie ou à une enquête criminelle.

Comme je l'ai mentionné, s'il s'agit d'une enquête criminelle, nous demanderons toujours une autorisation judiciaire. S'il s'agit d'un code interne, l'enquêteur consultera éventuellement les spécialistes de la criminalistique numérique et évaluera si c'est nécessaire ou non.

Mme Pam Damoff: Merci.

M. Aaron McCrorie: Merci de la question.

Non. Nous utilisons ces outils uniquement dans le cadre d'enquêtes criminelles liées à notre mandat frontalier, toujours en vertu d'une autorisation judiciaire.

Mme Pam Damoff: Merci.

Mme France Gratton: La réponse est non. Nous n'utilisons pas les logiciels sur les téléphones cellulaires des employés. Nous l'utilisons seulement sur les téléphones cellulaires interdits qui ont été saisis après avoir été introduits illégalement dans notre établissement.

Mme Pam Damoff: Merci. Ma prochaine question s'adresse à l'ASFC.

Vous avez parlé d'appareils saisis. Si je subis un contrôle de sécurité à mon entrée au Canada, que je suis soumise à un contrôle secondaire et que mon téléphone est saisi, est-ce que ce logiciel serait utilisé dans une telle situation?

M. Aaron McCrorie: Non.

Il y a deux situations distinctes ici. Lorsque vous traversez la frontière, il y a des exigences réglementaires applicables qui nous permettent d'effectuer une fouille. Si on procède à la fouille d'un téléphone cellulaire, nous le faisons manuellement, avec la coopération de la personne qui est devant nous.

Au sein de mon organisation, cette technologie est utilisée dans le cadre d'enquêtes criminelles qui, la plupart du temps, ont lieu dans un bureau intérieur et ont trait à des choses comme la contrebande d'armes à feu ou des violations de la Loi sur l'immigration et la protection des réfugiés. Cela concerne, par exemple, des infractions prévues à la Loi sur l'immigration et le fait de conseiller aux gens de faire de fausses déclarations à leur propre sujet afin d'obtenir de nouveaux documents d'immigration.

Mme Pam Damoff: Lorsqu'il y a saisie et examen manuel, ce logiciel n'est pas utilisé?

M. Aaron McCrorie: Non.

Mme Pam Damoff: D'accord. Merci.

Je pense que la GRC serait mieux placée pour en parler.

Pouvez-vous expliquer la procédure que vous devez suivre afin d'extraire des renseignements d'un téléphone cellulaire? Il s'agit d'une enquête criminelle. Quelle procédure devez-vous suivre pour pouvoir utiliser ce logiciel ou quoi que ce soit d'autre afin d'accéder à un téléphone?

M. Nicolas Gagné (surintendant, Gendarmerie royale du Canada): L'examinateur en criminalistique numérique doit d'abord obtenir une copie du mandat — l'autorisation judiciaire — pour en établir la portée. Il détermine l'outil à utiliser en fonctions des capacités, lesquelles varient selon la marque, le modèle et le système d'exploitation. Il extrait, dans la mesure du possible, une image de l'appareil. Parfois, ce n'est pas possible. Il arrive qu'il soit impossible d'extraire quoi que ce soit. Une fois les renseignements extraits, l'examinateur en criminalistique numérique les restreint à l'ampleur et à la portée du mandat.

C'est le rapport qui serait remis à l'enquêteur.

Mme Pam Damoff: Certains ont insinué que ce logiciel était utilisé pour accéder aux téléphones des Canadiens. Si je comprends bien, vous dites tous que, si ce logiciel est utilisé pour le grand public... Nous avons déjà entendu dire qu'il était utilisé sur des téléphones d'employés. Aucun d'entre vous n'est dans cette situation, mais je pense que, de façon plus générale, les Canadiens peuvent avoir l'assurance que vous n'accédez pas à leurs téléphones cellulaires sans suivre la procédure judiciaire voulue.

● (1230)

S.-comm. Bryan Larkin: C'est exact. Ces outils visent un appareil en particulier. Par exemple, en 2023, nous avons examiné 6 452 appareils — notamment des téléphones intelligents, des tablettes et des ordinateurs — à l'échelle du pays, mais ces appareils étaient visés par une autorisation judiciaire, de sorte que nous disposons d'une preuve tangible. Comme je l'ai mentionné, un témoin ou une victime d'un crime peut donner son consentement parce qu'il veut fournir une preuve documentaire.

Compte tenu de la complexité de la question, j'aimerais proposer quelque chose au Comité. Si vous souhaitez assister à une séance d'information technique, le surintendant Nicolas Gagné et son équipe, à votre convenance et celle de la greffière, seraient heureux de vous accueillir dans une installation de la GRC et de vous expliquer comment nous extrayons des preuves numériques en vertu d'une autorisation judiciaire afin que vous puissiez comprendre la complexité, l'ensemble de compétences, la formation et le travail que nous faisons.

Mme Pam Damoff: Merci.

En fait, j'ai déjà assisté à une séance d'information technique de la GRC sur un autre sujet, et je serais ravie d'accepter votre proposition. J'encouragerais peut-être le président à donner suite à l'offre qui vient d'être faite au Comité.

Le président: Merci, madame Damoff.

Je veux seulement informer les membres que, si cela les intéresse, il faudra présenter, au nom du Comité, une demande de déplacement qui sera envoyée au Comité de liaison. Je crois que la date limite est le 16 février. C'est une chose que le Comité doit examiner.

[*Français*]

Monsieur Villemure, vous avez la parole pour six minutes.

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

Je vais m'adresser aux trois organismes et leur demander de répondre à tour de rôle.

Lors de l'enquête de Radio-Canada, vous avez dit ne pas avoir réalisé d'évaluation des facteurs relatifs à la vie privée. Ai-je bien compris?

Commençons par vous, monsieur Larkin.

[*Traduction*]

S.-comm. Bryan Larkin: C'est exact.

Nous sommes en train d'y mettre la dernière main. Nous avons rencontré le commissaire à la protection de la vie privée en 2021. Cependant, nous prévoyons que notre évaluation des facteurs relatifs à la vie privée sera terminée d'ici 2024. Nous n'avons pas mené d'évaluation pour ce qui est des outils de criminalistique numérique. Nous en avons effectué une concernant les outils d'enquête sur appareil. En fait, elle est affichée sur notre site Web.

[*Français*]

M. René Villemure: Merci.

Monsieur McCrorie, je vous écoute.

[*Traduction*]

M. Aaron McCrorie: Pour l'instant, nous utilisons le fichier de renseignements personnels pour présenter les renseignements que nous recueillons et la façon dont nous les utilisons. Nous sommes aussi en train d'effectuer une EFVP, et nous espérons la mener... Ce sera probablement un peu plus long que pour la GRC, mais nous espérons la mener en collaboration avec le Commissariat à la protection de la vie privée.

[*Français*]

M. René Villemure: C'est donc en cours, mais ce n'est pas terminé.

[*Traduction*]

M. Aaron McCrorie: Exactement.

[*Français*]

M. René Villemure: Madame Gratton, c'est à vous.

Mme France Gratton: Dès l'achat du logiciel en 2010, nous avons effectué la série de vérifications qui permettent de déterminer si une évaluation des facteurs relatifs à la vie privée est nécessaire. Selon le programme que nous mettions en place, l'outil que nous allions utiliser et la façon dont l'information allait être gérée, il a été déterminé que ce n'était pas nécessaire.

M. René Villemure: D'accord. Est-ce la réponse que vous avez donnée à Radio-Canada dans le cadre de son enquête?

Mme France Gratton: Oui, nous avons répondu que nous avions suivi la liste des vérifications en vue d'une évaluation des facteurs relatifs à la vie privée.

M. René Villemure: Monsieur McCrorie, avez-vous répondu la même chose à Radio-Canada dans le cadre de son enquête, c'est-à-dire que vous étiez en train de suivre le processus, ou avez-vous répondu non?

[*Traduction*]

M. Aaron McCrorie: Ce que nous avons fait, c'est que nous avons décrit le processus que nous suivions. Tout comme nos collègues du Service correctionnel, nous avons évalué les besoins conjointement avec nos collègues à l'interne. Ce que nous avons établi, c'est qu'au lieu de faire une EFVP pour chaque appareil, nous devions mener une EFVP visant l'ensemble du programme. Il ne s'agit donc pas seulement de la façon dont nous utilisons un appareil donné, mais aussi de la façon dont les appareils sont utilisés dans le cadre du programme.

[*Français*]

M. René Villemure: Est-ce ce que vous avez répondu à Radio-Canada dans le cadre de son enquête?

M. Aaron McCrorie: Je suis désolé, mais il faudrait que je confirme les mots exacts que nous avons utilisés pour répondre à Radio-Canada.

M. René Villemure: D'accord.

Monsieur Larkin, je vous écoute.

S.-comm. Bryan Larkin: Je répondrais la même chose. Je ne suis pas sûr de ce que nous avons répondu à Radio-Canada, mais nous allons vérifier cela.

M. René Villemure: D'accord.

Madame Gratton, tantôt, vous avez parlé de proportionnalité de l'usage de cet outil. Pouvez-vous nous en dire plus?

Mme France Gratton: J'ai dit que nous utilisions l'outil pour des objets qui ont été saisis. Nous constatons une augmentation marquée du nombre d'incidents impliquant des drones, ainsi qu'une augmentation importante du nombre de téléphones cellulaires qui sont saisis dans les établissements.

Par conséquent, à des fins de collecte de renseignements de sécurité, nous utilisons ces systèmes pour extraire des données et prévenir d'autres incidents. Pour ce qui est de la proportionnalité de l'usage de cet outil, celui-ci est effectivement nécessaire pour s'attaquer à la contrebande et prévenir les incidents de sécurité.

● (1235)

M. René Villemure: Diriez-vous qu'il est plus facile d'obtenir de l'information à l'aide de l'outil même si, en fin de compte, cela exige des autorisations qui sont également difficiles à obtenir?

Mme France Gratton: Non, ce n'est pas plus facile. L'information ainsi obtenue s'ajoute à d'autres renseignements de sécurité que nous avons déjà. Elle nous permet d'aller plus loin dans nos démarches pour prévenir l'introduction dans nos établissements de marchandise de contrebande.

M. René Villemure: Merci.

Monsieur McCrorie, je vous pose la même question: utilisez-vous l'outil parce que c'est plus facile? L'information ainsi obtenue est-elle plus fiable même si cela implique une évaluation des facteurs relatifs à la vie privée et d'autres méthodes?

[*Traduction*]

M. Aaron McCrorie: Je ne pense pas que la question soit de savoir si c'est plus… Pour accéder à un appareil verrouillé avec un mot de passe, nous avons besoin de la technologie. À une autre époque, nous aurions demandé à un serrurier d'ouvrir une boîte contenant des reçus, par exemple. Aujourd'hui, lorsque nous avons affaire à de la contrebande d'armes à feu, les reçus électroniques se trouvent dans un téléphone cellulaire ou un ordinateur. Notre seul moyen d'accéder à cette information est de déverrouiller l'appareil et de traduire ensuite l'information qu'il contient sous une forme qui peut être utilisée devant un tribunal.

La question n'est pas de savoir si c'est plus facile. Il s'agit de la technologie que nous devons utiliser pour suivre l'évolution de la technologie utilisée par les criminels.

[*Français*]

M. René Villemure: D'accord.

Monsieur Gagné, je crois que vous avez une réponse à cette question.

M. Nicolas Gagné: Monsieur le président, je partage le point de vue de M. McCrorie. Les outils technologiques servent à obtenir des preuves nécessaires aux enquêtes. Ce n'est pas une question de facilité, c'est une question d'avoir autant que possible accès à des preuves.

M. René Villemure: Utilisez-vous les outils pour contourner le mot de passe qui verrouille le téléphone ou pour obtenir l'information qui se trouve dans le téléphone?

M. Nicolas Gagné: Ça dépend de plusieurs facteurs, comme la marque, le modèle ou les types de mesures de verrouillage du téléphone. Contourner le mot de passe n'est qu'une des nombreuses choses que l'outil permet de faire.

M. René Villemure: C'est parfait.

Madame Gratton, nous tentons au Comité d'évaluer diverses situations en vue de proposer des améliorations législatives permettant d'obtenir de meilleures politiques publiques.

La protection de la vie privée est un sujet qui est sur toutes les lèvres depuis longtemps. Les gens sont craintifs. Dans les divers témoignages que nous entendons au Comité, les gens nous disent que, quand ils cliquent en ligne sur « j'accepte », ils ne savent pas toujours ce qu'ils acceptent. Ils savent qu'ils veulent obtenir un logiciel, par exemple, mais nous nous rendons compte que l'éducation sur la vie privée n'est pas adéquate.

Une autre des tâches confiées au Comité est de préserver la confiance du public envers des institutions comme la Gendarmerie royale du Canada, l'Agence des services frontaliers du Canada et le Service correctionnel du Canada.

Certaines nouvelles parues dans les médias, comme celle publiée par CBC/Radio-Canada, peuvent semer des doutes dans l'esprit du public. Dès la publication de la nouvelle en question, les gens m'ont interpellé pour me demander ce qui se passait. Ils étaient craintifs. Croyez-vous être en mesure de renforcer la confiance du public ce matin grâce à votre témoignage visant à expliquer aux gens comment vous vous servez des outils technologiques?

Le président: Monsieur Villemure, votre témoin devra répondre très rapidement, car votre temps est écoulé.

Mme France Gratton: Pour ce qui est de la confiance, il est important de souligner que ces outils technologiques nous permettent d'augmenter la sécurité dans nos établissements. Comme ils sont utilisés sur des téléphones cellulaires de contrebande, ils servent donc à des fins très précises, et l'information extraite des téléphones cellulaires est utilisée à des fins de renseignement seulement. Je pense ainsi démontrer que les outils dont on parle ne sont pas utilisés hors du cadre de ce mandat.

M. René Villemure: D'accord, je vous remercie beaucoup.

[*Traduction*]

Le président: Merci.

Monsieur Green, vous avez six minutes. Allez-y, s'il vous plaît.

M. Matthew Green: Merci.

Comme je le disais à mon collègue, je viens de demander que plus de 100 organisations nous transmettent de l'information, et j'ai de la difficulté à imaginer qu'il y aura beaucoup d'écart dans les réponses que nous allons recevoir.

Je pense que nous avons établi — n'hésitez pas à me corriger si je me trompe — que cette technologie est utilisée à des fins d'enquête par des organismes d'application de la loi ou par des membres du personnel, c'est-à-dire des employés fédéraux. Je crois comprendre que la plupart d'entre vous le font dans le cadre prévu par la loi.

Est-ce que l'un ou l'autre de vos organismes l'a utilisée relativement à ses employés?

S.-comm. Bryan Larkin: Nous l'avons utilisée à une occasion dans le cadre d'une affaire interne concernant le consentement, en fait. Nous avons utilisé des outils de criminalistique numérique. C'était une affaire relative au consentement.

M. Matthew Green: D'accord.

Monsieur McCrorie.

M. Aaron McCrorie: Pas à ma connaissance.

M. Matthew Green: Madame Gratton.

Mme France Gratton: Non, nous ne l'avons pas utilisée relativement à des employés.

M. Matthew Green: Excusez-moi. Je ne veux pas contester qui que ce soit, mais les drones comptent parmi les moyens utilisés pour introduire des objets interdits. On laisse parfois entendre que le personnel est, à de rares occasions, impliqué dans la contrebande.

Avez-vous déjà eu l'occasion d'enquêter ou d'utiliser cette technologie relativement à un membre du personnel correctionnel?

● (1240)

Mme France Gratton: Non. Il est arrivé que nous menions une enquête concernant un membre du personnel. Nous n'utiliserions pas de logiciel légal particulier. Il faudrait que ce soit expressément dans le cadre d'une enquête.

M. Matthew Green: Est-il juste de dire que tous vos employés reçoivent des appareils fournis par le gouvernement fédéral?

S.-comm. Bryan Larkin: Oui, une grande partie d'entre eux. C'est exact.

M. Matthew Green: Dans votre cas, aucun d'entre eux n'est jamais contrôlé de cette façon.

M. Aaron McCrorie: De par son mandat, mon organisation est tournée sur l'extérieur. Nous menons des enquêtes criminelles sur des infractions aux lois frontalières.

M. Matthew Green: Très bien.

Indépendamment des vols de voitures, je pense que nous avons établi les faits, à savoir que les membres de ce groupe de témoins — qui, selon moi, auraient les meilleures raisons et seraient les plus susceptibles d'utiliser cette technologie à des fins d'enquête — ont fourni des réponses très claires quant à ce que c'est et à ce que ce n'est pas. J'en conviens.

Nous avons tous ces autres groupes, et je le dis simplement pour la gouverne du Comité, pas dans le cadre de mes questions… Nous avons au moins trois ou quatre réunions de deux heures chacune là-dessus.

Le président: Il y en a au moins six.

M. Matthew Green: Je vais vous dire tout de suite que j'ai de la difficulté à voir à quoi cela aboutira pour ce qui est de la valeur et du rendement décroissant des questions.

Je vais avouer au Comité que je me demande si nous pourrions communiquer par voie électronique avec les gens et leur transmettre une liste de questions dont nous aurons convenu en vue d'obtenir des réponses, car je ne sais pas ce que cela donnera de continuer ainsi pendant encore 3 jours, 6 heures, 8 heures ou 10 heures. Je sais qu'il y a beaucoup de gens qui ont déposé des motions. Je tiens également à dire que j'en suis maintenant à un point où j'espère ramener le Comité à son calendrier législatif et l'éloigner de ce qui a fait les manchettes hier de manière à ce qu'il fasse son important travail et, espérons-le, qu'il commence à s'occuper des lacunes dans la législation.

Je ne sais pas du tout combien de temps il me reste, mais je n'ai plus de questions.

Je vous remercie tous d'être ici. Je ne pense pas qu'il y ait quoi que ce soit à ajouter au sujet de la portée de votre travail. Je vous suis reconnaissant de ce que vous faites. Je dirais que j'ai hâte de vous revoir ici, mais ce n'est pas toujours le cas.

Sur ce, je cède mon temps au Comité.

Le président: Merci, monsieur Green. Je vais utiliser les deux minutes qu'il vous reste pour expliquer où nous en sommes à ce moment-ci, pour la gouverne du Comité.

Un autre groupe de témoins doit comparaître jeudi. Je ne crois pas que l'avis de convocation ait été publié pour l'instant, mais il le sera plus tard aujourd'hui. Selon la liste qui figurait dans la motion, les groupes seront composés de représentants d'au moins trois ou quatre de ces ministères.

La greffière a recueilli toutes les coordonnées concernant la motion adoptée l'autre jour au sujet des évaluations des facteurs relatifs à la vie privée. Nous n'avons rien fait à cet égard parce que nous venons de recevoir la liste complète pendant la réunion. Cela nous amène à la semaine prochaine, moment où nous sommes censés poursuivre avec d'autres groupes de témoins selon la motion. Cela nous amène au 27, date à laquelle le commissaire et le sergent d'état-major de la GRC viendront nous parler de la motion relative à SNC-Lavalin qui a également été adoptée.

Voilà où nous en sommes pour ce qui est des réunions du Comité, monsieur Green.

Allez-y, monsieur.

M. Matthew Green: Le groupe que je suis le plus désireux d'entendre est celui des syndicats. Je veux entendre les représentants, car s'il n'y a pas de véritable plainte de la part des représentants des fonctionnaires fédéraux proprement dits, il devient très difficile pour moi de poursuivre quelque chose qui pourrait ou non constituer une question de protection de la vie privée. Il me semble que les cas de violations des droits à la vie privée des employés seraient énoncés très explicitement dans les conventions collectives.

Si possible, monsieur le président, il faudrait accorder la priorité aux invitations à comparaître destinées aux représentants syndicaux. À mon avis, cela permettrait de déterminer s'il s'agit de quelque chose que je juge bon de poursuivre.

Le président: C'est une réunion très dynamique. Nous venons de recevoir une confirmation de l'Institut professionnel de la fonction publique au sujet de Jennifer Carr, dont le nom figurait sur la liste. Sa présence est confirmée pour le 15 février. Nous pourrons peut-être progresser. Nous avons reçu une autre confirmation de l'un des syndicats, M. Green. Nous pourrions adapter le calendrier des réunions en fonction de ce que vous avez dit, mais nous avons la présidente de l'Institut professionnel de la fonction publique, Mme Carr.

Nous en sommes encore à nos séries de questions, mais je vais donner la parole à M. Barrett pour quelques commentaires. Je donnerai également la parole à Mme Khalid ou à d'autres membres s'ils ont des commentaires à formuler.

Allez-y, monsieur Barrett.

● (1245)

M. Michael Barrett: Je suis généralement d'accord avec l'idée d'éviter que nos réunions ressemblent au *Jour de la marmotte*, mais je crois que la question de la responsabilité ministérielle est importante. Les EFVP ne sont pas facultatives, donc si nous devons établir un plan de travail en vue de conclure nos travaux en moins de six réunions et que M. Green veut accorder la priorité à la comparution des représentants des travailleurs, si cette case est cochée, alors je dirais que nous devrions accorder la priorité à la comparution des personnes qui sont responsables de ne pas avoir effectué les EFVP.

Nous devrions établir l'ordre de priorité des ministres que nous voulons entendre. Je pense qu'il a été question de faire comparaître le ministre de l'Approvisionnement ou la présidente du Conseil du Trésor devant le Comité, alors nous devrions les inscrire dans les livres. Ensuite, M. Kurek a suggéré que, s'il y a des questions pour les autres ministères, nous devrions peut-être les recueillir auprès des membres de tous les partis, fixer une date limite, communiquer les questions aux ministères en précisant le délai de réponse, puis passer à autre chose.

Le président: D'accord. Je vous remercie de ces commentaires, monsieur Barrett.

En tant que président, je suis guidé par la greffière et les analystes pour ce qui est du respect de la motion adoptée par le Comité. S'il y a une volonté d'accepter certaines des suggestions formulées au cours de cette discussion, j'aurai besoin de l'avis du Comité quant à ce qu'il faut faire à ce sujet.

Madame Khalid, M. Villemure vous a cédé son temps de parole. Allez-y, s'il vous plaît, madame Khalid.

Je vais simplement demander aux témoins de faire preuve de patience, car nous pourrions reprendre les questions. Il ne nous reste pas beaucoup de temps.

Madame Khalid, allez-y.

Mme Iqra Khalid: Merci beaucoup, monsieur le président.

Je pense vraiment que la question qui a été soulevée est importante. Je suis très intriguée par certains témoignages que nous avons entendus jusqu'à maintenant. Je suis tout à fait d'accord avec M. Green pour dire que nous devons entendre les représentants des syndicats et de la fonction publique.

M. Matthew Green: Je vais inscrire cela sur mon affiche de campagne.

Mme Iqra Khalid: Je pense vraiment qu'au lieu de mettre fin à l'étude maintenant, nous devrions l'abréger et voir si le Comité a quelque chose à recommander pour faire en sorte que la confidentialité et les évaluations des facteurs relatifs à la vie privée soient appréciées à leur juste valeur au sein de nos ministères.

À ce moment-ci, je suis en faveur de l'idée que nous abrégions l'étude en mettant davantage l'accent sur les syndicats et la fonction publique, comme l'a suggéré M. Green, et que nous partions de là.

Le président: Je vous remercie de vos commentaires. Je peux vous dire que la présidente du Conseil du Trésor a été invitée. Nous attendons de connaître la date.

Ce que j'entends, ce sont les deux côtés. Il y a ce que M. Green a proposé, puis ce que M. Barrett a proposé. M. Green veut entendre ce que les personnes touchées ont à dire. M. Barrett veut entendre les responsables. La greffière, les analystes et moi-même pourrions peut-être trouver une façon d'arriver à ce point au cours des prochaines réunions. Le problème, c'est que la réunion doit avoir lieu jeudi, et les ministères y participeront conformément à la motion. Nous pouvons poursuivre dans cette voie. Nous pourrions réduire le nombre de réunions de six à peut-être cinq pour l'instant, parce que c'est la deuxième que nous avons eue à ce sujet.

Monsieur Green, je vous ai vu lever la main. Allez-y, s'il vous plaît.

M. Matthew Green: Nous pouvons négocier en public avec la présidente du Conseil du Trésor et les membres du personnel qui nous regardent et leur dire que, s'ils peuvent se présenter devant le Comité le plus tôt possible, nous pourrons conclure. Autrement, nous nous retrouverons dans la situation où tous les ministères devront comparaître devant le Comité. Espérons que cela incitera la présidente à venir comparaître ici.

● (1250)

Le président: Voici donc ce que j'aimerais faire.

Monsieur Green, si c'est possible, nous pouvons continuer pendant les prochaines minutes avec nos témoins. Je propose que nous poursuivions à la prochaine réunion avec les ministères. Nous aurons une réunion sur les travaux du Comité, au cours de laquelle je pourrai faire le point sur notre situation avec les témoins. Nous avons consacré 10 ou 15 minutes à ce sujet, ce qui est injuste pour les témoins qui se sont présentés aujourd'hui.

Je pense que le Comité nous a clairement indiqué la voie à suivre. Je demande maintenant que nous poursuivions avec nos témoins. Nous continuerons lors de la réunion de jeudi, puis nous tiendrons une réunion du sous-comité à ce moment-là. Je vais prévoir du temps pour cela, si cela vous convient. Je pourrai ensuite vous dire où se trouve la présidente du Conseil du Trésor et où se trouvent certains des autres témoins qui ont été proposés ici dans le cadre de cette discussion. Cela vous convient-il? Sommes-nous d'accord? Bien.

Le tour de M. Green est terminé.

Je crois que c'est au tour de M. Kurek, pour cinq minutes.

Allez-y.

Nous allons avoir des tours très courts. Nous disposons d'un peu de temps supplémentaire en raison de la suspension, mais nous aurons deux fois cinq minutes et deux fois deux minutes et demie, puis nous conclurons.

Allez-y, monsieur Kurek.

M. Damien Kurek: Merci beaucoup.

Je remercie les témoins.

Je vais seulement vous donner un conseil non sollicité. Soyons proactifs en ce qui concerne les EFVP. Le commissaire a comparu devant le Comité et a dit qu'il voulait travailler avec vous et qu'il serait le plus réceptif possible, alors assurons-nous — plutôt que de l'apprendre par les médias et de subir cette comédie — que les ministères, les organismes et les autres intervenants sont proactifs. Je pense que cela vous évitera à tous beaucoup de ces questions difficiles.

Au cours de la première heure de la réunion, nous avons entendu différents témoins qui ont beaucoup parlé de l'utilisation potentielle de cette technologie pour les employés. Je sais qu'il y a ECCC, RNCan et une foule d'autres. Vous en parlez relativement à l'application de la loi, mais si vous me le permettez, j'aimerais savoir où vous en êtes en ce qui concerne les gens qui travaillent pour vos ministères… ceux qui font partie de l'administration chargée de l'application de la loi. Je ne parle pas du programme en particulier, parce que vous avez répondu très clairement à ce sujet, mais j'aimerais que vous me disiez s'il existe des outils, des techniques et des méthodes qui vous permettraient d'observer les employés et les autres personnes qui travaillent pour vous pour ce qui est des données qui pourraient se trouver sur leurs appareils.

Commençons par la GRC. J'espère que les réponses seront très brèves, parce que j'ai d'autres questions.

S.-comm. Bryan Larkin: Merci de votre question.

Bref, non, nous n'utilisons aucune technologie pour surveiller, gérer ou superviser nos employés. Nous avons un contrat d'utilisation pour tous les appareils que nous déployons. Nous avons une politique qui régit l'utilisation de ces appareils.

Naturellement, au sein de notre organisation, il arrive que des membres fassent l'objet d'allégations concernant le code de conduite ou des obligations pénales, et il se peut que nous devions lancer une enquête interne, dont une partie pourrait consister à envisager l'utilisation d'outils d'investigation numériques. Comme je l'ai mentionné, nous les avons utilisés à une occasion avec le consentement des intéressés.

M. Damien Kurek: Je m'excuse, mais je n'ai vraiment pas beaucoup de temps.

Monsieur McCrorie, allez-y.

M. Aaron McCrorie: Je le répète, les enquêtes sur les normes professionnelles se font à l'extérieur de mon organisation. Il m'est donc difficile de commenter leurs techniques et ce qu'elles font.

M. Damien Kurek: Je vous demanderais de poser la question à la personne responsable au sein de l'ASFC et de lui demander de fournir la réponse au Comité par écrit. Ce serait très utile.

Madame Gratton, allez-y.

Mme France Gratton: Je dirais la même chose. Nous n'utilisons aucun outil pour observer ou surveiller notre personnel. C'est à peu près la même situation…

M. Damien Kurek: Encore une fois, je vous demanderais de relayer la question à vos supérieurs et de veiller à ce que ces réponses parviennent au Comité.

Monsieur McCrorie, je suis curieux, parce qu'on a parlé d'enquêtes. Au cours de la pandémie de COVID-19, il y a eu des conversations au sujet d'ArriveCAN et d'une foule d'autres cas connexes, et au sujet des personnes qui ont traversé la frontière pendant la pandémie alors qu'il y avait des restrictions. A-t-on déjà ouvert ce genre d'enquête en raison de l'application des mesures liée à la COVID-19?

M. Aaron McCrorie: Ce que nous faisons, c'est appliquer les dispositions pénales des lois frontalières, par exemple, en ce qui concerne les personnes qui en ont conseillé d'autres sur la façon d'obtenir frauduleusement des documents d'immigration, un visa d'étudiant ou un visa de travail, ou encore les personnes qui ont participé à la contrebande d'armes à feu ou de pièces. Une affaire a été portée devant les tribunaux l'an dernier, en avril 2023, et l'individu a écopé d'une peine d'environ 12 ans pour avoir fabriqué des armes fantômes et fait entrer des pièces en contrebande. Ce sont là les cas où nous avons utilisé ces outils pour obtenir des preuves, comme l'ont fait nos collègues de la GRC, afin de mener à bien les poursuites intentées contre ceux qui avaient enfreint les lois pénales.

M. Damien Kurek: Cela se limite de toute évidence aux infractions au Code criminel, donc pour quelqu'un qui…

● (1255)

M. Aaron McCrorie: Il s'agissait d'une loi frontalière, alors ils étaient accusés, par exemple, en vertu de notre propre Loi sur les douanes.

M. Damien Kurek: D'accord. Vous me dites — et n'hésitez pas à apporter des précisions — qu'en ce qui concerne l'application des mesures liée à la COVID-19, cette technologie n'aurait pas été utilisée.

M. Aaron McCrorie: Je ne suis au courant d'aucun cas et je ne vois aucun cas où nous l'utiliserions dans le contexte de la COVID. Je le répète, les seuls cas où nous l'utiliserions seraient avec une autorisation judiciaire préalable.

M. Damien Kurek: Je comprends.

Madame Gratton, il ne me reste que quelques secondes. Il y a, par exemple, des sites d'injection supervisée dans nos prisons, mais il y a une sorte de « loi du silence » lorsqu'un détenu se rend dans un site d'injection supervisée pour consommer des produits de contrebande. Très souvent, il doit se les procurer quelque part. J'essaie simplement de résoudre la quadrature du cercle en ce qui concerne l'application de la loi et tout le reste lorsqu'il s'agit de la dynamique dans une prison, où il y a des activités criminelles présumées, mais où on « ferme les yeux » sur certains aspects.

Pourriez-vous nous dire brièvement… comment puis-je concilier cela?

Le président: Il faut toujours être bref.

[*Français*]

Madame Gratton, je suis désolé, mais vous devrez répondre rapidement.

[*Traduction*]

Mme France Gratton: Rapidement, en ce qui concerne les sites de prévention des surdoses, le problème n'est pas qu'on ferme les yeux. Il s'agit d'un programme de réduction des méfaits, qui vise essentiellement à offrir un soutien aux détenus aux prises avec des problèmes de toxicomanie. La différence, c'est que, lorsqu'il est question de trafic, nous appliquons la loi. C'est là que nous prenons des mesures disciplinaires pour empêcher le trafic et la contrebande. Ce sont deux approches différentes.

Le président: Merci, madame Gratton.

Merci, monsieur Kurek.

Monsieur Housefather, vous êtes le suivant. Vous avez un temps de parole illimité…

Des voix: Ha, ha!

Le président: … puisque vous êtes un nouvel invité au Comité.

M. Anthony Housefather (Mont-Royal, Lib.): Merci, monsieur le président. C'était très flatteur.

Pour gagner du temps, je voudrais régler certaines questions. Je vais poser mes questions à la GRC, et je vais demander aux autres ministères de confirmer si les réponses que la GRC me donne sont les mêmes que celles qu'ils auraient données.

Tout d'abord, la question est celle de la confusion entre les logiciels espions, les maliciels et la technologie d'extraction de données. Les logiciels espions et les maliciels sont des éléments nuisibles que les gens installent sur votre téléphone afin d'extraire continuellement des données et de les utiliser à des fins malveillantes.

En ce qui concerne la GRC, pouvons-nous supposer qu'aucun logiciel espion ou maliciel n'est utilisé et que seuls des outils d'extraction de données sont utilisés?

[*Français*]

M. Nicolas Gagné: Non, aucunement.

[*Traduction*]

M. Anthony Housefather: Est-ce la même chose?

[*Français*]

M. Aaron McCrorie: C'est la même chose de notre côté.

[*Traduction*]

M. Anthony Housefather: C'est la même chose aussi. Cela voudrait dire que, lorsque vous voulez extraire des données, vous prenez l'appareil, vous extrayez les données et vous ne laissez rien sur le téléphone ou l'outil à partir duquel vous les avez extraites. Est-ce exact? Vous le redonnez sans y laisser aucun logiciel qui continuerait d'extraire des données.

M. Nicolas Gagné: C'est exact.

M. Anthony Housefather: Est-ce la même chose?

M. Aaron McCrorie: Je dirais que cela varie selon les circonstances. N'oubliez pas qu'il s'agit de preuves dans le cadre d'une procédure pénale, nous les conserverons donc comme éléments de preuve et, pour une partie d'entre elles, nous utiliserons les outils pour extraire les données et les traduire dans un format qui peut être utilisé dans le cadre d'une procédure judiciaire…

M. Anthony Housefather: Non, je comprends, mais vous ne redonnez pas à quelqu'un un téléphone contenant un outil qui continue d'extraire ses données à son insu.

M. Aaron McCrorie: Non.

M. Anthony Housefather: Est-ce la même chose, madame Gratton?

Mme France Gratton: Nous ne remettons pas les téléphones parce que ce sont des objets interdits, donc nous les gardons.

M. Anthony Housefather: Je comprends.

Est-il vrai, dans le cas de la GRC, que, pour extraire des données, vous utilisez une technologie conforme à celles d'organisations du genre de la GRC aux États-Unis, au Royaume-Uni et dans d'autres pays semblables?

M. Nicolas Gagné: Je dirais que oui.

M. Anthony Housefather: Diriez-vous que les politiques que vous utilisez sont également conformes, compte tenu de la différence dans notre droit pénal?

M. Nicolas Gagné: Je dirais que c'est un peu semblable, oui.

M. Anthony Housefather: Merci.

Diriez-vous la même chose pour l'ASFC?

M. Aaron McCrorie: À ma connaissance, oui, et je dirais que c'est aussi très semblable à la façon dont nos collègues l'utilisent.

[*Français*]

M. Anthony Housefather: Est-ce la même chose du côté du Service correctionnel du Canada?

[*Traduction*]

Mme France Gratton: Je dirais qu'il y a des différences selon la juridiction, mais cela peut être semblable, oui.

M. Anthony Housefather: Parfait.

J'aimerais maintenant établir que ces outils que vous avez ne peuvent pas être utilisés à distance. Pour utiliser la technologie d'extraction de données, il faut avoir l'appareil en main. Est-ce bien cela? Vous ne pouvez pas extraire subrepticement des données d'un appareil que vous n'avez pas en votre possession alors que l'utilisateur ne sait pas que vous le faites. Est-ce exact?

M. Nicolas Gagné: En ce qui concerne la technologie en question, les Cellebrites ou les Magnet Forensics de ce monde, oui. Nous avons besoin d'avoir l'appareil en notre possession pour extraire les données.

M. Anthony Housefather: Un Canadien se trouvant à Winnipeg peut être certain que la GRC n'est pas en train d'extraire des données de son appareil puisqu'elle ne l'a jamais eu en sa possession.

M. Nicolas Gagné: À l'aide de ces outils, c'est exact, oui.

● (1300)

M. Anthony Housefather: Nous ne parlerons pas des autres outils dont vous disposez pour l'instant, parce que ce serait une autre étude.

ASFC...?

M. Aaron McCrorie: Oui, nous utilisons la technologie dans nos laboratoires de criminalistique numérique, nos installations sécurisées. Il est en notre possession physique, encore une fois, obtenu au moyen d'un mandat de perquisition.

[*Français*]

M. Anthony Housefather: Parfait.

Est-ce la même chose de votre côté, madame Gratton?

[*Traduction*]

Mme France Gratton: C'est exactement la même chose, oui.

M. Anthony Housefather: J'ai une dernière question.

Vous avez mentionné la seule fois où vous l'avez utilisé pour un employé. D'après ce que je comprends, donc, si vous l'utilisez pour un employé, c'est en raison d'activités criminelles potentielles de cet employé. Ce n'est pas parce qu'il enfreint les protocoles de la GRC en matière de ressources humaines qui ne relèvent pas du droit pénal, sauf dans ce cas particulier. Est-ce exact?

S.-comm. Bryan Larkin: En fait, il ne s'agissait pas d'une enquête criminelle. C'était une affaire interne. C'était une enquête de sécurité ministérielle, et l'employé y avait consenti. Il a consenti à ce qu'on utilise l'outil sur son appareil.

M. Anthony Housefather: Je présume qu'il l'a fait pour se disculper. Il estimait que l'information qui s'y trouvait lui permettrait de se disculper.

Ce que je demande donc, c'est que, comme pour toute autre activité criminelle potentielle qui existe, je suppose, si l'activité criminelle concernait un employé de la GRC, alors elle relèverait des dispositions relatives au mandat et des autres dispositions que vous appliquez pour n'importe qui d'autre. Vous ne traiteriez pas avec l'employé pour des affaires qui le concernent, sauf, comme vous l'avez mentionné, par consentement.

S.-comm. Bryan Larkin: Dans le cas d'une enquête criminelle, nous demanderions une autorisation judiciaire, bien que la Loi sur la GRC nous autoriserait à utiliser la technologie, à utiliser les outils, mais nous le ferions au cas par cas. L'équipe du surintendant Gagné se penche sur l'établissement d'un seuil et d'un cadre, et des consultations ont lieu avec notre bureau de la responsabilité professionnelle et les enquêteurs chargés de l'enquête sur le code de conduite.

M. Anthony Housefather: Cela se fait en toute connaissance de cause. Les employés adhèrent déjà aux politiques dont ils disposent. Ils le savent.

S.-comm. Bryan Larkin: C'est exact.

M. Anthony Housefather: Est-ce la même chose?

Mme France Gratton: Oui.

M. Anthony Housefather: Merci beaucoup, monsieur le président.

Le président: Merci, monsieur Housefather.

Cela met fin à la deuxième heure de la séance.

Monsieur Gagné, monsieur Larkin, monsieur McCrorie, madame Gratton et monsieur Matson, merci beaucoup d'avoir comparu devant le Comité aujourd'hui.

Pour la gouverne des membres du Comité, ce jeudi, nous prévoyons entendre des représentants d'Environnement et Changement climatique, de Pêches et Océans, du CRTC et de l'Agence du revenu du Canada. Nous suivons vos conseils. Nous essayons de savoir qui doit comparaître devant le Comité le plus tôt possible afin de poursuivre cette étude.

Je remercie la greffière, les analystes et les techniciens pour la réunion d'aujourd'hui.

La séance est levée.