



CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

44^e LÉGISLATURE, 1^{re} SESSION

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

TÉMOIGNAGES

NUMÉRO 100

Le jeudi 1^{er} 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 jeudi 1er février 2024

• (1100)

[Traduction]

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

[Français]

Bienvenue à la 100^e 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) du Règlement et à la motion adoptée par le Comité le mercredi 6 décembre 2023, le Comité entreprend aujourd'hui son étude de l'utilisation par le gouvernement fédéral d'outils technologiques permettant d'extraire des données sur les appareils mobiles et les ordinateurs.

[Traduction]

La réunion d'aujourd'hui se déroule sous forme hybride, conformément au Règlement de la Chambre. Les députés participent en personne dans la salle et à distance au moyen de l'application Zoom.

J'aimerais rappeler à tous les députés de ne pas mettre les oreillettes près des microphones, car cela provoque un effet Larsen qui risque de causer des blessures à nos interprètes.

J'aimerais maintenant souhaiter la bienvenue à nos témoins d'aujourd'hui. Nous accueillons des représentants des Commissariats à l'information et à la protection de la vie privée au Canada: le commissaire à la protection de la vie privée du Canada, M. Philippe Dufresne; et la directrice exécutive, Direction des politiques, de la recherche et des affaires parlementaires, Mme Lara Ives. Nous vous souhaitons la bienvenue.

Avant de donner la parole à M. Dufresne, je tenais à vous aviser qu'il m'a demandé s'il pouvait disposer de 10 minutes pour sa déclaration préliminaire. J'ai accepté sa demande.

J'aimerais également vous dire que puisque nous n'accueillons que ces deux témoins pour les deux prochaines heures, nous remettrons le chronomètre à zéro à la fin de cette heure-ci et donnerons plus de temps à M. Villemure et M. Green, s'ils en ont besoin.

Encore une fois, je vous souhaite la bienvenue, monsieur Dufresne. Comme toujours, nous sommes heureux de vous accueillir au Comité.

Vous pouvez commencer votre déclaration liminaire.

M. Philippe Dufresne (commissaire à la protection de la vie privée du Canada, Commissariats à l'information et à la protection de la vie privée au Canada): Monsieur le président et mesdames et messieurs les membres du Comité, je vous remercie de m'avoir invité à contribuer à votre étude sur l'utilisation par le

gouvernement fédéral d'outils technologiques permettant d'extraire des données sur des appareils mobiles et ordinateurs.

L'automne dernier, Radio-Canada/CBC a rapporté que 13 institutions fédérales avaient fait l'acquisition de tels outils. Les reportages dans les médias ont soulevé des questions sur les motifs de leur utilisation et sur la mesure dans laquelle les organisations concernées respectaient leurs obligations en matière de protection de la vie privée lorsqu'elles en faisaient usage.

Dans les premiers reportages, ces outils étaient qualifiés d'outils de surveillance secrète ou de « logiciels espions ». Depuis, il a été précisé qu'il ne s'agit pas de logiciels espions, mais plutôt d'outils d'investigation informatique. Les outils d'investigation informatique servent à extraire et à examiner un grand nombre de fichiers stockés sur des ordinateurs portables, des disques durs ou des appareils mobiles. On les utilise généralement dans le cadre d'enquêtes ou d'analyses techniques, et le propriétaire de l'appareil en est souvent informé.

[Français]

On peut les utiliser pour analyser les métadonnées d'un fichier ou pour créer une chronologie des événements, par exemple pour établir le moment où un compte a été utilisé, des sites Web ont été consultés ou un système d'exploitation a été modifié. On peut aussi les utiliser pour récupérer des données supprimées, pour s'assurer que les données ont été correctement effacées d'un appareil avant qu'il ne soit jeté ou utilisé à d'autres fins. Ils constituent donc des outils d'enquête utiles qui peuvent contribuer à préserver l'intégrité d'une chaîne de preuves.

Les outils d'investigation informatique se distinguent des logiciels espions par le fait que ces derniers sont généralement installés à distance sur l'appareil d'une personne à l'insu de celle-ci. Les logiciels espions peuvent ensuite recueillir secrètement les renseignements personnels, comme les touches utilisées sur le clavier d'ordinateur et l'historique de navigation sur le Web. On peut citer, à titre d'exemple, les outils d'enquête sur appareil qui sont utilisés par les organismes d'application de la loi pour obtenir des données secrètement et à distance à partir d'appareils ciblés. Il est important de noter que, dans le contexte de l'application de la loi, une autorisation judiciaire est requise avant de pouvoir utiliser ces outils.

• (1105)

[Traduction]

En août 2022, j'ai comparu devant le présent Comité dans le cadre de son étude au sujet de l'utilisation des outils d'enquête sur appareil par la Gendarmerie royale du Canada, la GRC. Vous vous souviendrez que dans cette affaire, la GRC avait informé la Chambre qu'elle utilisait ce type d'outils depuis quelques années pour obtenir des données secrètement et à distance à partir d'appareils ciblés, mais qu'elle n'avait pas réalisé d'évaluation des facteurs relatifs à la vie privée, ou EFVP, et qu'elle n'avait pas informé le Commissariat.

Pendant ma comparution à cette occasion, j'ai fait remarquer que les EFVP étaient obligatoires selon les politiques du Conseil du Trésor, mais qu'elles n'étaient pas une obligation prévue par les lois sur la protection des renseignements personnels. J'ai alors recommandé que la réalisation de telles évaluations devienne une obligation juridique contraignante pour le gouvernement au titre de la Loi sur la protection des renseignements personnels.

[Français]

Dans son rapport de novembre 2022, le Comité a souscrit à cette recommandation et a également demandé que le préambule de la Loi sur la protection des renseignements personnels soit modifié afin de préciser que le droit à la vie privée est un droit fondamental et que la Loi soit modifiée pour inclure le concept de protection de la vie privée dès la conception et des obligations de transparence explicite pour les institutions gouvernementales. J'ai accueilli favorablement ces recommandations et je les ai soutenues. Le Comité souhaitera peut-être les réitérer, car elles demeurent en suspens et sont toujours pertinentes.

[Traduction]

Comme la technologie change de plus en plus la manière dont les renseignements personnels sont recueillis, utilisés et communiqués, il demeure important que les institutions gouvernementales portent une attention particulière aux répercussions de leurs activités sur la vie privée et les évaluent soigneusement afin d'établir si une EFVP est nécessaire et à quel moment elle doit être réalisée.

Ma vision de la protection de la vie privée en est une où le droit à la vie privée est considéré comme un droit fondamental, où la protection de la vie privée est un moyen de favoriser l'intérêt public et d'appuyer l'innovation, et où les Canadiennes et les Canadiens ont confiance dans le fait que leurs institutions protègent leurs renseignements personnels. Réaliser une EFVP et consulter le Commissariat avant d'utiliser une nouvelle technologie ayant une incidence sur la vie privée permettraient de renforcer la protection de la vie privée, de soutenir l'intérêt public et de susciter la confiance. C'est pourquoi les institutions gouvernementales devraient être tenues par la loi de procéder ainsi; il devrait s'agir d'une obligation au titre de la Loi sur la protection des renseignements personnels.

[Français]

À l'heure actuelle, conformément à la Directive sur l'évaluation des facteurs relatifs à la vie privée du Secrétariat du Conseil du Trésor, les institutions doivent effectuer de telles évaluations lorsque les renseignements personnels peuvent être utilisés dans le cadre d'un processus décisionnel touchant directement un individu; lorsque des modifications importantes sont apportées à des programmes ou à des activités déjà en place dans lesquels des renseignements personnels peuvent être utilisés à des fins administra-

tives; lorsque la sous-traitance ou le transfert d'un programme ou d'une activité à un autre ordre du gouvernement ou au secteur privé constitue une modification importante à ce programme ou à cette activité; ou lorsque des activités ou des programmes nouveaux ou ayant subi des modifications importantes auront une incidence sur la vie privée en général, même si aucune décision n'est prise concernant les individus.

[Traduction]

Lors de nos entretiens avec les institutions fédérales dans le cadre de consultations, nous présentons les EFVP en tant que processus efficace de gestion des risques. Ces évaluations permettent de cerner et d'atténuer les risques qui pèsent sur la vie privée, idéalement dès le départ, dans l'ensemble des programmes et des services à l'intérieur desquels des renseignements personnels sont recueillis et utilisés. Cela dit, l'utilisation d'un nouvel outil n'entraîne pas toujours le besoin de réaliser une EFVP. Tout dépendra de la manière dont l'outil sera utilisé et de l'usage qui sera fait des renseignements qu'il permettra de recueillir.

Le Commissariat a utilisé des outils d'investigation informatique, par exemple, dans le cadre d'enquêtes sur certaines allégations d'atteinte à la vie privée afin d'établir la nature, l'envergure et la portée d'un incident, y compris ce qui a mené à l'atteinte et quels types de renseignements personnels ont été compromis, s'il y a lieu.

[Français]

Les outils d'investigation informatique peuvent cependant être utilisés d'une manière qui soulève des risques importants sur le plan de la vie privée et qui mériteraient la tenue d'une évaluation complète des facteurs relatifs à la vie privée.

Par exemple, on peut les utiliser lors d'une enquête interne sur la conduite d'un employé au terme de laquelle une décision qui aura une influence directe sur cette personne sera prise, ou s'en servir dans le cadre d'une enquête sur des allégations d'activités criminelles ou illégales.

Dans ces types d'utilisation, il faudrait mener une évaluation des facteurs relatifs à la vie privée. Celle-ci porterait non seulement sur l'outil précis utilisé pour recueillir les renseignements personnels, mais également sur le programme général dans le cadre duquel on a recours à l'outil.

• (1110)

[Traduction]

Toutes les institutions fédérales sont tenues d'examiner leurs programmes et leurs activités en conséquence. Lorsque des outils d'investigation informatique sont utilisés dans le contexte de la surveillance des employés, les institutions doivent prendre des mesures pour garantir le respect du droit fondamental à la vie privée et pour favoriser la transparence et la confiance en milieu de travail. Il devrait y avoir des règles claires qui régissent quand et comment les technologies de surveillance devraient être utilisées. Le Commissariat a mis à jour son document d'orientation sur la protection des renseignements personnels au travail en mai 2023, et mes collègues provinciaux et territoriaux et moi-même avons publié une résolution conjointe sur la protection de la vie privée des employés sur les lieux de travail en octobre 2023.

Dans le cas présent, à la suite des reportages de CBC/Radio-Canada concernant l'utilisation des outils d'investigation informatique au gouvernement fédéral, le Commissariat a effectué un suivi auprès des institutions qui y étaient mentionnées et de celles figurant dans la motion déposée par ce comité afin de procéder à la présente étude.

[Français]

Pour résumer ce que nous avons appris, trois organismes ont indiqué avoir réalisé et présenté une évaluation des facteurs relatifs à la vie privée, ou EFVP, sur le programme pertinent; un organisme a indiqué qu'il avait acheté l'outil, mais qu'il ne l'avait jamais utilisé; un organisme a indiqué qu'une EFVP n'était pas requise; et les huit autres organismes ont indiqué qu'ils avaient commencé à réaliser une nouvelle EFVP ou qu'ils étudieraient la possibilité de le faire ou de mettre à jour une EFVP existante à la lumière de leur utilisation des outils.

[Traduction]

Nous continuerons de faire un suivi auprès des institutions afin d'insister sur la nécessité de réaliser des EFVP dans les cas où elles sont requises selon les politiques du Conseil du Trésor. Mais sans une obligation au titre de la Loi sur la protection des renseignements personnels, il y a des limites à ce que nous pouvons faire pour assurer la conformité. Les EFVP, dans les cas appropriés, sont avantageuses pour la vie privée, avantageuses pour l'intérêt public et elles suscitent la confiance. Dans un monde de plus en plus axé sur le numérique, elles devraient être obligatoires au titre de la loi en matière de protection des renseignements personnels.

Je serai heureux de répondre à vos questions.

Le président: Je vous remercie, monsieur Dufresne. Je vous remercie d'avoir plus que respecté le temps imparti.

Nous allons commencer la première série de questions.

Monsieur Barrett, vous avez six minutes. La parole est à vous.

M. Michael Barrett (Leeds—Grenville—Thousand Islands et Rideau Lakes, PCC): Bonjour.

Les Canadiens ont-ils droit à la vie privée?

M. Philippe Dufresne: Absolument.

M. Michael Barrett: Pourriez-vous nous donner des exemples de logiciels que le gouvernement du Canada a utilisés pour espionner les Canadiens?

M. Philippe Dufresne: Comme je l'ai mentionné, ces outils d'investigation informatique permettent d'extraire des données supprimées ou non supprimées sur des appareils et sur des ordinateurs. Ils permettent d'obtenir des renseignements, y compris des renseignements personnels. C'est la raison pour laquelle, lorsqu'ils visent des particuliers, comme des employés, ou, lorsqu'ils sont utilisés d'une manière qui soulève des risques sur le plan de la vie privée, une évaluation des facteurs relatifs à la vie privée mérite d'être réalisée.

M. Michael Barrett: Le logiciel que le gouvernement utilise lui permet-il de déverrouiller un téléphone intelligent?

M. Philippe Dufresne: À ma connaissance, cela est possible dans certains cas.

M. Michael Barrett: Ce logiciel peut-il accéder au contenu des ordinateurs portables ou des iPad qui sont protégés par un mot de passe?

M. Philippe Dufresne: À ma connaissance, oui. Vous devriez aussi poser ces questions aux représentants des institutions.

M. Michael Barrett: Pourriez-vous nous donner une idée de la gamme de renseignements personnels auxquels on pourrait avoir accès?

M. Philippe Dufresne: Il peut s'agir de données qui sont stockées sur l'appareil: des renseignements, des fichiers, des données qui portent sur l'utilisation de l'appareil, notamment si un élément a été supprimé ou non, ou si un site Web a été consulté. Ces outils peuvent faire une foule de choses. C'est pourquoi, dans les situations où ils sont utilisés pour cibler des particuliers ou mener des enquêtes à leur endroit, nous nous attendons à ce que des évaluations des facteurs relatifs à la vie privée soient effectuées pour cerner et atténuer les risques qui pèsent sur la vie privée.

M. Michael Barrett: Ces outils donnent accès aux photos, aux messages textes, aux messages personnels et à l'historique de navigation.

M. Philippe Dufresne: C'est juste. Sauf erreur, c'est bien le cas.

M. Michael Barrett: Les outils que le gouvernement utilise lui permettent-ils de suivre les déplacements des Canadiens?

M. Philippe Dufresne: Suivre les déplacements des Canadiens...?

M. Michael Barrett: Je parle de l'endroit où ils se trouvent en temps réel, ou de l'historique des endroits où ils se trouvaient.

M. Philippe Dufresne: D'habitude, ces outils ne seront pas utilisés à distance si l'enquêteur n'a pas l'appareil en sa possession. L'enquêteur doit avoir l'appareil en sa possession. Ces outils se distinguent donc des outils d'enquête sur les appareils, ou logiciels espions, qui permettent d'accéder à un appareil à l'insu du propriétaire et sans que l'enquêteur soit en possession de l'appareil.

• (1115)

M. Michael Barrett: Disons les choses clairement: le logiciel espion, une fois que le gouvernement a l'appareil en sa possession, peut recueillir des renseignements, même des renseignements qui ont été supprimés, mais il est aussi possible d'installer le logiciel à distance, secrètement, pour ensuite surveiller l'emplacement d'un appareil et l'usage qu'on en fait.

M. Philippe Dufresne: Si nous parlons des outils d'investigation informatique, et c'est ce dont nous parlons dans ce contexte, ils peuvent être utilisés pour recueillir des preuves numériques, récupérer des fichiers supprimés, analyser des dossiers d'intérêt et créer une chronologie des événements. Ils exigent presque toujours un accès physique à l'appareil.

Ces outils se distinguent des logiciels espions, ou outils d'enquêtes sur les appareils, avec lesquels ces tâches peuvent être accomplies à distance, sans que le propriétaire de l'appareil en soit informé. Il s'agit d'outils différents, mais qui procurent néanmoins des capacités importantes.

M. Michael Barrett: Combien de ministères fédéraux ont cette capacité?

M. Philippe Dufresne: Je ne suis pas au fait de tous les ministères qui ont ces outils, mais, d'après le reportage, il y en aurait treize. Nous avons fait un suivi auprès d'eux et avons obtenu des renseignements.

M. Michael Barrett: Comment pouvez-vous — ou le Commissariat — savoir si un ministère a l'intention d'utiliser ces outils ou s'il a ces outils? La seule façon de le savoir est-elle de demander à chaque ministère de réaliser une évaluation des facteurs relatifs à la vie privée à l'avance?

M. Philippe Dufresne: Dans de nombreux cas, c'est ce qu'il faut faire, car nous ne savons pas ce que fait un ministère s'il ne nous en informe pas ou s'il ne nous consulte pas. La politique du Conseil du Trésor exige la réalisation de ces évaluations, mais il ne s'agit pas d'une obligation légale. Je recommande donc que la réalisation de telles évaluations devienne une obligation légale. Il est toujours préférable, dans l'intérêt du ministère, des Canadiens et du Commissariat, que le ministère prenne les devants et communique avec nous. Cela nous donne l'occasion de faire valoir notre point de vue et de signaler les risques, en plus de permettre aux Canadiens d'être au fait de ce qui se passe.

Certains de ces outils peuvent être utilisés judicieusement — il y a de bonnes raisons de le faire —, mais il est nécessaire de réaliser cette évaluation relative à la vie privée. Nous en avons besoin.

M. Michael Barrett: L'approche est-elle différente pour d'autres outils que les ministères utilisent, comme l'application Alerte COVID? Le gouvernement a déclaré qu'il ne l'utiliserait pas pour suivre les déplacements des Canadiens, mais c'est exactement ce qu'il a fait. J'ai l'impression que l'attitude du gouvernement à l'égard du droit à la vie privée des Canadiens fait défaut.

M. Philippe Dufresne: Je pense que nous devons préciser les règles dans ce domaine, de manière générale. De plus en plus de technologies sont utilisées et elles offrent de plus grandes possibilités. Cela stimule l'innovation et crée des occasions, mais nous devons avoir le réflexe d'inclure le concept de protection de la vie privée dès la conception, au début du processus. Souvent, on développera un outil et on l'utilisera, pour ne réaliser l'évaluation des facteurs relatifs à la vie privée qu'après coup, ou n'inclure ces éléments que plus tard.

Il sera toujours plus rentable et plus prudent d'intégrer la protection de la vie privée dès le départ. Alors que l'intelligence artificielle et la technologie sont de plus en plus performantes, cette pratique est plus importante que jamais. Voilà pourquoi nous recommandons que la réalisation des EFVP devienne obligatoire.

Le président: Je vous remercie, messieurs Barrett et Dufresne.

Madame Khalid, vous avez six minutes. La parole est à vous.

Mme Iqra Khalid (Mississauga—Erin Mills, Lib.): Merci beaucoup, monsieur le président.

Je remercie nos témoins de leur présence aujourd'hui.

J'aimerais obtenir quelques précisions à propos de deux ou trois points que M. Barrett a soulevés. Ces outils d'investigation informatique visent plus particulièrement les employés de ces ministères, n'est-ce pas?

M. Philippe Dufresne: Oui, dans les cas où ils sont utilisés pour des enquêtes administratives. Cependant, ils peuvent être utilisés à d'autres fins. Certains ministères les utilisent pour d'autres types d'enquêtes, mais s'il s'agit d'enquêtes administratives, les outils ne viseront que les employés du ministère.

Mme Iqra Khalid: Je veux m'assurer de bien comprendre. Ces ministères mènent-ils des enquêtes ou surveillent-ils tous les Canadiens et tous leurs appareils, ou parlons-nous plus particulièrement

des appareils que le gouvernement fournit aux employés du gouvernement dans le cadre de leur travail au sein de notre gouvernement?

M. Philippe Dufresne: Cela dépend. Certains ministères utiliseront ces outils pour mener des enquêtes sur les infractions à la loi commises par les Canadiens. D'autres les utiliseront pour faire enquête sur leurs employés. Dans le cas des trois ministères qui les ont utilisés dans le cadre d'enquêtes administratives, ce n'était pas tous les Canadiens qui étaient visés, mais seulement leurs employés.

Toutefois, les employés ont aussi des droits en matière de protection de la vie privée. Il existe des obligations en matière de protection de la vie privée. Nous avons publié un document d'orientation à ce sujet. Les ministères doivent veiller à ce que l'usage de l'outil soit lié aux objectifs d'un projet. Ils doivent faire preuve de transparence, s'adapter aux différentes situations, et réaliser une évaluation des facteurs relatifs à la vie privée, au besoin.

• (1120)

Mme Iqra Khalid: Je vois.

Ces outils d'investigation informatique sont-ils installés sur les appareils des employés, ceux qui sont fournis par les ministères, ou sur leurs appareils personnels?

M. Philippe Dufresne: Je n'ai pas tous les détails à ce sujet. Vous pourriez leur poser ces questions.

En général, il s'agit des outils que l'employeur fournit à l'employé, comme le courriel, l'ordinateur portable, etc. Cela dit, il existe certaines attentes en matière de protection de la vie privée en ce qui concerne l'utilisation de ces outils, mais tout dépend du contexte. Les employeurs ont des raisons légitimes d'obtenir certains renseignements. Nous en parlons dans notre document d'orientation et nous sommes clairs à ce sujet. Les ministères doivent évaluer l'outil et évaluer les principes de nécessité et de proportionnalité liés à son utilisation. Ils doivent être transparents à ce sujet pour que les gens soient au fait de ce qui se passe.

Dans notre rapport annuel de l'année dernière, nous avons parlé d'une enquête que nous avons réalisée dans le secteur privé sur une entreprise de camionnage qui surveillait les camionneurs à l'aide d'un dispositif de surveillance. Même lorsque les camionneurs n'étaient pas en service, ils étaient filmés et enregistrés 24 heures sur 24, sept jours sur sept. Nous avons estimé que cette pratique était exagérée. Il était légitime d'exercer cette surveillance lorsque les camionneurs conduisaient, pour des raisons de sécurité, mais nous avons déterminé qu'il fallait s'en tenir à ce contexte. Des changements ont été apportés.

C'est le genre de questions que nous posons lors d'une évaluation des facteurs relatifs à la vie privée. Lorsque l'on consulte le Commissariat, surtout en amont, nous avons la chance de poser ce genre de questions. Nous devons prévenir de telles situations, et veiller à ce que les Canadiens ne soient pas inquiets. Ils doivent savoir quel outil est utilisé et à quelle fin, en plus de savoir que le Commissariat à la protection de la vie privée a été consulté et a donné son avis.

Je voudrais que cette façon de faire soit plus répandue, car il arrive souvent que nous apprenions après coup qu'un outil a été utilisé.

Mme Iqra Khalid: Je trouve préoccupant que cette directive n'ait pas été suivie. Est-ce que vous ou le Commissariat avez communiqué avec ces ministères?

Ensuite, vous avez dit qu'il s'agissait d'une politique du Secrétariat du Conseil du Trésor. Quelle est la différence entre une politique et un processus obligatoire en matière de respect de la vie privée dès la conception, en particulier dans ces ministères?

M. Philippe Dufresne: La politique est une règle interne que le gouvernement s'impose à lui-même, ainsi c'est une directive émise, dans ce cas, par le Conseil du Trésor. Elle énonce ce que l'on attend du ministère. C'est sûrement important, mais cela n'a pas la même force juridique contraignante et cela ne me permet certainement pas d'effectuer une enquête de la même façon qu'avec la Loi sur la protection des renseignements personnels. C'est pourquoi je recommanderais, et le bureau a recommandé, d'en faire une obligation légale. Je l'ai également recommandé pour le secteur privé, tout particulièrement en ce qui concerne l'intelligence artificielle, parce que je compare cela aux vérifications qu'on fait avant le départ dans les avions. C'est quelque chose qui réconforte et rassure lorsque nous utilisons des outils puissants.

Dans un cas comme celui-là, nous avons communiqué avec les ministères. Nous les consultons régulièrement et nous avons une équipe consultative gouvernementale toujours prête à entendre les conseils des ministères. Encore une fois, ce que l'on entend parfois c'est : « D'accord. Nous allons maintenant faire une évaluation des facteurs relatifs à la vie privée (EFVP). Nous allons l'actualiser et nous aurons un programme. » Parfois, on nous dit que c'est autorisé en vertu des autorités juridiques du programme ou bien qu'ils le font par le biais d'un mandat. Il faut rappeler à ces ministères que, même s'ils le font sous le coup d'un mandat ou d'une autorité juridique appropriée, l'évaluation des facteurs relatifs à la vie privée est une question distincte. Il vous faudra encore la faire si l'utilisation légale que vous faites de cet outil a une incidence sur la vie privée des Canadiens.

Il s'agit d'une étape supplémentaire et, si c'était une obligation légale, je crois qu'on verrait plus de conformité en amont que dans des situations comme celles-ci, où les gens découvrent parfois l'importance de ces outils par le biais de rapports importants dans les médias. Encore une fois, il est tout à fait possible que ces outils soient adaptés à leurs objectifs. Ils sont différents des logiciels espions. Ils sont différents des outils d'enquête sur l'appareil. Même les outils d'enquête sur l'appareil peuvent être acceptables dans certains cas, mais le fait d'avoir cette discipline et de savoir que ces EFVP sont effectuées renforce la confiance que les Canadiens peuvent avoir en se disant « D'accord, je n'ai pas besoin de regarder par-dessus mon épaule en permanence. Les institutions elles-mêmes disposent de ces outils et ont ces réflexes ».

Mme Iqra Khalid: Pouvez-vous souligner la différence entre les logiciels espions et les outils d'enquête sur l'appareil, comme vous venez de le mentionner?

M. Philippe Dufresne: Généralement, quand nous parlons de logiciels espions, nous parlons de ce type d'outils qui accèdent secrètement aux téléphones, qui récupèrent des données, qui activent des caméras ou des enregistreurs. C'est la catégorie générale de logiciels espions auxquels nous faisons référence pour les utilisations illégales ou non autorisées. Lorsque nous parlons d'outils d'enquête sur l'appareil, nous parlons de ce type d'outils qui sont utilisés par les autorités policières. Ce sont des outils semblables, mais lorsqu'ils sont utilisés par les autorités policières, c'est avec une autorisation légale ou un mandat judiciaire, ils sont donc légaux et appropriés. Il reste que même les autorités policières doivent effectuer une évaluation des facteurs relatifs à la vie privée avant d'utiliser ces outils.

• (1125)

Mme Iqra Khalid: J'ai une dernière question, monsieur le président. Elle est très courte.

Le président: Cela fait six minutes et 38 secondes que vous parlez.

Je vais passer la parole à M. Villemure, vous aurez une autre occasion, lors d'un tour suivant.

[Français]

Monsieur Villemure, vous avez la parole pour six minutes.

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

Monsieur Dufresne, bienvenue au Comité encore une fois. Nous sommes toujours heureux de vous revoir.

Avez-vous été surpris quand vous avez entendu la nouvelle que 13 ministères et organismes utilisaient ce genre d'outils?

M. Philippe Dufresne: Ce que j'aurais aimé, dans une situation comme celle-ci, c'est que mon bureau ait été consulté au préalable dans les 13 cas et que nous ayons toute l'information nécessaire, de telle sorte que nous puissions, en réponse aux médias, leur confirmer ce qui est arrivé, leur dire que nous avons été avisés, que nous avons donné des avis, qu'une évaluation a été faite et que cela ne nous pose aucun problème ou le contraire, puis présenter les recommandations que nous avons données.

La surprise, c'est plutôt le fait que nous ayons finalement à faire un suivi auprès des ministères pour savoir ce qu'il en est.

M. René Villemure: La surprise, c'est donc d'apprendre que les gens n'ont pas nécessairement le réflexe de consulter le commissaire dans ce genre de situation.

Est-ce que les ministères et organismes comprennent bien la Loi sur la protection des renseignements personnels ou leurs obligations en matière de protection de la vie privée?

M. Philippe Dufresne: Je pense qu'il y a toutes sortes de défis, que ce soit sur le plan des ressources ou à l'égard de la pression qui s'exerce sur les ministères. Ils sont mieux placés que moi pour en parler.

La difficulté est liée au fait que les évaluations des facteurs relatifs à la vie privée sont obligatoires aux termes de la Directive du Conseil du Trésor, mais ne le sont pas aux termes de la Loi. La Directive établit des distinctions, par exemple entre un nouveau programme et la mise à jour d'un programme, ou entre l'évaluation d'un programme et l'évaluation de l'outil lui-même.

Étant donné ces distinctions, le ministère peut dire de bonne foi qu'il est d'avis qu'une évaluation n'est pas requise, car la Directive ne l'exige pas. Pourtant, peut-être que cela devrait être requis. Avec la technologie qui devient de plus en plus puissante, il pourrait devenir encore plus important de rassurer les Canadiennes et les Canadiens en leur disant qu'on fait tout cela d'une façon encore plus proactive. Il serait donc préférable que ce soit une obligation juridique.

D'ailleurs, ce n'est pas une question qui concerne seulement le Canada, évidemment. Mes collègues internationaux, à la conférence de l'Assemblée mondiale pour la protection de la vie privée, ont adopté une résolution sur l'intelligence artificielle dans le domaine de l'emploi. Elle appelle les gouvernements et les parlementaires à prendre conscience de la nécessité de baliser cela. Si on utilise les technologies de l'intelligence artificielle pour recruter des travailleurs et évaluer leur performance, cela peut avoir une incidence sur la vie privée. Alors, il faut être transparent et tenir compte des notions de nécessité et de proportionnalité. Ce sont des questions fondamentales.

M. René Villemure: Dans sa forme actuelle, la Loi sur la protection des renseignements personnels n'oblige pas les ministères et les organismes à être exemplaires en matière de vie privée. Nous en avons déjà discuté.

M. Philippe Dufresne: Cela ne constitue pas pour eux une obligation juridique, qui deviendrait une priorité de premier plan. Ce n'est une obligation que dans le cadre de la Directive.

M. René Villemure: Nous allons tout faire pour que ce soit inclus, soyez-en assuré.

Quand j'ai vu la liste des 13 ministères et organismes, j'ai été surpris de constater tout ce qu'elle couvrait. Il ne s'agissait pas uniquement d'organismes de contrôle comme la GRC, la police ou le Service correctionnel.

Est-ce qu'il s'agit ici de désinvolture, de paresse, de négligence ou d'erreurs? Vous avez parlé d'un manque de ressources. Cependant, en matière de vie privée, surtout si celle-ci est considérée comme un droit fondamental, le manque de ressources n'est pas une réponse acceptable. Ces gens traitent-ils la vie privée d'une manière désinvolte?

M. Philippe Dufresne: Avant de mettre un programme sur pied, ils n'ont pas toujours le réflexe de vérifier si mon bureau en a été informé. Il y a de l'amélioration à apporter de ce côté. On parle ici de ministères qui utilisent cet outil dans un but précis: certains l'utilisent pour des enquêtes internes et d'autres pour des enquêtes dans le cadre de leur mandat.

L'utilisation n'est pas nécessairement inappropriée en soi, mais il faut faire cette évaluation. Or, comme nous l'avons constaté, les gens disent parfois ne pas avoir besoin de faire cette évaluation parce que leur mandat juridique comporte l'autorisation de mener ces activités. Or, mon message aux ministères est que ce n'est pas suffisant. L'évaluation des facteurs relatifs à la vie privée est un sujet distinct qu'il faut traiter de façon plus proactive.

M. René Villemure: Un peu plus tôt, vous avez parlé de proportionnalité. C'est un aspect qui m'inquiète. On peut parfois obtenir le résultat recherché en utilisant une méthode moins intrusive, mais on a remarqué que, dans d'autres domaines, la méthode la plus intrusive était utilisée, non parce qu'elle est intrusive, mais simplement parce qu'elle est plus rapide.

Cette proportionnalité est-elle incluse quelque part, dans une directive, ou serait-il souhaitable qu'elle figure éventuellement dans une loi?

• (1130)

M. Philippe Dufresne: Pour ce qui est du secteur public, je dois dire, là encore, que cette notion de proportionnalité n'est pas incluse dans la Loi sur la protection des renseignements personnels. Nous avons recommandé, et ce comité l'a fait également, que la question de la nécessité et de la proportionnalité y soit incluse. À ce stade,

cela relève plutôt d'une directive du Conseil du Trésor voulant que cette utilisation soit nécessaire pour atteindre l'objectif visé.

En ce moment, la Loi exige que l'utilisation soit liée à un mandat de l'organisme. De notre côté, au Commissariat, nous allons mettre en œuvre cette nécessité et cette proportionnalité en soulevant des questions à ce propos dans le cadre de nos enquêtes. Nous en parlons maintenant, tout comme nous en avons parlé lors des enquêtes portant sur les mesures prises durant la pandémie, notamment. Quand nous abordons ce sujet, cependant, nous devons reconnaître d'entrée de jeu qu'il ne s'agit pas d'une obligation juridique et que, si cette notion n'était pas respectée dans une situation donnée, cela ne constituerait pas une violation de la loi.

On parle ici d'une recommandation très importante. L'approche ressemble beaucoup à la façon dont on procède dans le contexte de la Charte canadienne des droits et libertés pour déterminer s'il y a de la discrimination ou une atteinte aux droits fondamentaux. On vérifie si l'objectif visé est important, si la mesure proposée permet d'atteindre l'objectif, si la méthode employée pour y parvenir est la moins intrusive et, enfin, si cette méthode est proportionnelle.

Vous avez tout à fait raison: on peut être tenté d'utiliser un outil parce qu'on le trouve vraiment très performant et rapide. On peut penser ici à l'intelligence artificielle. Oui, c'est efficace, mais on parle ici d'un droit fondamental.

Cela dit, il n'est pas question de choisir entre l'un ou l'autre. Pour ma part, je suis favorable à la technologie. Au bureau, nous en avons fait une de nos trois priorités stratégiques récemment. Nous voulons utiliser la technologie, mais d'une façon qui protège la vie privée. En ce sens, les outils d'évaluation des facteurs relatifs à la vie privée sont essentiels. Il faut non seulement que ces évaluations soient faites, mais également qu'on voie qu'elles le sont.

Le président: Merci, messieurs Dufresne et Villemure.

[Traduction]

Monsieur Green, vous disposez de six minutes. Allez-y, je vous prie.

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

Vous savez, je repense au travail que nous avons mené sur la GRC et j'espère qu'à l'époque ces ministères étaient peut-être à l'écoute, sachant qu'ils se livraient au même genre d'activités. Ce qui me déçoit c'est qu'il ait fallu autant de temps pour que ça se sache. On parle de 13 ministères. Il y a certainement beaucoup d'autres ministères fédéraux, et certains peuvent ou non le déclarer. Je ne remettrai pas en cause ce que font les autres ministères.

Je remarque que dans le libellé de la Directive sur l'évaluation des facteurs relatifs à la vie privée, au paragraphe 3.3, il est indiqué que la Loi sur la protection des renseignements personnels demande d'« évaluer les incidences que peuvent avoir des programmes ou des activités, nouveaux ou ayant subi des modifications importantes comportant des renseignements personnels, sur la vie privée ». Je crois que vous venez d'y faire référence, monsieur. Puis la ligne suivante dit, « Toutefois, la préparation d'une ÉFVP peut être exigeante en termes de ressources si elle n'est pas correctement intégrée dans le cadre général de la gestion du risque de l'institution ».

Quelles sont les exigences en termes de ressources?

M. Philippe Dufresne: Il faut de la discipline. Il vous faut étudier le programme et répondre à certaines questions. C'est pourquoi les ressources ne sont pas nécessaires dans tous les cas. Qu'il y ait des critères est tout à fait légitime. Ils ne sont pas si gourmands en ressources qu'ils ne valent pas la peine d'être appliqués.

M. Matthew Green: Cela me semble être une condition étrange. Qu'il y ait « toutefois » dans le libellé d'une directive et qu'on l'associe avec les ressources. Compte tenu de ce que je pense que nous avons établi à ce comité sur l'importance de la démocratie et l'importance de notre vie privée, cela semble une phrase bizarre. C'est mon opinion. Ce n'est pas la vôtre.

Je crois que vous avez dit que le Conseil du Trésor encourageait les ÉFVP. Je vous signale qu'à l'article 5.1 de la directive du Conseil du Trésor, il est précisé que les évaluations des facteurs relatifs à la vie privée sont effectuées pour des « programmes nouveaux ou ayant subi des modifications importantes ».

Si c'est dans le libellé d'une directive, d'après vous — et je vous demande juste votre opinion — une directive est différente d'un encouragement, n'est-ce pas?

M. Philippe Dufresne: Je répondrais que oui.

M. Matthew Green: Est-il juste de dire que le Conseil du Trésor n'encourage pas...? En fait, par la directive, il précise que c'est ce qui doit se passer.

M. Philippe Dufresne: Je suis d'accord.

M. Matthew Green: Étant donné qu'il s'agit de l'article 5.1 de la Directive sur la Loi sur la protection de la vie privée et que les ministères n'ont pas... est-il juste de dire, à première vue, qu'ils ont enfreint l'article 5.1 de la directive du Conseil du Trésor?

M. Philippe Dufresne: Dans ce cas, un certain nombre de ministères qui n'ont pas effectué d'ÉFVP ne sont pas conformes à cette directive.

• (1135)

M. Matthew Green: Il est probable qu'il y en ait d'autres, à ce stade, dont nous n'avons peut-être pas connaissance. L'article 5.2.1 de la directive stipule que « les évaluations des facteurs relatifs à la vie privée sont effectuées d'une manière proportionnée au niveau de risque déterminé avant l'établissement d'une activité ou d'un programme nouveau ou ayant subi des modifications importantes ». Non seulement les ministères sont négligents dans leur application des ÉFVP, mais le fait même qu'ils aient lancé le programme sans les effectuer.... Ce que je comprends de ce paragraphe, c'est qu'il indique qu'il s'agit d'une infraction assez considérable.

M. Philippe Dufresne: Oui, il y a la composante « avant les faits et non après les faits ».

M. Matthew Green: Cependant, c'est une directive.

M. Philippe Dufresne: C'est la directive.

M. Matthew Green: Ce n'est pas un encouragement.

M. Philippe Dufresne: C'est exact.

M. Matthew Green: Cependant, ces agences sont allées de l'avant et ont quand même lancé leur programme.

À cet égard, je crois qu'il est important de faire une distinction, parce que je ne voudrais pas que les Canadiens aient l'impression que le gouvernement fédéral a cette capacité sur tous les appareils du pays. Nous avons certainement étudié, à notre grand regret, l'utilisation des technologies de suivi des mouvements dans le cadre de la COVID. Je pense que nous avons fait un assez bon travail d'ana-

lyse. Dans ce cas, il s'agit d'employés fédéraux et, si je comprends bien votre témoignage, ceux qui font l'objet d'une enquête sont en infraction à la loi.

Est-ce exact?

M. Philippe Dufresne: Oui.

M. Matthew Green: Quand nous examinons Pêches et Océans, le CRTC, Environnement et Changement climatique Canada, le Bureau de la concurrence, l'ASFC, la GRC, la Défense nationale cela pourrait concerner des civils. Est-ce exact?

M. Philippe Dufresne: Oui.

M. Matthew Green: Dans le cas où cela comprendrait des civils, je suppose, sur la base de votre témoignage, que cette technologie doit être en la possession du gouvernement... Est-ce qu'il faudrait un mandat?

M. Philippe Dufresne: Dans certains cas, oui. Dans d'autres, non. Dans la situation où vous effectuez une enquête interne sur des employés, non.

M. Matthew Green: Cependant, pour des civils, par exemple...?

M. Philippe Dufresne: Dans de nombreux cas, un mandat est nécessaire. Les ministères l'ont indiqué. Comme c'était le cas de l'étude de la GRC sur l'utilisation des outils d'enquête sur l'appareil, il faut également des mandats. Cependant, c'est une question distincte de celle des évaluations des facteurs relatifs à la vie privée. Le mandat peut être fondé sur des critères distincts des considérations relatives à la vie privée qui sont au cœur des évaluations d'incidence sur la vie privée.

M. Matthew Green: Ce qui m'inquiète c'est qu'il n'y a pas eu de « oui, ils auraient besoin d'un mandat lorsqu'ils l'appliquent à des civils » ferme.

Dans quelles situations les mandats ne seraient-ils pas nécessaires pour des civils qui ne sont pas à l'emploi du gouvernement fédéral?

M. Philippe Dufresne: C'est une question à poser de préférence au ministère concerné, parce que c'est leur utilisation de leur...

M. Matthew Green: C'est tout à fait juste.

Dans votre évaluation ou dans votre enquête sur tout cela, est-ce quelque chose dont vous tenez compte ? Ont-ils l'obligation de signaler les instances pour lesquelles il n'y avait ni mandat ni EFVP?

M. Philippe Dufresne: La question du mandat est pertinente pour nous lorsque nous examinons le fondement juridique de l'utilisation. C'est un des critères. Une enquête menée il y a quelques années concernait l'utilisation de tours de transmission cellulaire. Certains aspects de l'enquête se sont faits sans mandat et nous avons déclaré que cela n'était pas justifié.

M. Matthew Green: Vous parlez plus particulièrement de la technologie Stingray?

M. Philippe Dufresne: Je crois bien. Nous pourrions obtenir le nom exact.

Cela constituait un problème. C'est ce que nous avons étudié comme première question. Même si vous avez un mandat et un fondement juridique, une deuxième question se pose: devez-vous procéder à une EFVP?

M. Matthew Green: Juste pour résumer, en ce qui concerne l'évaluation des facteurs relatifs à la vie privée, vous la considérez comme un élément à prendre en compte en plus du mandat. Même pour quelque chose de légal appuyé par un mandat, cela pourrait ne pas être éthique ou conforme à la loi, selon vous, dans le cadre d'une EFVP.

Si vous établissez, dans le cadre d'une EFVP, que ce n'est pas le cas, avez-vous l'autorité nécessaire pour les empêcher dans les faits de mettre en œuvre ces technologies?

M. Philippe Dufresne: Non, parce qu'il ne s'agit pas d'une obligation légale. Nous pouvons le signaler et le Conseil du Trésor peut le soulever, mais tout cela relève des règles du gouvernement.

M. Matthew Green: Je vous remercie.

Le président: Je vous remercie, monsieur Dufresne, ainsi que monsieur Green.

Notre premier tour de questions est donc terminé. Nous allons passer au deuxième tour.

Vous savez à quel point je déteste interrompre les gens. Nous avons bien dépassé les six minutes pour chacun, simplement pour être juste envers tout le monde. Essayons cette fois de nous tenir aux cinq minutes ou au temps qui vous est imparti. Nous en arrivons au vif du sujet, me semble-t-il, et je voudrais que tout le monde puisse avoir sa chance.

Monsieur Kurek, vous avez la parole pour cinq minutes, je vous prie.

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

Je vous remercie, monsieur le commissaire, d'être là. Je vous remercie ainsi que votre équipe de votre travail.

Je voudrais simplement souligner quelque chose pour ceux qui nous écoutent et nous regardent. Treize institutions gouvernementales ont été mises en cause dans l'article mentionné. Il s'agit de Pêches et Océans Canada, Environnement et Changement climatique Canada, le CRTC, l'ARC, Services partagés Canada, le Bureau de la concurrence, Affaires mondiales, le Bureau de la sécurité des transports Canada, Ressources naturelles Canada, Services correctionnels Canada, l'Agence des services frontaliers du Canada, la Défense nationale et la GRC.

Certains de ces noms ne me surprennent pas, comme je crois que beaucoup de Canadiens n'en seraient pas surpris. La question de la confiance est certainement mise en évidence ici.

Monsieur le commissaire, pensez-vous que nous aurions su tout cela sans ce signalement médiatique? Existe-t-il un mécanisme de signalement au sein du gouvernement qui aurait permis de dire si ces outils étaient utilisés et combien de fois ils l'ont été? Sans cet article qui y fait référence, ces informations seraient-elles apparues autrement?

● (1140)

M. Philippe Dufresne: Nous n'étions pas au courant de toutes ces utilisations. Nous étions au courant pour certains programmes, mais c'est la question à laquelle l'évaluation des facteurs relatifs à la vie privée était censée répondre. Nous devrions être informés. Mon bureau devrait être informé avant le déploiement de ces nouveaux outils et de ces nouvelles activités.

M. Damien Kurek: J'espère qu'un jour ou l'autre, ce sera un ministre qui répondra aux questions à votre place.

Votre bureau a-t-il les ressources pour veiller à ce que les réponses à ces questions concernant les EFVP, que l'un ou l'autre de ces 13 ministères pourrait vous poser, leur parviennent en temps utile?

Franchement, je crains qu'il n'y ait pas que cela. Si nous avons 13 ministères qui travaillent avec beaucoup d'autres ministères... et ainsi de suite....

Êtes-vous sûr que votre bureau est en mesure de répondre et de donner des conseils si nécessaire, que ce soit à ces 13 ministères ou à d'autres ministères qui pourraient employer des outils comme ceux-là?

M. Philippe Dufresne: D'une manière générale, j'ai demandé au Parlement davantage de ressources pour mon bureau, y compris pour nos activités promotionnelles. Nous avons une équipe consultative gouvernementale qui se tient prête à fournir des conseils aux ministères. Nous déterminons la priorité de ce que nous recevons en fonction de l'importance et des répercussions. Nous continuerons de surveiller cela. Nous pourrions faire d'autres demandes pour obtenir des ressources supplémentaires.

L'essentiel, c'est sûr, est que nous soyons informés de ces questions. Les ministères doivent nous informer avant de commencer ce genre de choses. Cela fait également partie de la directive du Conseil du Trésor.

C'est ce que j'aimerais voir plus souvent, une prise de contact plus proactive de la part de ces ministères pour dire: « Nous envisageons de le faire. Avons-nous besoin d'une EFVP? Voici les informations. » De sorte que nous n'apprenions pas cela par les médias. La couverture médiatique est très importante dans ce cas, mais dans l'idéal, nous devrions le savoir à l'avance.

M. Damien Kurek: Simplement pour plus de clarté, si quelqu'un vous appelle, même s'il s'agit d'une situation en cours qui ne peut pas vraiment attendre, il y aurait quelqu'un pour répondre au téléphone qui serait en mesure de donner des réponses et de prodiguer des conseils. Juste pour plus de clarté.

M. Philippe Dufresne: C'est tout à fait juste. C'est notre rôle. Nous donnons des conseils. Nous signalons les problèmes. Nous ne sommes pas là pour nuire à l'innovation et à l'intérêt de la population. Nous sommes là pour donner des conseils et dire: « Voici les répercussions sur la vie privée et la façon de les aborder. » Nous améliorons la transparence. C'est dans l'intérêt de tout le monde.

M. Damien Kurek: J'en suis ravi, car nous entendons bien souvent dire que c'était urgent, de sorte que les responsables n'ont pas eu le temps ou les ressources nécessaires. Je vous remercie d'avoir clarifié ce point aujourd'hui.

Parmi ces 13 ministères, des évaluations des facteurs relatifs à la vie privée, ou EFVP, ont-elles été réalisées depuis?

M. Philippe Dufresne: Trois de ces ministères ont terminé l'EFVP sur les programmes en question. C'est fait. Pour les autres, l'un d'entre eux a acheté l'outil et ne l'a pas utilisé — il n'y a donc pas d'EFVP —, alors que la majorité d'entre eux, soit huit, vont mettre à jour leur évaluation ou en réaliser une nouvelle. Tout est en suspens.

M. Damien Kurek: Pour ce qui est de la question qui a été posée visant à savoir qui est touché... Ce n'est pas un problème généralisé, comme le croient M. Green et Mme Khalid. Ce ne sont pas tous les Canadiens qui sont concernés, mais il y a assurément des cas où ce sont les employés d'un ministère. Cela ne diminue en rien les attentes en matière de protection de la vie privée, comme nous l'avons dit. Il est toutefois arrivé que les données de citoyens aient été utilisées sans mandat.

Je voudrais juste utiliser les dernières secondes pour m'assurer d'interpréter correctement vos propos.

M. Philippe Dufresne: En fait, je m'en remets aux ministères pour qu'ils se conforment à leurs obligations légales entourant la nécessité ou non d'un mandat et leurs pouvoirs.

Ce que je souligne, c'est qu'ils doivent procéder à des EFVP. Certains n'en ont pas fait.

Le président: Je remercie M. Kurek et M. Dufresne.

Monsieur Bains, vous avez la parole pour cinq minutes. Allez-y, monsieur.

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

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

Monsieur le commissaire, votre bureau a-t-il commencé à enquêter sur l'un ou l'autre de ces ministères à la suite des révélations?

• (1145)

M. Philippe Dufresne: Je crois que vous demandez si nous avons enquêté sur l'un ou l'autre de ces ministères à la suite des révélations. Ce n'est pas le cas. Comme je l'ai indiqué, il n'y a pas d'obligation légale en vertu de la Loi sur la protection des renseignements personnels. Je n'ai donc pas de raison d'enquêter sur le non-respect de cette directive. Nous avons pris contact avec les ministères, et nous poursuivons sur cette voie. Nous allons continuer à insister sur le fait que les EFVP doivent être réalisées.

Je recommande au Comité et à la Chambre d'en faire une obligation légale prévue à la Loi sur la protection des renseignements personnels. Il faudrait également que ce soit une obligation légale dans la législation sur la protection des renseignements personnels du secteur privé. Ce serait ainsi une obligation proactive qui me donnerait plus évidemment le mandat et le pouvoir de m'assurer que c'est fait. Les Canadiens considéreraient que cela fait partie de leur protection en matière de vie privée.

Trop souvent, les Canadiens ont l'impression d'être livrés à eux-mêmes. C'est à eux de donner leur consentement. C'est à eux de s'informer. Nous donnons des conseils aux Canadiens sur les meilleures pratiques en matière de protection de la vie privée, entre autres. Or, les Canadiens méritent de se sentir protégés par leurs institutions et de pouvoir s'y fier, en sachant que le gouvernement utilise cette technologie, qu'il a consulté le Commissariat à la protection de la vie privée et que des experts en la matière participent à sa conception.

C'est ce que je souhaite voir plus souvent. Tout commence par une obligation enchâssée dans la Loi sur la protection des renseignements personnels.

M. Parm Bains: Une partie de notre travail prend la forme de recommandations. Votre principale recommandation consiste à rendre obligatoire l'évaluation des facteurs relatifs à la vie privée.

L'article 5.1 de la Directive sur l'évaluation des facteurs relatifs à la vie privée prévoit qu'une telle évaluation doit être effectuée « pour des activités ou programmes nouveaux ou ayant subi des modifications importantes nécessitant la création, la collecte et le traitement de renseignements personnels. »

Les institutions fédérales font-elles une distinction claire entre une activité ou un programme nouveau et ceux qui existent déjà?

M. Philippe Dufresne: Elles le font. C'est ici que les institutions estiment parfois qu'il ne s'agit pas d'un nouveau programme, mais bien d'un programme existant, et qu'elles n'ont pas vraiment changé ce qu'elles font. Elles ont juste un nouvel outil plus puissant. Elles n'ont pas soumis l'outil à une EFVP parce que le programme a déjà été évalué. Ce type de situation pourrait bien être conforme à la politique étant donné que la directive n'exige pas de nouvelle évaluation des facteurs relatifs à la vie privée dans ce cas.

Lorsque nous parlons d'outils très puissants — il ne s'agit peut-être pas d'un nouveau programme, mais le mécanisme change tellement la donne qu'il procure désormais une capacité —, il y a lieu de se demander si les Canadiens tireraient profit d'une plus grande transparence sur celui-ci, même s'il s'agit du même programme.

M. Parm Bains: Faut-il apporter d'autres modifications à la directive du Conseil du Trésor sur l'EFVP? Quels autres éléments pourraient être changés?

M. Philippe Dufresne: Ce que j'aimerais, c'est que mon bureau soit davantage sollicité en amont lors de nouvelles initiatives. La politique comporte cette exigence, mais ce n'est pas respecté dans la plupart des cas.

Je pense qu'il faut avoir le réflexe de dire: « Vous n'irez pas de l'avant dans ce dossier tant que vous n'aurez pas eu de consultation et fait preuve de la diligence nécessaire. » Il faudrait peut-être aussi préciser que, lorsqu'un outil est beaucoup plus puissant, il peut nécessiter un second examen d'un programme existant.

M. Parm Bains: Vous avez fait ces demandes. Quelles sont les prochaines étapes après aujourd'hui pour ces 13 ministères?

M. Philippe Dufresne: De notre point de vue, nous allons continuer à tendre la main à ces ministères. Nous allons faire un suivi pour veiller à ce que les évaluations manquantes soient réalisées. Nous allons continuer à poser des questions et à travailler en collaboration avec eux.

J'espère que, dans le cadre des travaux du Comité et du processus législatif, nous assisterons à une modernisation de la Loi sur la protection des renseignements personnels. Je souhaite que celle-ci comprenne une obligation légale de réaliser des EFVP lorsque les circonstances le justifient, ainsi que d'autres éléments tels que la nécessité et la proportionnalité, dont nous avons discuté. Il y a là une occasion à saisir.

La Chambre est actuellement saisie d'une réforme de la législation dans le secteur privé. Nous espérons que les changements nécessaires seront apportés, mais la Loi sur la protection des renseignements personnels est encore plus ancienne. J'espère vraiment que la Chambre s'en occupera bientôt.

• (1150)

Le président: Merci, monsieur Bains.

Merci, monsieur Dufresne.

[Français]

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

M. René Villemure: La Loi sur la protection des renseignements personnels date de 1983, n'est-ce pas?

La proactivité dont vous faites état, ici, est-ce une chose qu'on doit justement mettre dans une loi? Est-ce que cela va faciliter les choses?

M. Philippe Dufresne: Je pense que lorsqu'une obligation est inscrite dans une loi, cela met l'accent sur cette obligation; c'est toujours le cas. Effectivement, il est beaucoup plus facile de se rabattre sur une directive ou une politique, mais une loi impose vraiment de la pression, des contraintes, le besoin de prendre le temps, et de gérer la situation différemment.

En effet, la Loi devrait imposer, avant la mise sur pied d'un programme, l'obligation de fournir au Commissariat les détails pertinents dans un délai prescrit. Ces détails peuvent être précisés soit dans la Loi, soit dans le règlement. Cette proactivité est importante.

M. René Villemure: Évidemment, en 1983, ce n'était peut-être pas aussi urgent.

La loi 25 au Québec aurait-elle empêché ce genre de surveillance?

M. Philippe Dufresne: Je sais que la loi 25 comporte certaines exigences en matière d'évaluation des facteurs relatifs à la vie privée, notamment lorsque des données quittent le Québec ou en lien avec l'utilisation de nouvelles données par le gouvernement ou par le secteur privé. La Loi a certainement codifié le besoin de telles évaluations dans certains cas, mais il faudrait que je vous fournisse des détails à ce sujet plus tard.

M. René Villemure: Dans le contexte d'une éventuelle révision de la Loi sur la protection des renseignements personnels, y a-t-il des enseignements de la loi 25 qu'on pourrait retenir?

M. Philippe Dufresne: La loi 25 a donné à la Commission d'accès à l'information du Québec le pouvoir d'émettre des ordonnances et la possibilité d'imposer des sanctions administratives pécuniaires. C'est peut-être moins essentiel dans le contexte du secteur public, mais cela peut quand même aider à traiter la question de la vie privée comme un droit fondamental et d'en faire une priorité.

Je pense que, tant pour le secteur privé que pour le secteur public, on peut certainement s'inspirer d'éléments comparables, y compris la loi 25.

M. René Villemure: J'y vais au hasard, mais la Loi, telle que rédigée en 1983, ne contient sûrement aucune disposition traitant de l'intelligence artificielle, n'est-ce pas?

M. Philippe Dufresne: C'est sûr. La Loi a été rédigée avant l'avènement d'Internet et des médias sociaux. Il y a eu énormément de changements qui font que les lois doivent être modernisées.

Cela étant dit, je profite de l'occasion pour le répéter: mes collègues, tant au Canada qu'à l'international, et moi-même avons fait plusieurs déclarations sur l'intelligence artificielle indiquant que les lois existantes s'appliquent. Elles ne tenaient peut-être pas compte de l'intelligence artificielle, mais elles sont neutres sur le plan technologique. Quant à nous, nous les interprétons certainement comme si elles s'appliquent à l'intelligence artificielle. Nous avons des plaintes en cours à ce sujet. Nous avons émis une déclaration com-

mune à ce sujet. Nous travaillons très étroitement avec nos homologues des provinces et des territoires.

Il est sûr que la modernisation de ces lois viendrait clarifier certaines choses, notamment cet aspect de la proactivité. Je l'ai recommandé explicitement en ce qui a trait à l'intelligence artificielle dans le contexte de la modernisation de la loi régissant le secteur privé. Il est question entre autres d'évaluations algorithmiques et on parle de tout cela, car c'est très important.

L'idée n'est pas de refuser la technologie, mais de la baliser.

Le président: Merci, messieurs Dufresne et Villemure.

J'ai accordé plus de temps à M. Dufresne pour lui permettre de compléter sa réponse.

[Traduction]

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

M. Matthew Green: Merci beaucoup, monsieur le président.

Je regarde le dossier, et je pense que vous avez fait référence à un terme important lorsque vous avez parlé des obligations en vertu de la Loi sur la protection des renseignements personnels et du fait que les Canadiens se fient aux institutions. En fin de compte, seriez-vous d'accord pour dire que la protection de la vie privée est une question de confiance?

M. Philippe Dufresne: Je suis d'accord.

M. Matthew Green: Pour ce qui est de cette confiance, nous envisageons des scénarios pour nos employés fédéraux dans un monde où le téléphone portable est de plus en plus le reflet de presque tous les aspects de sa vie, qu'il s'agisse de la mobilité ou de... Je pense aux applications que j'ai sur mon téléphone. J'ai des applications de suivi de santé et d'autres choses très personnelles. En tant qu'employé fédéral... Je pense même à la montre que je porte, par exemple, et à mon rythme cardiaque. Le téléphone suit tout — les finances et absolument tout.

Nous avons beaucoup parlé des aspects technologiques et du contexte de cette technologie. Nous n'avons pas abordé le contexte humain, qui se trouve en fin de compte de l'autre côté. Quelqu'un y a accès.

Dans votre travail, examinez-vous qui, précisément, a accès à l'information? Y a-t-il une cote de sécurité, ou s'agit-il d'un informaticien de niveau intermédiaire qui pourrait vouloir vérifier si j'ai des photos ou des messages textes de quelqu'un qu'il n'aime pas forcément?

M. Philippe Dufresne: C'est un élément très pertinent à prendre en considération pour la gestion de l'information en général, mais aussi dans le cadre d'une EFVP. Il ne s'agit pas seulement de vérifier les renseignements recueillis, la raison et le besoin, mais aussi de savoir comment vous protégez les données.

Nous voyons de plus en plus d'atteintes à la vie privée, de cyberattaques et de vols d'informations. La sécurité de ces renseignements est donc primordiale, et il faut savoir qui y a accès et a besoin de les connaître...

• (1155)

M. Matthew Green: Pour en venir directement au sujet, est-ce que l'EFVP tient compte de la cote de sécurité requise pour consulter ce qui pourrait être en fin de compte des informations profondément personnelles?

M. Philippe Dufresne: Oui. Il y a un examen des pratiques de conservation et de sauvegarde. Cela irait à...

M. Matthew Green: D'après votre expérience, qui aurait accès à ces informations dans les équipes de technologies de l'information de ces ministères? Quel serait leur niveau de responsabilité?

M. Philippe Dufresne: Ces gens seraient les mieux placés pour répondre à la question, mais il est certain que le Commissariat à la protection de la vie privée examine les informations suivantes: de quel type d'information s'agit-il? S'agit-il de documents classés protégé A, B ou C? La perte de ces informations présente-t-elle des risques pour la sécurité des personnes? Y a-t-il des enjeux de sécurité nationale?

Il existe toute une série de règles et de critères à respecter pour assurer la protection. Il va falloir...

M. Matthew Green: J'ai une dernière question. Avez-vous reçu des plaintes, suite à la publication de cette histoire, de la part d'employés ou du syndicat en raison de l'utilisation de cette technologie? Votre commissariat a-t-il reçu des plaintes?

Le président: Veuillez donner une réponse rapide.

M. Philippe Dufresne: À ma connaissance, nous n'avons pas reçu de plaintes à ce sujet.

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

Nous allons céder la parole à M. Brock, qui a cinq minutes, et ce sera ensuite au tour de M. Erskine-Smith.

Nous n'avons pas encore fait d'essai avec M. Erskine-Smith. Nous verrons ce qu'il en est lorsqu'il commencera, puis nous reprendrons pour six minutes.

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

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

J'aimerais remercier les témoins de leur présence aujourd'hui. Il s'agit d'une question très importante et très sérieuse non seulement pour les Canadiens, mais aussi pour la fonction publique. J'aimerais commencer par examiner certains principes juridiques.

Chaque Canadien, y compris les fonctionnaires, a le droit absolu, conformément à l'article 8 de la Charte canadienne des droits et libertés, à la protection contre les fouilles, les perquisitions ou les saisies abusives. Même si vous avez déclaré qu'une autorisation légale a été obtenue dans certains cas, monsieur, vous ne pouvez pas affirmer avec certitude que c'était ainsi dans tous les cas. Cela soulève des questions relatives à la Charte. La violation d'un droit prévu à l'article 8 est une infraction grave qui, si je me réfère à mes années en tant que procureur de la Couronne, n'est pas toujours couronnée de succès. Il y a des conséquences strictes pour les droits à la vie privée des Canadiens, comme l'ont confirmé les tribunaux de tout le pays.

Cette toile de fond était importante pour moi afin de formuler cette question. Lorsque je regarde les 13 institutions qui ont été identifiées, rien ne garantit qu'elles étaient les seules à avoir utilisé cette technologie. Est-ce juste, monsieur?

M. Philippe Dufresne: C'est possible.

M. Larry Brock: Oui... Ce sont les institutions qui ont été identifiées par la journaliste de la CBC, n'est-ce pas?

M. Philippe Dufresne: C'est vrai.

M. Larry Brock: Lorsque j'examine cette liste, je pourrais m'attarder à Pêches et Océans Canada, et peut-être au Bureau de la concurrence. Mais lorsque je vois l'Agence du revenu du Canada, les Affaires mondiales, les Services correctionnels, l'Agence des services frontaliers du Canada, la Défense nationale et, surtout, la GRC, je constate que ces agences ont toutes d'excellentes équipes juridiques qui travaillent en coulisse — c'est bien souvent le ministère de la Justice. Ils donneraient certainement des instructions non seulement à la direction de ces ministères, mais aussi à leurs employés, au sujet de la protection des droits à la vie privée. Apprendre que, dans de nombreux cas, l'autorisation judiciaire n'a pas été accordée, qu'une évaluation des facteurs relatifs à la vie privée n'a pas été soumise à votre examen et que des données ont été collectées, soulève de sérieuses inquiétudes en matière de protection de la vie privée.

Monsieur, vous avez mentionné une chose tout à l'heure dans votre déclaration liminaire, je crois. Bien souvent, lorsque ce dispositif a été utilisé sur des employés du secteur public, c'était avec le consentement du propriétaire du dispositif. Or, vous ne pouvez pas dire que tous les cas d'extraction de données avec ce logiciel avaient déjà le consentement du détenteur du dispositif. Est-ce que c'est juste, monsieur?

M. Philippe Dufresne: C'est juste. Je n'en suis pas certain.

M. Larry Brock: Je vois. Il y a donc encore d'autres atteintes à la vie privée.

La GRC a dit après coup qu'elle avait soumis une EFVP en décembre, je crois. Est-ce exact? Certaines organisations ont dit qu'elles l'avaient remise plus tôt. Pouvez-vous nous dire si vous avez consulté les ministères qui n'ont pas soumis d'évaluation et si vous leur avez demandé précisément pourquoi ils ont contourné la directive du Conseil du Trésor dans ces circonstances?

• (1200)

M. Philippe Dufresne: Nous avons contacté les 13 organisations. Comme je l'ai dit au début, trois d'entre elles ont indiqué avoir fait une EFVP de leur programme. Les autres ne l'avaient pas fait. Nous allons discuter avec chacune d'elles. Nous allons poursuivre les échanges, assurer un suivi et leur dire: « Nous voulons comprendre quand ce sera fait et pourquoi l'évaluation n'a pas été effectuée, et nous assurer que ce sera fait comme il se doit. » Cependant, nous n'avons pas l'autorité légale de l'imposer si l'entité n'est pas d'accord.

M. Larry Brock: C'est une chose qui pourrait être améliorée par un amendement à la Loi sur la protection des renseignements personnels, n'est-ce pas?

M. Philippe Dufresne: C'est exact. C'est ce que je recommande.

M. Larry Brock: Sans surprise, la Loi sur la protection des renseignements personnels ne prévoit pas de conséquences juridiques ou de sanctions en cas de non-respect des exigences en matière d'EFVP. Est-ce que c'est juste, monsieur?

M. Philippe Dufresne: C'est vrai. Dans mon bureau, je n'ai pas le pouvoir de rendre des ordonnances, même pour des choses qui sont dans cette loi. Je peux mener une enquête et faire une constatation, mais je dois m'en remettre au gouvernement ou à l'institution pour qu'ils s'y conforment.

M. Larry Brock: Est-ce un amendement que vous recommanderiez aussi, monsieur?

M. Philippe Dufresne: Oui, c'en est certainement un.

M. Larry Brock: Je vous remercie.

Le président: Je vous remercie, monsieur Brock.

[Français]

Merci, monsieur Dufresne.

[Traduction]

Monsieur Erskine-Smith, vous avez cinq minutes. Nous allons nous assurer que votre technologie fonctionne. Allez-y.

M. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Merci, monsieur Brassard. C'est un plaisir de vous voir.

Je suis ravi de voir tout le monde ici, en particulier les analystes.

Monsieur le commissaire, est-ce que l'un des 10 ministères sur 13 qui n'ont pas encore fait d'EFVP a refusé d'en réaliser une?

M. Philippe Dufresne: Un d'entre eux a indiqué qu'il avait acheté l'outil, mais ne l'avait jamais utilisé. Il n'a pas dit qu'il allait se prêter à l'exercice. L'un d'eux a mentionné qu'à son avis, ce n'était pas nécessaire. Nous allons faire un suivi pour voir si nous sommes d'accord avec cette conclusion et en discuter.

M. Nathaniel Erskine-Smith: Quelle entité a dit que ce n'était pas nécessaire?

M. Philippe Dufresne: C'était le Bureau de la concurrence.

M. Nathaniel Erskine-Smith: D'accord.

Pour ce qui est des autres, il serait utile que vous leur fixiez un délai, disons de 20 à 30 jours. Vous pourriez alors nous revenir et nous aviser si vous n'avez pas eu de réponse. Vous n'avez peut-être pas de pouvoirs, mais nous avons évidemment le pouvoir d'assigner à comparaître.

En ce qui concerne les instances, un ministère a répondu qu'il n'avait jamais eu recours à la technologie. Quelle est l'ampleur de son utilisation par les différents ministères? Avez-vous une idée de la fréquence à laquelle cet outil a été utilisé?

M. Philippe Dufresne: Nous avons des réponses diverses. Certains semblent utiliser couramment l'outil dans le cadre de leurs activités. D'autres ont indiqué un nombre plus restreint d'utilisations. De notre point de vue, que la technologie soit utilisée deux, trois ou quatre fois ou régulièrement, nous regardons la situation de la même manière. Est-ce une utilisation convenable, et le ministère doit-il faire l'EFVP ou non?

M. Nathaniel Erskine-Smith: Voyons cela de plus près.

Il est évident qu'ils devraient faire une évaluation des facteurs relatifs à la vie privée. Je ne peux pas imaginer que quelqu'un ici soit en désaccord avec cette affirmation. Je comprends votre point de vue. Il est bien formulé. La loi devrait obliger ces organisations à procéder à une EFVP lorsqu'elles utilisent un nouvel outil ayant une incidence sur la vie privée.

Mais parlons de l'utilisation convenable. Dans le rapport de la CBC, j'ai vu des agences et des ministères indiquer qu'ils utilisaient parfois cet outil sans autorisation judiciaire, et, d'autres fois, uniquement sur des appareils appartenant au gouvernement et dans des affaires impliquant des employés soupçonnés de harcèlement.

En gros, ces deux cas me semblent tout à fait raisonnables. Connaissez-vous d'autres situations dont nous devrions nous préoccuper?

M. Philippe Dufresne: J'ai vu les réponses des ministères. Ils ont fourni des renseignements sur les types de programmes pour lesquels ils utiliseraient cet outil. Je n'ai vu aucun objectif ou utili-

sation inappropriés qui pourrait soulever des inquiétudes. Ils utilisent cet outil pour remplir leur mandat, pour appliquer leur loi habilitante ou pour mener des enquêtes.

Ce qui me préoccupe, c'est de savoir si l'évaluation des facteurs relatifs à la vie privée a été bien menée, si elle a été menée en temps voulu et si les risques ont été atténués. Évidemment, c'est ce qui est de mon ressort. Des questions précises sur les pouvoirs législatifs dont ils disposent ou sur leurs mandats sont des questions distinctes qui pourraient être posées par le Comité.

Ce qui me préoccupe à ce moment-ci, c'est que nous devons tenir compte des facteurs relatifs à la vie privée dans toutes les situations qui peuvent avoir une incidence sur la vie privée des Canadiens, mais cela n'a pas toujours été fait.

• (1205)

M. Nathaniel Erskine-Smith: Je sais que vous revenez sur la nécessité de mener une évaluation des facteurs relatifs à la vie privée, mais même si une telle évaluation était menée, on pourrait imaginer que la portée d'une enquête donnée s'inscrirait dans le cadre de cette évaluation ou qu'elle la dépasserait. On ne vous a pas fourni d'exemples de cas ou de situations, du moins à votre connaissance, dans lesquels l'utilisation dépasse visiblement les limites des attentes de quiconque en matière de protection de la vie privée.

M. Philippe Dufresne: Non, mais cela met en évidence, une fois de plus, une autre recommandation que j'ai formulée et que votre comité a approuvée dans le cadre de l'étude sur l'outil d'enquête sur l'appareil. Il s'agit du principe de nécessité et de proportionnalité. Ce principe devrait également se trouver dans la loi, car c'est là où vous voulez en venir, c'est-à-dire que l'objectif peut être légitime, mais est-ce qu'on va trop loin dans la manière de l'atteindre?

M. Nathaniel Erskine-Smith: Oui, la portée de la recherche est une considération importante selon le contexte, l'objectif et la gravité de toute allégation, par exemple s'il s'agit d'une affaire de harcèlement d'un employé.

C'est tout en ce qui concerne mes questions. Toutefois, monsieur le commissaire, si vous avez des exemples de cas dans lesquels, selon vous, le caractère raisonnable ou le principe de nécessité et de proportionnalité n'ont pas été respectés, je vous serais reconnaissant de les communiquer au Comité.

M. Philippe Dufresne: Je vous remercie. J'en prends note.

Le président: Est-ce que c'est tout?

D'accord. Je vous remercie, monsieur Erskine-Smith. Il vous restait un peu de temps. Je vous remercie.

C'est ce qui termine notre première série de questions. Nous allons maintenant remettre le chronomètre à zéro et revenir à des séries de questions de six minutes.

La parole est d'abord à M. Barrett.

Monsieur Barrett, vous avez la parole.

M. Michael Barrett: Pouvez-vous nous expliquer la distinction qui existe, aux yeux de la loi, entre les données ou les renseignements qui sont stockés dans un appareil et les renseignements ou les données qui ne sont accessibles que par l'entremise de l'appareil?

La pertinence de ma question ou la précision que j'aimerais obtenir est liée à l'utilisation courante du stockage infonuagique. Même si l'appareil physique est la propriété du gouvernement du Canada ou d'un ministère, une personne qui a ouvert une session pour récupérer ses renseignements dans le stockage infonuagique est d'avis que ces renseignements ne sont pas stockés dans l'appareil du gouvernement, car ils sont accessibles par l'entremise de cet appareil grâce aux données d'authentification de cette personne qui servent à ouvrir une session. Quelle est la différence aux yeux de la loi?

M. Philippe Dufresne: Nous considérons que les renseignements personnels sur cette personne sont des renseignements personnels pour cette personne. Qu'ils se trouvent dans l'appareil, dans le nuage ou sous une autre forme, nous nous demandons notamment si ces renseignements sont protégés de manière appropriée, qui a accès à ces renseignements, qui les contrôle, si le gouvernement a le pouvoir de saisir ces renseignements et quelles sont les limites en place.

Nous ne nous arrêtons pas trop à la question de savoir si les renseignements se trouvent dans le nuage ou dans l'appareil. Nous nous concentrons plutôt sur la façon dont ils ont été obtenus, la technologie utilisée et les attentes des personnes concernées. Ce sont toutes des questions que nous nous poserions dans ce contexte.

M. Michael Barrett: Le gouvernement n'est donc soumis à aucune limite liée à l'utilisation de ces technologies pour espionner les Canadiens. Microsoft — de nombreuses personnes utilisent Microsoft pour stocker leurs documents —, Dropbox et Google sont tous fondés sur l'infonuagique. Les gens y stockent leurs photos de famille, leur correspondance personnelle et leurs renseignements médicaux confidentiels et privés.

Le gouvernement pourrait-il, par exemple, utiliser le prétexte selon lequel une personne s'est connectée une fois à son compte infonuagique à partir d'un appareil gouvernemental pour affirmer qu'il a maintenant un accès complet à ce compte? La seule mesure est-elle celle appliquée après coup, c'est-à-dire qu'on identifie les renseignements examinés par le gouvernement, qui peut affirmer qu'il n'a examiné que certaines choses?

Une fois qu'il a consulté les renseignements d'un employé, la vie privée de cet employé a été violée. La vie privée de ce Canadien a été violée. Y a-t-il des cas où c'est justifié?

• (1210)

M. Philippe Dufresne: Il existe un principe de la limitation de la collecte qui, encore une fois, est lié au principe de nécessité et de proportionnalité. Un employeur qui consulte les données de son employé doit faire preuve de transparence. Il doit s'assurer que l'employé est conscient qu'il s'agit de son appareil de travail. Si l'employé utilise cet appareil à des fins personnelles, les deux types de renseignements se chevauchent-ils? Quelles sont les attentes en ce qui concerne les choses auxquelles l'employeur aura accès? Pourquoi l'employeur doit-il avoir accès à ces choses?

Il s'agit de s'assurer que l'employeur ou tout autre organisme ne collecte pas et n'utilise pas plus de renseignements que ce qui est nécessaire. Cela signifie qu'il faut considérer l'objectif et le contexte. J'ai donné l'exemple des camionneurs filmés pendant leur temps libre. Ce n'était pas nécessaire pour la sécurité sur les routes.

Des questions similaires seront posées. Plus on tente d'obtenir des renseignements personnels, plus on devrait avoir à en justifier la raison. Encore une fois, c'est la raison d'être des évaluations des facteurs relatifs à la vie privée, ainsi que du principe de nécessité et

de proportionnalité. Nous vivons à une époque où cette technologie, comme vous l'avez dit, est de plus en plus invasive. Parfois, la vie personnelle et la vie professionnelle empiètent l'une sur l'autre, ce qui soulève des questions liées à la protection de la vie privée.

M. Michael Barrett: L'évaluation des facteurs relatifs à la vie privée sera-t-elle utilisée pour approuver le logiciel ou la technologie que le gouvernement prévoit d'utiliser ou existe-t-il un autre processus à cet égard? Ne devrait-on pas prévoir une exigence selon laquelle tout ministère doit faire approuver la technologie et le logiciel qu'il utilisera avant même de commencer à collecter des renseignements? Lorsqu'on dit qu'il ne s'agit que des employés du gouvernement du Canada, il ne faut pas oublier que le gouvernement est un employeur assez important dans notre pays. Dans l'ensemble, ces employés sont des Canadiens. Ne l'oublions pas.

Il semble que le gouvernement et les ministères sont très souvent en mode « rattrapage » lorsqu'il s'agit des questions liées à la protection de la vie privée. Recommanderiez-vous d'exiger que le logiciel en question soit approuvé avant l'achat?

M. Philippe Dufresne: Je vais vous lire l'article 4.2.2 de la *Politique sur la protection de la vie privée* du Conseil du Trésor. Le voici:

Aviser le commissaire à la protection de la vie privée de toute initiative prévue (loi, règlement, politique, programme) pouvant avoir un rapport avec la Loi sur la protection des renseignements personnels ou l'une de ses dispositions, ou pouvant avoir une incidence sur la vie privée des Canadiens et des Canadiennes. Cet avis doit être transmis suffisamment tôt pour permettre au commissaire d'examiner les questions et d'en discuter.

C'est la même chose. Il faut s'en occuper avant, et non après, afin d'être en mesure de signaler les problèmes.

Le président: Je vous remercie, MM. Dufresne et Barrett.

Madame Damoff, vous avez la parole. Vous avez six minutes.

Mme Pam Damoff (Oakville-Nord—Burlington, Lib.): Je vous remercie, monsieur le président.

Je remercie sincèrement les témoins d'être ici aujourd'hui et de nous éclairer sur cette question importante.

Tout d'abord, j'aimerais vous poser une question. S'agit-il d'un logiciel espion?

M. Philippe Dufresne: Ce n'est pas un logiciel espion. En effet, les logiciels espions sont installés à distance et à l'insu de la personne. Il est donc possible de le faire sans avoir accès à l'appareil. Dans le cas qui nous occupe, il s'agit d'un outil d'investigation informatique, et c'est donc un type d'outil différent.

Mme Pam Damoff: Mes collègues conservateurs ont parlé à plusieurs reprises aujourd'hui d'un « logiciel espion », et je tenais donc à apporter ces éclaircissements.

Je me souviens qu'en 1996, avant l'apparition de ces types de téléphones, je travaillais dans les services bancaires d'investissement immobilier chez Midland Walwyn. Je savais qu'on se servait des technologies de l'information pour surveiller ce qui se trouvait sur mon ordinateur, car on me l'avait dit. C'était mon ordinateur de travail et il devait être utilisé à cette fin. Le même principe s'applique à mon iPhone de la Chambre des communes. Je sais que c'est un téléphone de travail qui est censé être utilisé à cette fin.

Comme mon collègue néo-démocrate, j'ai une montre Apple. Elle est connectée à mon téléphone personnel.

Pourquoi le gouvernement aurait-il accès à des renseignements personnels sur la santé d'une personne, à moins que cette personne ait décidé d'entrer ses renseignements personnels dans un téléphone de travail tout en sachant pertinemment que ce téléphone est censé n'être utilisé que pour le travail? Je ne comprends pas très bien.

M. Philippe Dufresne: Nous en parlons dans notre document intitulé *La protection des renseignements personnels au travail* que nous avons révisé en mai 2023. Il y est question de surveillance et de transparence. Pour répondre à votre question, si vous, à titre d'employée, avez été informée de ce que l'employeur peut et ne peut pas faire et de ce que les outils de l'employeur peuvent faire si vous les utilisez, vous êtes donc au courant à titre d'utilisatrice. Vous avez accès à cette transparence.

Dans certaines circonstances, il peut être justifié que l'employeur ait accès à certaines choses. Toutefois, même si ces autres renseignements se trouvent sur le téléphone, pourquoi l'employeur aurait-il besoin d'accéder à vos renseignements en matière de santé? Vous les avez entrés dans ce téléphone, peut-être à juste titre, peut-être à tort, mais l'employeur a-t-il besoin d'y avoir accès?

Comment peut-on trouver un équilibre entre les limites liées à l'utilisation et à la collecte de renseignements et la transparence? Nous devons moderniser ces règlements et les appliquer à une technologie en constante évolution. C'était beaucoup plus facile avant, car comme vous l'avez dit, ces appareils brouillent la frontière entre la vie professionnelle et la vie personnelle.

Nous avons parlé du fait que la GRC avait utilisé des outils d'enquête sur appareil parce que les dispositifs d'écoute électronique ne fonctionnaient plus. En effet, les gens n'utilisent plus les lignes téléphoniques terrestres. Toutefois, les lignes terrestres fournissaient considérablement moins de renseignements que les téléphones intelligents. C'est un exemple d'un outil différent, mais qui a une plus grande portée.

• (1215)

Mme Pam Damoff: J'ai déjà posé ce type de questions à la GRC, car je faisais partie du Comité permanent de la sécurité publique et nationale.

Je suis un peu perplexe, car si je ne me trompe pas, je pense que les tribunaux ont donné raison à la société Apple, qui refuse de fournir des mots de passe pour avoir accès à des téléphones intelligents. J'ai entendu les services de police et la GRC affirmer qu'ils sont bloqués dans des affaires parce qu'ils ne peuvent pas avoir accès à ces renseignements, même dans des cas potentiels de crime organisé.

D'après ce que j'entends ici aujourd'hui, il semblerait que la GRC ait obtenu un accès. Nous parlons d'employés, n'est-ce pas? Nous ne parlons pas de criminels organisés pour lesquels la GRC aimerait avoir cet accès. Je pense que nous ne savons pas exactement de quoi nous parlons lorsqu'il s'agit de nos services de police.

M. Philippe Dufresne: Dans ce cas-ci, la GRC utilise ces outils pour ses enquêtes en général. Elle n'enquête pas sur ses employés. Trois des organismes en question les utilisent dans le cadre d'enquêtes internes.

Mme Pam Damoff: Mais il faut toutefois qu'ils obtiennent le téléphone. Il faudrait qu'ils me convoquent et que je leur fournisse physiquement mon téléphone. Est-ce exact?

M. Philippe Dufresne: C'est exact.

Mme Pam Damoff: Il ne s'agit donc pas d'opérations furtives où la GRC collecte les renseignements personnels de Canadiens pendant qu'ils sont assis chez eux dans leur salon.

M. Philippe Dufresne: C'est exact. Ce n'est pas la même chose qu'un logiciel espion. Dans ce cas-ci, il faut être en possession de l'appareil et extraire les renseignements qu'il contient.

Encore une fois, dans certains cas, il est tout à fait justifié que la GRC ou un employeur obtiennent ces renseignements. Le problème, c'est que nous devons veiller à ce que la protection de la vie privée soit prise en compte dans ces cas. Nous devons assurer la transparence et la mise en place de mesures de protection. Je ne veux pas laisser entendre que l'utilisation de cet outil est complètement inacceptable et qu'il faut y mettre un terme, mais il s'agit de tenir compte des considérations en matière de protection de la vie privée, afin que nous puissions profiter de cet outil tout en protégeant nos droits fondamentaux.

Mme Pam Damoff: Avez-vous découvert à quelles fins ces ministères utilisaient cet outil? J'ai entendu parler de fraude, de harcèlement... Êtes-vous au courant d'autres circonstances dans lesquelles cet outil a été utilisé?

M. Philippe Dufresne: Oui, nous avons obtenu des renseignements à ce sujet. Certains d'entre eux l'ont utilisé dans le cadre de dispositions législatives antipourriel. D'autres l'ont utilisé dans le cadre d'enquêtes sur la cybercriminalité ou sur des questions de sécurité nationale. D'autres l'ont utilisé aux fins de l'impôt ou dans le cadre d'enquêtes en matière d'impôt. D'autres l'ont utilisé pour des raisons liées à la Loi sur la concurrence, à l'environnement, à la pêche, à des programmes de conservation, à des enquêtes sur les transports et à d'autres types de questions qui relèvent de la compétence des ministères. Trois ministères les ont utilisés pour mener des enquêtes à l'interne.

Mme Pam Damoff: Il ne me reste que 15 secondes. Pourriez-vous nous faire part de vos recommandations, le cas échéant, par écrit?

M. Philippe Dufresne: Oui, certainement.

Mme Pam Damoff: Je vous remercie.

Le président: Je vous remercie, madame Damoff et monsieur Dufresne.

[Français]

Monsieur Villemure, vous avez maintenant la parole pour six minutes.

M. René Villemure: Merci, monsieur le président.

J'aimerais proposer une motion, qui a été envoyée au Comité dans les deux langues officielles.

Considérant que la *Loi sur la protection des renseignements personnels* n'a pas été révisée depuis 1983,

Considérant que le comité ETHI a demandé une telle révision dans ses précédents rapports,

Que le Comité demande au gouvernement du Canada de procéder à la révision de la *Loi sur la protection des renseignements personnels*.

Le président: Merci, monsieur Villemure.

La motion est recevable. Cela dit, j'y vois un seul problème: le Comité n'a pas le pouvoir de demander au gouvernement de faire quelque chose; il peut seulement lui recommander de le faire. Je vous suggère donc de remplacer le mot « demande » par « recommandation ».

• (1220)

M. René Villemure: J'accepte d'écrire « recommande », mais il est important de préciser que cette recommandation a déjà été faite. Ici, nous ne faisons que la réitérer. Dans cette optique, je n'y vois pas de problème.

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

Monsieur Dufresne, je vous demande de rester pendant que nous discutons de la motion.

Quelqu'un veut-il intervenir sur la motion proposée par M. Villemure?

[Traduction]

Madame Khalid, je vois que vous avez levé la main. Vous avez la parole.

Mme Iqra Khalid: Je vous remercie, monsieur le président.

Certains de mes collègues sont en ligne et j'aimerais savoir si nous pouvons suspendre la séance pendant deux minutes pour me permettre de m'entretenir avec eux.

Le président: Je suis seulement en train de confirmer avec la greffière que la motion a été envoyée à tout le monde.

Je vais autoriser une brève suspension de deux minutes pour que vous puissiez en discuter, si personne n'y voit d'inconvénient.

Je vous remercie.

• (1220)

(Pause)

• (1223)

Le président: La séance reprend. Comme je l'ai dit, un courriel a été envoyé au sujet de la motion proposée par M. Villemure.

Madame Damoff, vous avez la parole pour parler de la motion.

Mme Pam Damoff: Je vous remercie, monsieur le président.

Comme le savent les membres du Comité, le gouvernement est en train de réviser la Loi sur la protection des renseignements personnels.

J'aimerais donc demander au député pourquoi nous devrions adopter une motion sur ce sujet plutôt que de l'inclure dans le rapport. Nous venons de commencer l'étude aujourd'hui. J'aimerais savoir si le député pourrait nous dire pourquoi nous ne pourrions pas tout simplement formuler une recommandation à ce sujet dans le rapport que nous rédigerons dans le cadre de cette étude.

Le président: Oui, je pense que c'est une question qui mérite d'être posée. M. Villemure et moi-même venons d'avoir une discussion en aparté sur le sujet, mais je vais laisser M. Villemure s'expliquer.

[Français]

Monsieur Villemure, veuillez s'il vous plaît expliquer votre point de vue à Mme Damoff et au Comité.

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

Le Comité a recommandé à de nombreuses reprises une révision de la Loi sur la protection des renseignements personnels. Le Conseil du Trésor a annoncé en 2021 une révision de la Loi. Dans le cadre de cette révision, je crois qu'on est en train de consulter chaque Canadien un par un, ce qui peut prendre du temps. Le Comité a déjà recommandé des choses. Ce matin, nous avons avec

nous M. Dufresne qui, je crois, nous a dit un million de fois que cela doit être fait. En conséquence, nous devons insister sur le besoin de ramener le sujet à l'ordre du jour, parce que la recommandation ne semble pas porter ou être prise au sérieux.

C'est comme n'importe quelle autre chose: éventuellement, l'accumulation devient intenable. On a eu les outils intégrés. Il y a eu d'autres études sur la vie privée. Chaque fois, la recommandation de réviser la Loi est revenue. Éventuellement, la somme de tout cela va mener à quelque chose.

Au Comité, je crois que nous sommes d'accord, puisque nous avons entendu les mêmes témoignages. Le commissaire ici présent et son prédécesseur nous ont dit la même chose: il y a péril en la demeure. L'intelligence artificielle va venir changer la donne complètement. Même si l'outil change et que la Loi de 1983 demeure, il reste que le monde a changé.

Après en avoir fait la recommandation n° 1 dans deux rapports, nous devons appuyer une telle motion dans l'intérêt public. J'insiste une fois de plus.

• (1225)

Le président: Merci, monsieur Villemure.

[Traduction]

Madame Damoff, vous avez la parole.

Mme Pam Damoff: Je vous remercie beaucoup. Le gouvernement prend la situation au sérieux. C'est la raison pour laquelle cet examen est en cours, mais je comprends que l'honorable député souhaite faire connaître son point de vue et je le remercie également des connaissances qu'il apporte sur cette question.

Je l'en remercie.

Devons-nous modifier la motion, monsieur le président, comme vous l'avez suggéré un peu plus tôt?

Le président: Je pense que M. Villemure l'a déjà fait.

[Français]

C'est correct.

[Traduction]

Mme Pam Damoff: Quel est son libellé actuel?

Le président: Nous remplaçons le mot « demande » par le mot « recommande », car comme je l'ai dit plus tôt, le Comité n'a pas le pouvoir de demander au gouvernement de faire quoi que ce soit. Nous pouvons cependant recommander au gouvernement de faire quelque chose, et je pense que c'est l'intention de M. Villemure dans ce cas-ci.

Je vois M. Erskine-Smith.

Vous avez la parole pour parler de la motion.

M. Nathaniel Erskine-Smith: Je ne suis pas opposé à ce que le gouvernement révisé la Loi. Je pense que j'étais membre du comité de l'éthique lorsque nous en avons fait la recommandation au cours de la première législature à laquelle j'ai participé, de 2015 à 2019.

Cependant, j'aimerais poser une question à M. Villemure. N'est-ce pas un peu inutile et une perte de temps? Le gouvernement ne va-t-il pas simplement répéter ce qu'il a dit en réponse au dernier rapport? Ne serait-il pas plus efficace de l'inclure, comme pour le témoignage du commissaire, dans un bref rapport et d'insister sur le fait que nous l'avons recommandé à de nombreuses reprises, de mentionner ces nombreuses fois et de dire que nous demandons une mise à jour de la Loi et pas seulement une révision? Il semble que ce soit ici une faible version de ce que nous pourrions faire.

Le président: Je vous remercie, monsieur Erskine-Smith.

Si la motion est adoptée, elle pourra être inscrite dans le procès-verbal du Comité et, bien entendu, lorsque nous travaillerons à l'ébauche du rapport une fois que nous aurons entendu tous les témoins, elle pourra être mise en évidence dans le rapport. En attendant, c'est ce que M. Villemure a proposé et ce dont nous discutons pour l'instant.

Je vous remercie de vos observations à ce sujet, monsieur Erskine-Smith.

[Français]

Sur la motion proposée par M. Villemure et modifiée, y a-t-il consensus?

Des voix: D'accord.

(La motion modifiée est adoptée.)

[Traduction]

Le président: Monsieur Dufresne, madame Ives, merci encore de votre patience.

Monsieur Villemure, vous avez la parole pour six minutes.

Allezloiy, s'il vous plaît.

[Français]

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

Merci à mes collègues.

Monsieur le commissaire, j'aimerais que vous nous parliez justement de l'impact de l'intelligence artificielle sur la protection des renseignements personnels, et si c'est un élément que l'on doit considérer dans le cas des 13 organismes qui, pour le moment, font l'objet d'une enquête.

M. Philippe Dufresne: L'intelligence artificielle est un élément fondamental qui touche la vie privée des Canadiennes et des Canadiens, ainsi que des citoyens partout dans le monde. Cet été, mes homologues du G7 et moi avons émis une résolution lors de notre réunion annuelle, dans laquelle nous rappelons l'importance de protéger la vie privée. Nous avons rappelé l'application des lois existantes, ainsi que la nécessité de les moderniser et de considérer les effets de l'intelligence artificielle, et ce, dès leur conception.

Au mois d'octobre, mes homologues provinciaux et territoriaux et moi avons aussi émis une déclaration. Le 7 décembre, nous avons organisé un symposium, ici, à Ottawa, avec nos homologues étrangers, et nous avons émis une déclaration sur l'intelligence artificielle à la lumière des principes canadiens concernant la vie privée. Nous avons aussi fait part de nos attentes, notamment pour ce qui est des notions d'autorité juridique, d'objectifs appropriés, de nécessité, de proportionnalité, de reddition de comptes et de limites sur l'utilisation. Nous avons appliqué cette lentille à l'intelligence artificielle.

Dans le contexte des outils dont il est question aujourd'hui, je n'ai pas eu d'information disant qu'il est question d'intelligence artificielle, mais c'est une possibilité qu'il faut toujours garder à l'esprit. Dans le contexte de l'emploi, la résolution que l'Assemblée mondiale pour la protection de la vie privée a émise l'automne dernier parlait précisément de l'utilisation de l'intelligence artificielle en matière d'emploi, notamment pour gérer le rendement du personnel et pour recruter des gens.

Je ne peux pas en parler en détail, mais, en ce moment, nous étudions une plainte contre OpenAI pour déterminer si la compagnie se conforme ou non à la Loi pour ce qui est de ChatGPT, et sur les recommandations à faire si ce n'est pas le cas.

Il y a aussi toutes les questions entourant les données qui sont utilisées pour entraîner l'intelligence artificielle. Quelles sont les protections et les limites? L'Organisation de coopération et de développement économiques a mené une étude sur l'intelligence artificielle avec des ministres du G7, et les trois risques les plus importants qui ont été déterminés étaient la désinformation ou la mésinformation, les effets sur les droits d'auteur et les effets sur la vie privée. C'est donc un sujet extrêmement important.

La semaine dernière, le Commissariat à la protection de la vie privée du Canada a annoncé ses trois priorités stratégiques. La première est d'optimiser et de moderniser les structures du Commissariat pour que nous ayons le plus grand impact possible. La deuxième est de s'assurer que la technologie respecte la vie privée et qu'on peut en bénéficier tout en la balisant. La troisième est la protection de la vie privée des enfants, un autre élément extrêmement important. D'ailleurs, cette semaine, les dirigeants des médias sociaux se sont présentés devant le Congrès américain pour parler de leur impact sur les enfants. Ces priorités sont au cœur de ce que nous faisons.

• (1230)

M. René Villemure: Au-delà de vos trois priorités, diriez-vous que le Commissariat est maintenant équipé pour évaluer les répercussions de l'intelligence artificielle sur la vie privée?

M. Philippe Dufresne: Nous sommes bien équipés pour le faire. Nous avons un laboratoire technologique, mais il faut que nous poursuivions nos efforts. En effet, la situation évolue, et les organisations que nous réglementons ont certainement beaucoup plus de ressources que nous. Il faut que nous continuions dans cette direction, et nous allons mettre l'accent là-dessus.

M. René Villemure: Vous avez mentionné ChatGPT, donc l'intelligence artificielle générative. Est-ce que vous voyez un impact différent sur la vie privée depuis l'arrivée de l'intelligence artificielle générative ou, au contraire, est-ce que cela n'a fait qu'accélérer l'impact actuel?

M. Philippe Dufresne: Nous voyons que c'est de plus en plus utilisé. Nous voyons l'impact potentiel de la fausse information ou du fait de prendre l'image de quelqu'un pour lui faire faire certaines choses. L'intelligence artificielle générative soulève donc énormément de risques pour la vie privée et la dignité, et les défis sont plus grands, bien sûr.

M. René Villemure: Récemment, l'image d'un humoriste américain décédé en 2008 a été utilisée dans un nouveau spectacle. La vidéo n'est pas parfaite, mais la voix, le ton et le propos sont les mêmes. On y parle de problèmes actuels.

Diriez-vous qu'une telle utilisation est une violation de la vie privée?

M. Philippe Dufresne: Je pense qu'il s'agit potentiellement d'une violation, oui, puisqu'on utilise des données personnelles à des fins qui ne sont pas acceptables ni acceptées. Cela a un impact sur la dignité et cela soulève toutes sortes de risques et de questions. C'est donc un élément sur lequel il faut se pencher.

Il est important que les gens sachent tout ce qu'on peut faire avec leurs données personnelles. Cela renforce l'importance de les protéger. Si une personne a accès à ma voix et à la façon dont je parle, elle peut, grâce à l'intelligence artificielle, faire beaucoup de choses qui peuvent me faire du tort ou faire du tort à d'autres.

M. René Villemure: Selon le Forum économique mondial, la désinformation ou la mésinformation et la vie privée sont les préoccupations principales.

Serait-il possible d'obtenir les déclarations publiques que vos homologues du G7 et du Canada et vous avez faites l'an dernier?

M. Philippe Dufresne: Tout à fait. Ces déclarations sont publiques et affichées sur notre site Web. Je pourrai les faire parvenir au Comité, incluant celles qui portent sur la question de l'emploi et sur la question de la protection de la vie privée des enfants.

M. René Villemure: Merci beaucoup.

Je sais que ma collègue Mme Khalid est très préoccupée par la protection de la vie privée des enfants.

Le président: Merci, messieurs Villemure et Dufresne.

[Traduction]

Monsieur Green, vous disposez de six minutes.

Allezloiy, s'il vous plaît.

M. Matthew Green: Merci.

Je suis content de pouvoir revenir sur la dimension humaine de la surveillance. Nous nous sommes certainement penchés sur la question lorsque nous avons parlé de l'IA et de son utilisation pour la surveillance sur des appareils dans le cadre de la réponse à l'audit. Nous avons couvert — de façon convaincante, je pense — la manière dont la partialité est ancrée.

Ce qui me frappe dans ce contexte, c'est la surveillance qui s'apparente davantage aux systèmes de télévision en circuit fermé. Vous savez que dans des pays comme le Royaume-Uni et les États-Unis, où l'utilisation de tels systèmes de vidéosurveillance est très répandue, on a constaté qu'ils étaient très susceptibles d'être utilisés à mauvais escient, simplement en raison de la nature humaine. L'Union américaine pour les libertés civiles a signalé quatre façons dont ces systèmes sont susceptibles de donner lieu à des abus. Ainsi, aux fins de ce tour, je veux que vous teniez simplement compte de ce contexte.

Premièrement, on parle d'abus de nature criminelle. Dans des cas comme celui-ci, évidemment, s'il s'agit du gouvernement fédéral, l'aspect légal pourrait indiquer qu'il s'agit d'un acte criminel si c'est fait sans mandat et en dehors du cadre du travail. Deuxièmement, il y a l'utilisation de façon clandestine, si nous parlons de la GRC, de la défense nationale ou peut-être plus spécifiquement de nos services de sécurité nationale et de la manière dont ils effectuent la surveillance en ligne. Je ne dis pas qu'ils le font, mais c'est une possibilité. Troisièmement, il y a les abus commis par des institutions, les excès, l'approche descendante, et la manière dont le gouvernement instaure la surveillance du public constitue un risque important. On a constaté que le recours à des systèmes de télévision en

circuit fermé était non seulement inefficace, mais aussi, selon certains, excessif.

Je pense que ce qui me préoccupe le plus, compte tenu de la nature sensible des renseignements, c'est l'utilisation abusive à des fins personnelles et c'est pourquoi j'ai essayé de savoir de qui l'on parle exactement. Je pense que, pour tous ceux qui ne connaissent pas les technologies de l'information, nous avons une idée de qui se trouve du côté des TI.

Seriez-vous d'accord pour dire que les intentions ou les possibilités, les susceptibilités, lorsqu'on parle d'abus relativement aux systèmes de télévision en circuit fermé ou au monde analogique devraient également être prises en compte dans le monde numérique, en particulier en ce qui concerne l'IA et les technologies et l'accès complet aux données et aux renseignements personnels des gens? Peut-on le supprimer?

● (1235)

M. Philippe Dufresne: Oui.

Je pense que plus la technologie est puissante, plus sa portée est large, plus il faut être prudent et prendre des mesures de protection de la vie privée et plus il y a de considérations liées à la protection de la vie privée dont il faut tenir compte. C'est ce qu'on appelle la proportionnalité. Étant donné que l'on dispose d'un outil plus intrusif, il est nécessaire de mettre en place un mécanisme de protection plus rigoureux.

Je suis d'accord avec vous. L'aspect humain est important. Nous parlons de la protection de la vie privée en tant que principe. C'est un droit fondamental, sans contredit, mais cela signifie que, sur le plan humain, nous sommes tous moins libres si nous perdons notre vie privée, si nous vivons en ayant l'impression d'être constamment scrutés à la loupe et que les gens peuvent voir ce que nous faisons, à quel endroit nous le faisons, ce que nous achetons...

Je pense à l'un des premiers articles portant sur la protection de la vie privée qui s'intitule *Right to Privacy*. On donnait l'exemple, dans les années 1800, d'une personne qui collectionnait des pierres et on disait que la vie privée signifiait qu'on avait le droit de le faire sans que tous les gens du village ne puissent savoir quelles pierres on achète. C'est une information qui vous appartient.

Évidemment, de nos jours, nous constatons que ce principe a encore plus de poids. Cela fait partie de notre liberté et de notre individualité et nous devons donc veiller à ce que... Il ne s'agit pas de dire qu'on ne peut pas utiliser la technologie — on le peut —, mais il faut le faire en tenant compte de la question de la vie privée.

M. Matthew Green: Je voudrais revenir plus précisément sur les évaluations des facteurs relatifs à la vie privée. Avez-vous un moyen de savoir qui a accès à l'information contenue dans la technologie sur laquelle vous vous penchez? C'est ma première question.

Ensuite, existe-t-il présentement des mécanismes législatifs ou des mécanismes de reddition de comptes qui permettraient de déterminer la fréquence à laquelle quelqu'un le fait? Par exemple, savoir que j'ai accès à ce type d'outils de, ce que j'appellerai, « voyeurisme numérique », est une chose, mais ne pas savoir combien de fois je l'utilise en est une tout autre. Dans le cas du système de télévision en circuit fermé, le voyeurisme est devenu une réalité lorsque c'est devenu... En ce qui concerne les services de police, des éléments prouvaient qu'on y avait recours pour suivre des femmes, obtenir des renseignements sur sa partenaire ou son ex-femme, et ainsi de suite.

Y a-t-il actuellement des mécanismes de protection contre ces outils technologiques, qui sont peut-être approuvés dans des ministères ou organismes, mais pour lesquels on n'a pas réellement de contrôle?

M. Philippe Dufresne: Il existe toute une série d'outils. Il y a les banques de renseignements personnels du gouvernement qui indiquent ce que nous possédons comme information, les raisons et les objectifs qui y sont associés. C'est une sorte de divulgation proactive. Les évaluations des facteurs relatifs à la vie privée sont un autre moyen de nous informer de manière proactive au sujet de cette utilisation. Encore une fois, il s'agit de s'assurer qu'un nombre limité de personnes ont accès aux renseignements...

M. Matthew Green: Mais il est clair que vous ne le savez pas — non?

M. Philippe Dufresne: Nous ne le savons pas tant qu'on ne nous a pas fourni l'information.

M. Matthew Green: L'autre aspect qui me préoccupe à propos de la reddition de comptes... Il semble que ce soit le cas avec le gouvernement... et encore une fois, je vais attribuer cela à la nature humaine et ne pas nécessairement en faire une attaque partisane. Je dirai simplement qu'il arrive souvent que les gens ne rendent des comptes que lorsqu'ils se font prendre. Ce qui me préoccupe actuellement, c'est que nous ne parlons que d'une douzaine d'organisations.

Si vous consultez vos comptes de courriel, vous constaterez que j'ai rédigé une motion. Je vais parler de la motion pendant que vous regardez vos comptes, car le répertoire des organisations et des intérêts fédéraux comprend 137 ministères ou organisations de la fonction publique fédérale: 23 ministères, 3 organismes de service, 17 établissements publics, 15 organismes ministériels et 12 organismes de service spéciaux. C'est assez vaste. Ce qui me pose problème, c'est que nous ne parlons actuellement que de 12 d'entre eux. Nous ne savons pas, au sein de ce comité, qui utilise les outils et quelle est la portée de l'utilisation.

Ce que je voudrais faire, c'est proposer une motion:

Que, dans le cadre de l'étude sur l'utilisation par les institutions gouvernementales d'outils capables d'extraire des données personnelles de téléphones et d'ordinateurs, le comité écrive à chaque ministère et organisme fédéral qui n'est pas déjà cité dans l'étude et leur demande de confirmer s'ils ont acheté ou s'ils ont accès à des logiciels utilisés pour extraire des informations de dispositifs électroniques; et demander que la réponse soit envoyée au comité au plus tard 10 jours ouvrables après réception.

● (1240)

Le président: Merci, monsieur Green.

Comme l'a dit M. Green, la motion a été envoyée à tout le monde par courriel avant qu'il ne la présente. La motion a été proposée. Je vais l'accepter parce qu'elle a trait à notre sujet d'étude d'aujourd'hui.

Y a-t-il des observations au sujet de la motion de M. Green? Non.

(La motion est adoptée.)

Le président: Merci, monsieur Green. Votre temps de parole est écoulé. La motion a été adoptée.

Les deux prochaines interventions seront de cinq minutes et les deux dernières, de deux minutes et demie.

Je sais que tout le monde est au courant que M. Barrett présentera une motion à la fin de la réunion. Nous devrions régler la question assez rapidement.

Nous allons commencer les interventions de cinq minutes avec M. Kurek.

Allez-y, monsieur Kurek.

M. Damien Kurek: Merci, monsieur le président.

Je pense que l'adoption de cette motion met en évidence une préoccupation à propos des inconnues. Lorsque j'ai vu qu'Environnement et Changement climatique...

Je représente une région qui compte beaucoup d'agriculteurs. Des agriculteurs qui reçoivent du courrier de différents ordres de gouvernement m'ont fait part de leurs inquiétudes. Ils ne savent pas ce que sont certaines exigences, ce qu'elles signifient ou ce qu'elles comprennent. On leur demande d'accepter des choses sans qu'ils connaissent nécessairement tous les détails.

Le fait qu'il y ait des questions sans réponse montre à quel point il est important d'aller au fond des choses. Si cela a une incidence sur le droit à la vie privée des Canadiens, nous devons certainement être très clairs à ce sujet.

Il y a aussi le fait qu'Environnement et Changement climatique Canada a récemment publié une offre d'emploi dans laquelle il recherchait des agents de l'autorité. En quoi cela consiste-t-il? Les agriculteurs de ma circonscription se le demandent. Je ne manquerais pas de poser ces questions.

Monsieur le commissaire, vous avez décrit certaines des préoccupations. Si possible, j'aimerais vous demander de fournir quelques exemples de ce qui doit être changé pour que vous puissiez non seulement disposer des outils qu'il faut, mais aussi garantir que le cadre législatif est en place de sorte que nous puissions obtenir des réponses aux questions que nous avons posées — et tous les partis l'ont fait. Pour le moment, il n'est pas possible de les obtenir en raison de lacunes ou parce que les cadres réglementaires ne vont pas assez loin au Canada.

Pourriez-vous nous donner un aperçu de ces éléments?

M. Philippe Dufresne: Certainement. Merci.

Je recommanderais qu'il soit obligatoire de procéder à une évaluation des facteurs relatifs à la vie privée lorsque de nouveaux outils puissants peuvent avoir une incidence sur la vie privée des Canadiens. Si l'on s'éloigne de la notion même de programme, si un nouvel outil modifie le contexte, il faut envisager une évaluation des facteurs relatifs à la vie privée.

Je recommanderais de préciser que le Commissariat doit être consulté et informé avant que de nouvelles technologies ne soient déployées et que des modifications ne soient apportées à de nouveaux programmes — et non pas après coup. En fait, ce ne serait pas seulement le jour même, mais suffisamment à l'avance pour que nous puissions contribuer de façon utile.

Je recommanderais que l'on modernise la Loi sur la protection des renseignements personnels pour y inclure les notions de nécessité et de proportionnalité. Il s'agit de se demander si, bien que le but puisse être important, on se limite au minimum lorsqu'il s'agit des renseignements recueillis.

Il s'agit là de points essentiels.

Je reprends la recommandation du Comité concernant la protection de la vie privée dès la conception. Par ailleurs, il va de soi que le pouvoir de rendre des ordonnances pour le Commissariat est un élément important qui devrait également être inclus dans la nouvelle loi.

• (1245)

M. Damien Kurek: Oui. Il est regrettable que nous devions même envisager le pouvoir de rendre des ordonnances. J'aurais espéré que l'on présume que la protection de la vie privée est importante pour les Canadiens. Manifestement, et je siége au sein de ce comité depuis environ quatre ans, ce n'est pas le cas.

Qu'il s'agisse du pouvoir de rendre des ordonnances ou de cas de non-conformité, je me demande, concernant les sanctions, la proportionnalité... Quelle solution recommanderiez-vous pour garantir qu'en fin de compte, il ne s'agisse pas simplement d'une recommandation ou d'un mandat du Conseil du Trésor dont on ne tient pas compte, sans conséquence pour ceux qui font fi de ce qui pourrait constituer le droit à la vie privée des Canadiens?

M. Philippe Dufresne: Dans le contexte du secteur privé, j'ai clairement fait une recommandation concernant le pouvoir de rendre des ordonnances et l'imposition d'amendes s'il y a lieu — et ce n'est pas parce que je veux imposer des amendes. Je veux que ce soit possible de le faire parce que cela incite le décideur à réfléchir.

Au sein du gouvernement, j'aimerais que ce ne soit pas nécessaire pour les ministères, mais c'est toujours...

M. Damien Kurek: Avez-vous des chiffres? C'est juste par curiosité. Vous avez parlé d'amendes. S'agit-il d'une sanction administrative? Quelle est l'idée?

M. Philippe Dufresne: Dans le secteur privé, on parle d'un pourcentage. Je pense que c'est 10 % dans une année pour une organisation, ou 10 ou 15 millions de dollars — j'oublie les détails —, mais c'est de cet ordre.

Pour les ministères, c'est peut-être différent, mais il y a aussi les sociétés d'État. Nous avons rendu une décision sur Postes Canada dans notre rapport annuel. Nous attendons que Postes Canada s'y conforme. Elle ne l'a pas fait — jusqu'à présent.

Ce type d'outil est utile.

Le président: Merci, monsieur Kurek.

Merci, monsieur Dufresne.

Monsieur Erskine-Smith, vous avez la parole pour cinq minutes. En commençant la dernière fois, vous avez salué les analystes. Je sais que vous avez été membre de ce comité pendant trois ans et, au nom des analystes, je vais vous rendre la pareille.

Des voix: Ha, ha!

Le président: Ils voulaient que je le fasse. Je sais qu'ils n'allaient pas le faire, mais je l'ai fait.

Allez-y, pour cinq minutes.

M. Nathaniel Erskine-Smith: Merci, monsieur Brassard.

Merci, madame Savoie. Merci, monsieur Thibodeau.

Monsieur le commissaire, mon collègue, Matthew Green, a fait un parallèle avec les systèmes de télévision en circuit fermé. Il n'y a donc aucun doute quant à des cas avérés d'abus dans l'utilisation de ces systèmes. Il s'agit bien sûr d'une technologie différente, et des technologies différentes posent des défis différents.

Il me semble que dans ce cas particulier, avec cette technologie particulière, vous devez tenir compte de deux aspects qui peuvent poser problème. Il s'agit tout d'abord de savoir si la fouille d'un appareil est justifiée — c'est le premier élément — et ensuite de savoir si les principes du caractère raisonnable, de la nécessité et de la proportionnalité sont respectés lorsqu'il s'agit de la portée de la fouille de l'appareil.

Cela vous semble-t-il exact?

M. Philippe Dufresne: Oui. Je suis d'accord avec vous.

M. Nathaniel Erskine-Smith: D'accord. Cela dit, parmi les ministères qui ont déployé cette technologie... Vous avez dit qu'un des 13 ne l'a pas fait, mais pour ce qui est des ministères et organismes qui l'ont fait, combien de fois l'a-t-on utilisée?

M. Philippe Dufresne: Combien de fois a-t-elle été utilisée? Il faudra peut-être que je trouve cette information pour vous. Je pense que certains d'entre eux ont dit qu'ils l'avaient utilisée à quelques reprises seulement, et d'autres ne l'ont pas précisé. Je n'ai pas ces détails. Je peux voir si nous pouvons vous les fournir ultérieurement.

M. Nathaniel Erskine-Smith: D'accord.

Par ailleurs, combien de fois y a-t-on eu recours sans qu'une autorisation judiciaire ait été obtenue? Dans un certain nombre des cas dont vous parlez, qu'il s'agisse des pêches ou de la GRC, il me semble que ce ne sont pas vraiment les employés qui sont en cause. On le fait aux fins des enquêtes qui sont menées. C'est peut-être la même chose avec l'ARC.

Ce qui me frappe, c'est que dans le cas d'un organisme d'enquête qui respecte une certaine procédure établie pour ses mécanismes régulateurs d'investigation, le recours à un tel outil s'inscrit probablement dans les paramètres de cette procédure en place. Vous allez faire votre travail en ce qui concerne la protection de la vie privée, mais je serai un peu moins préoccupé s'il y a effectivement une procédure établie déjà intégrée au processus d'examen. Cependant, si on a recours à l'outil à d'autres fins qu'une enquête — par exemple, pour l'application d'une loi ou le respect d'une procédure existante —, nous pourrions avoir certaines inquiétudes. Ces considérations vous semblent-elles justes?

• (1250)

M. Philippe Dufresne: Oui, et c'est l'un des aspects que j'examinerais également dans le cadre d'une évaluation des facteurs relatifs à la vie privée. Il faut obtenir ces détails. Quel est le contexte? Quelles sont les mesures de protection en place?

M. Nathaniel Erskine-Smith: D'accord, et il me semble que, dans le cadre de votre enquête et des questions que vous poseriez dans ce contexte, vous devriez entrer en contact... Je vois bien où M. Green veut en venir avec sa motion, mais il serait préférable, car vous êtes en fait mieux placé pour le faire, que ce soit vous qui communiquiez avec ces autres organisations pour leur poser exactement les mêmes questions et nous faire rapport par la suite. Nous pourrions chapeauter votre travail parce que nous avons des pouvoirs dont vous ne disposez pas. Vous avez toutefois le temps et la volonté de vous acquitter minutieusement d'une telle tâche en posant toutes les questions nécessaires.

Dans le cadre de cette démarche, il serait notamment bon de demander combien de fois on a eu recours à cet outil en l'absence d'une autorisation judiciaire ou d'une autre autorisation découlant des pouvoirs d'enquête existants — ce qui nous ramène à ma question précédente — et s'il y a eu des cas où on a perquisitionné des appareils gouvernementaux dans le contexte d'une enquête interne portant par exemple sur le harcèlement. C'est une autre catégorie de cas pour laquelle il me semble tout à fait logique que cette technologie soit employée.

Par ailleurs, il y a aussi lieu de s'interroger sur la portée de la perquisition, et il faudrait que vous posiez des questions à ce sujet. S'il y a des inquiétudes à cet égard, je vous prierais de bien vouloir nous en faire part. Il serait bon de savoir si cette technologie est utilisée dans d'autres cas pouvant être préoccupants, qui ne font pas l'objet d'une enquête et qui, à première vue, semblent le justifier.

Vous allez donc nous répondre ultérieurement quant au nombre d'utilisations, mais j'aurais une dernière question dans l'immédiat. En ce qui concerne la portée de la perquisition électronique, il serait bon, dans le cadre de vos évaluations des facteurs relatifs à la vie privée effectuées en collaboration avec ces organismes... M. Barrett a souligné à juste titre la distinction à faire entre le nuage et un appareil appartenant au gouvernement. Vous répondez comme il se doit que chacun a des attentes raisonnables quant à la protection de sa vie privée, et que ces attentes peuvent varier en fonction des équipements utilisés. On s'assure de répondre à ces attentes raisonnables en appliquant des critères de nécessité et de proportionnalité.

J'aimerais beaucoup savoir si des ministères, dans le cadre de leurs enquêtes, ont dépassé les limites de la nécessité et de la proportionnalité. Fouillent-ils inutilement dans le nuage aux fins des enquêtes sur le harcèlement? Font-ils des recherches dans l'information sur la santé? C'est là une préoccupation fondamentale pour notre comité. De telles choses se sont-elles vraiment produites?

Si votre enquête vous permet de mettre au jour de réelles préoccupations à ce sujet, nous vous serions reconnaissants de bien vouloir en informer le Comité.

M. Philippe Dufresne: Merci.

J'ai pris note de tous ces éléments. Nous ferons un suivi pour vous répondre ultérieurement.

M. Nathaniel Erskine-Smith: Merci.

Le président: Merci, monsieur Dufresne.

Merci, monsieur Erskine-Smith.

[Français]

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

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

Monsieur le commissaire, nous avons entendu beaucoup de recommandations aujourd'hui, que nous allons évidemment prendre en considération. Cependant, si on regarde un peu en avant, qu'est-ce qui s'en vient? Qu'est-ce qu'on n'a pas vu? À quoi le Comité devrait-il prêter attention afin de mieux voir venir les choses? Le futur se précipite vers nous assez rapidement depuis quelques années, et j'ai l'impression que nous sommes toujours un pas en retard, voire plusieurs pas en retard.

Si le Comité voulait prendre un peu d'avance, quelles seraient vos recommandations?

M. Philippe Dufresne: La semaine dernière, quand nous avons publié notre plan stratégique, que je transmettrai au Comité, nous avons parlé de trois priorités.

La première est de moderniser le commissariat et de maximiser son impact avec une nouvelle loi. À tout le moins, s'il n'y a pas de nouvelle loi, il faudra se demander comment protéger le plus possible la vie privée.

La deuxième est la technologie. Il faut dépasser la technologie ou, au moins, avancer à la même vitesse qu'elle. C'est un gros défi, parce que nous voyons que la technologie est de plus en plus adoptée. Les gens aiment la technologie, l'utilisent et en voient les bénéfices. Il faut donc s'assurer que leur vie privée est prise en compte et protégée.

La troisième est la vie privée des enfants. Cette question présente beaucoup de défis. Il y a les répercussions sur leur santé mentale, sur leur réputation et sur leurs données. Il y a donc du travail à faire là-dessus et nous mettrons l'accent sur ces éléments.

Sur le plan international, il y a encore la question de la protection des données dans le contexte des flux de données transfrontaliers.

En bref, en mettant l'accent sur la technologie et en essayant d'anticiper ses tendances et ses utilisations, ainsi qu'en se concentrant sur les enfants et leur vie privée, on mettra l'accent sur l'avenir. C'est pour cela que, de notre côté, nous allons mettre l'accent sur ces éléments. Cependant, nous sommes également ouverts aux recommandations que le Comité pourrait nous faire sur d'autres questions.

Pour ma part, je m'attarde à une grande thématique: on veut bénéficier de l'innovation et de la technologie, parce que cela amène beaucoup d'avantages dans de nombreux domaines. M. Green a parlé de l'utilisation de la technologie dans le domaine de la santé, et il y a aussi les sports et la musique. De bonnes choses viennent de cela et il ne faut pas tout refuser. Toutefois, je ne veux pas que les Canadiennes et les Canadiens aient à choisir entre profiter de la technologie et conserver leur vie privée. Il faut éviter d'avoir à choisir et éviter que le fardeau repose complètement sur les épaules des individus. Je veux que ces derniers sentent et sachent que les institutions sont là pour les protéger et pour les conseiller.

• (1255)

Le président: Monsieur Villemure, si j'ai bien compris, M. Green vous a donné son temps de parole. Vous pouvez donc continuer pendant deux minutes et demie.

M. René Villemure: C'est parfait, monsieur le président, et merci.

Monsieur le commissaire, pour vous tenir au courant de ces nouvelles tendances, allez-vous par exemple au Consumer Electronics Show à Las Vegas? Comment faites-vous?

M. Philippe Dufresne: Nous sommes très actifs au sein de certaines communautés au Canada et à l'international pour nous tenir au courant. Certaines communautés de protection de la vie privée impliquent aussi l'industrie, qui présente ses produits. Au commissariat, nous avons un laboratoire technologique qui s'informe et se tient au courant pour rester à la fine pointe de la technologie.

C'est justement la deuxième priorité du commissariat. Nous ne voulons pas dire aux gens de ne pas toucher à la technologie parce que c'est dangereux et qu'elle a des répercussions sur la vie privée. Nous voulons nous-mêmes pouvoir l'utiliser de façon responsable pour ensuite expliquer à ces gens comment l'utiliser tout en respectant la vie privée. Ainsi, les gens n'auront aucune raison de ne pas l'utiliser, parce que nous savons que c'est possible. Nous ne faisons pas que dire qu'il faut le faire, nous le faisons nous-mêmes.

M. René Villemure: Lorsqu'il est question de la vie privée des enfants, évidemment, on veut prévenir les abus, les blessures et les sévices potentiels. Pour un jeune d'aujourd'hui dont la première photo a été prise dans l'utérus de sa mère, la vie privée est un concept flou. On fait beaucoup passer le loisir avant cette protection-là. La plupart des jeunes donnent souvent la même réponse, que vous entendez sûrement aussi, c'est-à-dire qu'ils n'ont rien à cacher. On sait cependant qu'il en est autrement.

Qu'est-ce que cela prend pour éduquer la prochaine génération de manière à ce qu'elle comprenne bien l'importance et la valeur de la vie privée?

M. Philippe Dufresne: Vous avez raison. Les jeunes connaissent très bien la technologie, probablement mieux que les moins jeunes, parfois. Cependant, il faut renforcer cette sensibilité à la vie privée, non seulement chez les jeunes, mais aussi chez leurs parents. Je pense au surpartage parental, par exemple, lorsque ce sont souvent les parents qui vont publier de l'information sur les médias sociaux. Les enfants en subissent longtemps les conséquences par la suite. Il faut donc que le système juridique soit prêt à protéger leur information et il faut avoir ces conversations-là.

Je pense aussi aux écoles. Je voudrais qu'il y ait des cours obligatoires pour sensibiliser les jeunes à la protection de la vie privée. L'éducation étant évidemment de compétence provinciale, nous travaillons de près avec nos homologues. Nous avons émis une déclaration commune sur la protection de la vie privée des jeunes en interpellant l'industrie, les gouvernements et les éducateurs et éducatrices à ce sujet.

Au même titre qu'on enseigne la sécurité aux enfants et qu'on leur dit par exemple de ne pas monter dans une voiture avec un étranger, on devrait leur dire que, même s'il peut y avoir des choses vraiment intéressantes, il faut penser aux conséquences.

M. René Villemure: La semaine dernière, une concitoyenne me disait que sa fille de 9 ans faisait de la gymnastique et qu'elle était allée sur YouTube pour regarder des vidéos de gymnastique. D'une chose à l'autre, cependant, elle était tombée sur des images pornographiques de jeunes gymnastes. Pour qu'on l'attire, sa vie privée a dû être compromise. Cela m'a quand même choqué que cette petite fille qui regardait des vidéos de gymnastique olympique se soit retrouvée ailleurs sur Internet. Il est donc important d'agir pour protéger la vie privée des enfants et de faire de la sensibilisation.

Merci beaucoup.

Le président: Merci, monsieur Villemure et monsieur Dufresne.

Ceci met fin à notre séance aujourd'hui.

Monsieur Dufresne, au nom du Comité, des Canadiennes et des Canadiens, je vous remercie de votre témoignage d'aujourd'hui sur cette question très importante.

Je remercie également Mme Ives.

[Traduction]

Nous avons quelques questions à régler.

Je vais d'abord donner la parole à M. Barrett.

Monsieur Barrett, vous avez une motion que vous aimeriez présenter de vive voix au Comité. Je crois comprendre que vous avez parlé aux membres du Comité et qu'ils sont tous d'accord. Si vous présentez la motion, nous pourrions en discuter si cela est nécessaire.

À vous la parole, monsieur Barrett.

M. Michael Barrett: Voulez-vous que je lise la motion et que j'en parle très brièvement, monsieur le président?

Le président: Je vous en prie.

M. Michael Barrett: La motion qui a été distribuée est la suivante. Je propose:

Que le Comité envoie une lettre de condoléances à la famille de l'ancienne commissaire à l'éthique Mary Dawson en reconnaissance de ses années de service public, et que le Comité fasse rapport à la Chambre de ses condoléances à la suite de son décès.

Le président: Très bien.

La motion a été présentée et je la déclare recevable.

Nous vous écoutons, monsieur Barrett.

M. Michael Barrett: Mary Dawson est décédée le 24 décembre 2023. J'aimerais vous faire part de quelques faits marquants à son sujet pour mettre en lumière l'importance de cette motion. Je suis reconnaissant à mes collègues d'avoir accepté que le Comité en soit saisi et qu'elle fasse l'objet d'un rapport à la Chambre.

Elle n'a pas été seulement commissaire à l'éthique. Elle a eu un parcours tout à fait remarquable. Des pans très importants de notre histoire sont marqués de son empreinte. C'est notamment elle qui a rédigé la Loi sur l'accès à l'information, la Loi sur la protection des renseignements personnels, la Loi canadienne sur la santé, la Loi sur les langues officielles, la Loi sur la concurrence, la Loi sur les douanes et la Loi sur les jeunes contrevenants.

Elle a été nommée membre du Conseil de la Reine en 1978 et est devenue première conseillère législative adjointe au début des années 1980, en plus d'avoir été sous-ministre déléguée de la Justice pendant près de deux décennies. Elle était particulièrement fière de son travail constitutionnel, notamment en tant que rédactrice de la version officielle des documents pour le rapatriement de la Constitution en vertu de la Loi constitutionnelle de 1982 et pour la Charte des droits et libertés.

Il s'agit là d'un résumé succinct, incomplet et non exhaustif des services exceptionnels qu'elle a rendus à notre pays à titre de fonctionnaire et de commissaire chargée de trancher en faisant la part des choses. J'estime qu'un bon commissaire à l'éthique parvient à garder sur le qui-vive les députés de tous les partis, et c'est exactement ce que Mme Dawson arrivait à faire.

Le Canada a été bien servi par ses contributions, et je remercie mes collègues d'avoir bien voulu prendre cette motion en considération.

• (1300)

Le président: Je tiens à vous remercier, monsieur Barrett, pour cette motion que vous avez proposée et pour ces bonnes paroles concernant Mme Dawson.

Je n'ai jamais eu l'occasion de traiter avec elle directement. Il est toutefois certain que l'on ne peut pas assumer la présidence d'un comité comme le nôtre sans être bien conscient de la contribution inestimable de cette femme à notre pays, non seulement à titre de commissaire à l'éthique, mais, comme vous l'avez mentionné, dans le cadre de toute une carrière au sein de la fonction publique. Quel apport phénoménal!

Merci pour la motion.

Madame Damoff, nous vous écoutons au sujet de cette proposition.

Mme Pam Damoff: Merci, monsieur le président.

Très brièvement, je veux remercier mon collègue d'avoir présenté cette motion — que nous nous empressons bien sûr d'appuyer —, mais aussi pour sa description très éloquente de la feuille de route de Mme Dawson.

Je n'ai pas non plus eu l'occasion de travailler avec elle ou de la connaître, mais je pense que vous avez bien résumé sa contribution au bénéfice des Canadiens. Je tiens simplement à vous remercier d'avoir présenté cette motion. Nous souhaitons aussi transmettre nos condoléances à ses proches.

Le président: Merci, madame Damoff.

Elle figure certes au rang des véritables légendes.

Est-ce que quelqu'un d'autre voudrait intervenir? Je présume avoir votre consentement au sujet de cette motion...

M. Matthew Green: Non seulement y a-t-il consentement, mais il est unanime.

(La motion est adoptée.)

Le président: Merci d'avoir présenté cette motion, monsieur Barrett.

[Français]

Nous devons adopter une dernière motion. C'est au sujet du budget de l'étude sur laquelle nous travaillons en ce moment, soit l'utilisation par le gouvernement fédéral d'outils technologiques permettant d'extraire des données sur des appareils mobiles et des ordinateurs.

Monsieur Villemure, si le Comité veut adopter le budget de l'étude, le montant s'élève à 16 500 \$. Cela inclut les dépenses des témoins, les vidéoconférences, le rapport de travail et les autres dépenses.

Plaît-il au Comité d'adopter cette motion?

Des voix: D'accord.

(La motion est adoptée).

[Traduction]

Le président: Madame Khalid, vous avez encore une question dont nous pourrions traiter rapidement?

Mme Iqra Khalid: Je suis désolée, mais ce sera très bref. J'aimerais savoir quel est l'échéancier pour l'ébauche de rapport faisant suite à notre étude sur les médias sociaux.

Le président: Peut-être pourrais-je demander à nos analystes de vous éclairer sur ce point. Du même coup, vous me faites penser qu'il y a un autre élément dont nous devons traiter.

Mme Alexandra Savoie (attachée de recherche auprès du comité): L'ébauche de rapport a été rédigée. Elle est en cours de traduction. Nous devrions pouvoir la distribuer à la mi-février. Je pense que la date officielle que nous avons jusqu'à présent est le 19. Si nous pouvons la fournir plus tôt, nous le ferons, mais ce devrait être le 19 au plus tard, c'est-à-dire au début la semaine de relâche, de sorte que vous aurez une semaine pour l'examiner.

Le président: D'accord.

J'aurais une dernière question à régler. L'autre jour, nous avons adopté une motion visant à envoyer une lettre au Comité de la procédure et des affaires de la Chambre ainsi qu'au Bureau de régie interne. La lettre a été rédigée. Elle est en cours de traduction. Nous devrions être en mesure de la transmettre aux membres du Comité d'ici la fin de la journée. On avait demandé de pouvoir examiner cette lettre pour éventuellement y apporter des modifications. Conformément à ce dont nous avons convenu la dernière fois, c'est une lettre très courte qui n'aborde aucune question de fond.

Comme il ne semble pas y avoir d'autres points dont nous devrions traiter maintenant, je vais vous souhaiter un bon après-midi et une excellente fin de semaine.

Merci à notre greffière, à nos analystes et à nos techniciens pour la réunion d'aujourd'hui.

La séance est levée.

Publié en conformité de l'autorité
du Président de la Chambre des communes

PERMISSION DU PRÉSIDENT

Les délibérations de la Chambre des communes et de ses comités sont mises à la disposition du public pour mieux le renseigner. La Chambre conserve néanmoins son privilège parlementaire de contrôler la publication et la diffusion des délibérations et elle possède tous les droits d'auteur sur celles-ci.

Il est permis de reproduire les délibérations de la Chambre et de ses comités, en tout ou en partie, sur n'importe quel support, pourvu que la reproduction soit exacte et qu'elle ne soit pas présentée comme version officielle. Il n'est toutefois pas permis de reproduire, de distribuer ou d'utiliser les délibérations à des fins commerciales visant la réalisation d'un profit financier. Toute reproduction ou utilisation non permise ou non formellement autorisée peut être considérée comme une violation du droit d'auteur aux termes de la Loi sur le droit d'auteur. Une autorisation formelle peut être obtenue sur présentation d'une demande écrite au Bureau du Président de la Chambre des communes.

La reproduction conforme à la présente permission ne constitue pas une publication sous l'autorité de la Chambre. Le privilège absolu qui s'applique aux délibérations de la Chambre ne s'étend pas aux reproductions permises. Lorsqu'une reproduction comprend des mémoires présentés à un comité de la Chambre, il peut être nécessaire d'obtenir de leurs auteurs l'autorisation de les reproduire, conformément à la Loi sur le droit d'auteur.

La présente permission ne porte pas atteinte aux privilèges, pouvoirs, immunités et droits de la Chambre et de ses comités. Il est entendu que cette permission ne touche pas l'interdiction de contester ou de mettre en cause les délibérations de la Chambre devant les tribunaux ou autrement. La Chambre conserve le droit et le privilège de déclarer l'utilisateur coupable d'outrage au Parlement lorsque la reproduction ou l'utilisation n'est pas conforme à la présente permission.

Aussi disponible sur le site Web de la Chambre des communes à l'adresse suivante :
<https://www.noscommunes.ca>

Published under the authority of the Speaker of
the House of Commons

SPEAKER'S PERMISSION

The proceedings of the House of Commons and its committees are hereby made available to provide greater public access. The parliamentary privilege of the House of Commons to control the publication and broadcast of the proceedings of the House of Commons and its committees is nonetheless reserved. All copyrights therein are also reserved.

Reproduction of the proceedings of the House of Commons and its committees, in whole or in part and in any medium, is hereby permitted provided that the reproduction is accurate and is not presented as official. This permission does not extend to reproduction, distribution or use for commercial purpose of financial gain. Reproduction or use outside this permission or without authorization may be treated as copyright infringement in accordance with the Copyright Act. Authorization may be obtained on written application to the Office of the Speaker of the House of Commons.

Reproduction in accordance with this permission does not constitute publication under the authority of the House of Commons. The absolute privilege that applies to the proceedings of the House of Commons does not extend to these permitted reproductions. Where a reproduction includes briefs to a committee of the House of Commons, authorization for reproduction may be required from the authors in accordance with the Copyright Act.

Nothing in this permission abrogates or derogates from the privileges, powers, immunities and rights of the House of Commons and its committees. For greater certainty, this permission does not affect the prohibition against impeaching or questioning the proceedings of the House of Commons in courts or otherwise. The House of Commons retains the right and privilege to find users in contempt of Parliament if a reproduction or use is not in accordance with this permission.

Also available on the House of Commons website at the following address: <https://www.ourcommons.ca>