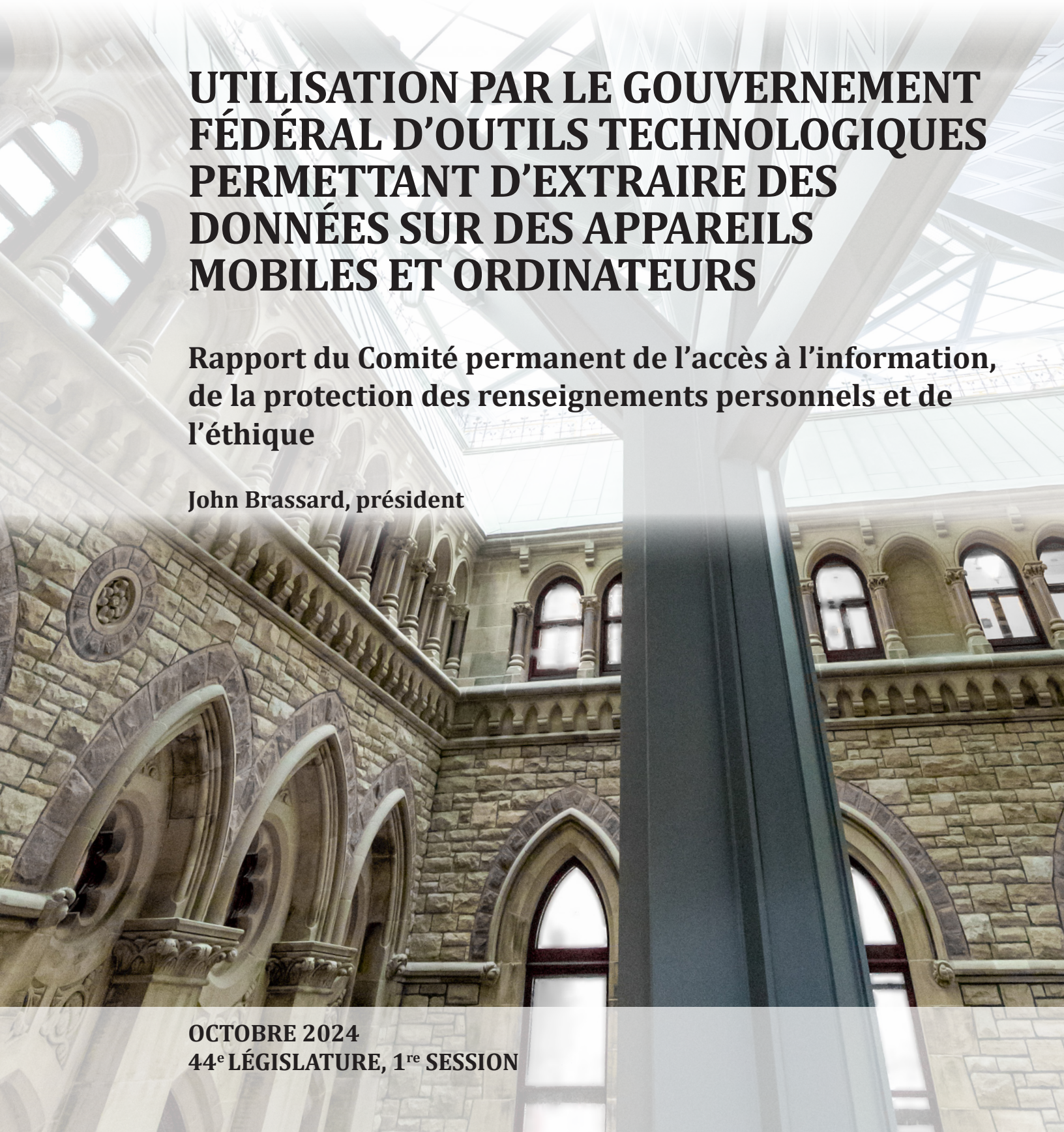
CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA



UTILISATION PAR LE GOUVERNEMENT FÉDÉRAL D'OUTILS TECHNOLOGIQUES PERMETTANT D'EXTRAIRE DES DONNÉES SUR DES APPAREILS MOBILES ET ORDINATEURS

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

John Brassard, président

OCTOBRE 2024
44e LÉGISLATURE, 1re SESSION

UTILISATION PAR LE GOUVERNEMENT FÉDÉRAL D'OUTILS TECHNOLOGIQUES PERMETTANT D'EXTRAIRE DES DONNÉES SUR DES APPAREILS MOBILES ET ORDINATEURS

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

Le président
John Brassard

OCTOBRE 2024

44e LÉGISLATURE, 1re SESSION

AVIS AU LECTEUR

Rapports de comités présentés à la Chambre des communes

C'est en déposant un rapport à la Chambre des communes qu'un comité rend publiques ses conclusions et recommandations sur un sujet particulier. Les rapports de fond portant sur une question particulière contiennent un sommaire des témoignages entendus, les recommandations formulées par le comité et les motifs à l'appui de ces recommandations.

COMITÉ PERMANENT DE L'ACCÈS À L'INFORMATION, DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET DE L'ÉTHIQUE

PRÉSIDENT

John Brassard

VICE-PRÉSIDENTS

Darren Fisher

René Villemure

MEMBRES

Parm Bains

Michael Barrett

Frank Caputo

Michael Cooper

Matthew Green

Anthony Housefather

Iqra Khalid

Brenda Shanahan

AUTRES DÉPUTÉS QUI ONT PARTICIPÉ

Pam Damoff

Nathaniel Erskine-Smith

L'hon. Mona Fortier

Lori Idlout

Mike Kelloway

Damien C. Kurek

Stephanie Kusie

Viviane Lapointe

Eric Melilo

Glen Motz

L'hon. Robert Oliphant

Francesco Sorbara

GREFFIÈRE DU COMITÉ

Nancy Vohl

BIBLIOTHÈQUE DU PARLEMENT

Recherche et éducation

Alexandra Savoie, analyste

Maxime-Olivier Thibodeau, analyste

LE COMITÉ PERMANENT DE L'ACCÈS À L'INFORMATION, DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET DE L'ÉTHIQUE

a l’honneur de présenter son

TREIZIÈME RAPPORT

Conformément à l'article 108(3)h) du Règlement, le Comité a étudié l'utilisation par le gouvernement fédéral d'outils technologiques permettant d'extraire des données sur des appareils mobiles et ordinateurs et a convenu de faire rapport de ce qui suit :

TABLE DES MATIÈRES

SOMMAIRE

En février 2024, le Comité a entamé une étude portant sur l'utilisation, par certaines institutions fédérales, d'outils technologiques permettant d'extraire des données sur des appareils mobiles et ordinateurs, soit des outils de criminalistique numérique.

Compte tenu de la capacité de ces outils, certains intervenants ont soulevé des craintes concernant la possibilité qu'ils soient utilisés de façon abusive, s'interrogeant particulièrement sur l'utilisation potentielle de ces outils dans le cadre d'enquêtes administratives internes impliquant des employés fédéraux.

Le commissaire à la protection de la vie privée du Canada, pour sa part, a noté que dans une ère où la technologie change de plus en plus la manière dont les renseignements personnels sont recueillis, utilisés et communiqués, les institutions fédérales doivent porter une attention particulière aux répercussions de leurs activités sur la vie privée, notamment en s'assurant de respecter les principes de nécessité et de proportionnalité. Un moyen d'évaluer les répercussions sur la vie privée d'un programme ou d'une activité est d'en faire une évaluation des facteurs relatifs à la vie privée avant sa mise sur pied.

Les représentants des institutions fédérales qui ont comparu devant le Comité ont insisté sur le fait que leur utilisation d'outils de criminalistique numérique est nécessaire pour faire face aux changements technologiques des dernières années. Ces outils leur permettent d'obtenir les preuves requises pour s'acquitter de leur mandat. Ces preuves ne se trouvent plus dans des endroits physiques, mais plutôt dans les classeurs des temps modernes : les appareils mobiles et ordinateurs.

La question de savoir si une évaluation des facteurs relatifs à la vie privée devrait être faite dès qu'un nouvel outil technologique puissant est nouvellement utilisé ou qu'elle soit plutôt faite au niveau du programme a fait l'objet de beaucoup de discussions durant l'étude. Le Comité a constaté qu'il semble y avoir un manque de clarté à cet égard dans la *Directive sur les évaluations des facteurs relatifs à la vie privée*. La présidente du Conseil du Trésor a d'ailleurs indiqué que cette directive sera mise à jour afin de clarifier les exigences relatives à ces évaluations.

À la lumière des témoignages entendus, du mémoire qu'il a reçu et des documents supplémentaires que lui ont fournis certains témoins, le Comité formule neuf nouvelles recommandations et réitère cinq recommandations du rapport qu'il a publié en 2022 concernant les outils d'enquête sur appareil utilisés par la Gendarmerie royale du

Canada, dont l'inclusion d'une obligation de faire des évaluations des facteurs relatifs à la vie privée dans la *Loi sur la protection des renseignements personnels*.

LISTE DES RECOMMANDATIONS

À l'issue de leurs délibérations, les comités peuvent faire des recommandations à la Chambre des communes ou au gouvernement et les inclure dans leurs rapports. Les recommandations relatives à la présente étude se trouvent énumérées ci-après.

Recommandation 1

Recommandation 2

Recommandation 3

Recommandation 4

Recommandation 5

CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

UTILISATION PAR LE GOUVERNEMENT FÉDÉRAL D'OUTILS TECHNOLOGIQUES PERMETTANT D'EXTRAIRE DES DONNÉES SUR DES APPAREILS MOBILES ET ORDINATEURS

INTRODUCTION

Contexte

Le 29 novembre 2023, Radio-Canada a publié un article indiquant que des contrats obtenus en vertu de la *Loi sur l'accès à l'information* avaient révélé que des outils permettant d'extraire les données personnelles d'appareils mobiles ou d'ordinateurs sont utilisés par au moins 13 ministères et agences du gouvernement fédéral[1]. L'article indiquait également que le recours à cette technologie n'avait pas fait l'objet d'une évaluation des facteurs relatifs à la vie privée (ÉFVP), malgré la *Directive sur l'évaluation des facteurs relatifs à la vie privée* (*Directive sur l'ÉFVP*) du Conseil du Trésor du Canada (Conseil du Trésor)[2]. Une version anglaise de l'article a été publiée le 1er décembre 2023[3].

Le 6 décembre 2023, en raison de ce reportage, le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes (le Comité) a adopté une motion unanime visant à entreprendre une étude portant sur l'utilisation par le gouvernement fédéral d'outils technologiques permettant d'extraire des données sur des appareils mobiles et ordinateurs.

Entre le 1er février et le 21 mars 2024, le Comité a tenu 6 réunions publiques au cours desquelles 32 témoins ont été entendus. Le Comité a invité les institutions visées par l'article ayant motivé l'étude pour qu'elles puissent clarifier la situation. Il a invité d'autres témoins pertinents, dont la présidente du Conseil du Trésor. Il a aussi reçu un mémoire. Le Comité remercie tous ceux et celles qui ont participé à l'étude.

1 Brigitte Bureau, *Des outils potentiellement intrusifs utilisés par au moins 13 ministères fédéraux*, *Radio-Canada*, 29 novembre 2023.

2 *Ibid*.

3 Brigitte Bureau, *Tools capable of extracting personal data from phones being used by 13 federal departments, documents show*, *CBC News*, 1er décembre 2023.

Structure du rapport

Le rapport est divisé en quatre chapitres. Le chapitre 1 fait un survol du cadre législatif et des politiques et directives du Conseil du Trésor qui s'appliquent à la protection des renseignements personnels dans le secteur public fédéral. Le chapitre 2 explique la distinction entre les outils permettant d'extraire les données personnelles d'appareils mobiles ou d'ordinateurs ou « outils de criminalistique numérique » et les logiciels espions[4]. Il fait aussi un survol de ce que les représentants des institutions fédérales qui ont comparu devant le Comité ont dit à l'égard de leur utilisation d'outils de criminalistique numérique et de la tenue d'une ÉFVP.

Le chapitre 3 aborde la protection de la vie privée des employés d'institutions fédérales et la possibilité que des outils de criminalistique numérique soient utilisés à des fins d'enquêtes administratives internes. Enfin, le chapitre 4 se penche sur les mesures, législatives ou autres, qui permettraient au gouvernement du Canada de mieux encadrer l'utilisation d'outils technologiques puissants par des institutions fédérales.

Les recommandations du Comité se trouvent à la toute fin des chapitres 3 et 4. Deux annexes à la fin du rapport fournissent des informations additionnelles sur l'utilisation d'outils de criminalistique numérique par des institutions fédérales.

CHAPITRE 1 : PROTECTION DES RENSEIGNEMENTS PERSONNELS ET INSTITUTIONS FÉDÉRALES

Loi sur la protection des renseignements personnels

La *Loi sur la protection des renseignements personnels* (LPRP) s'applique à la protection des renseignements personnels dans le secteur public fédéral. Elle prévoit les règles pour la collecte, l'utilisation et la communication des renseignements personnels qui relèvent d'une institution fédérale. La LPRP ne contient aucune disposition exigeant la tenue d'une ÉFVP.

4 En français, le terme utilisé pour décrire les outils permettant d'extraire des renseignements personnels d'appareils ou ordinateurs faisant l'objet de l'étude du Comité varie. Le terme le plus fréquemment utilisé en anglais par les témoins est « digital forensic tool », qui se traduit par « outil de criminalistique numérique ».

Politiques et directives du Conseil du Trésor

En plus de la LPRP, le Conseil du Trésor approuve aussi des politiques, directives, normes et lignes directrices destinées aux institutions du gouvernement du Canada. Ces dernières ne sont pas juridiquement contraignantes, mais on s'attend à ce qu'elles soient respectées par les institutions fédérales. Certaines concernent la protection des renseignements personnels.

Politique sur la protection de la vie privée

La *Politique sur la protection de la vie privée* du Conseil du Trésor fournit une orientation aux institutions fédérales pour assurer le respect de la LPRP. Elle vise entre autres à ce que la population canadienne soit convaincue que ses renseignements personnels qui relèvent des institutions fédérales soient protégés et gérés efficacement[5]. Au sujet de cette politique, Philipe Dufresne, le commissaire à la protection de la vie privée du Canada, a rappelé que l'article 4.2.2 prévoit qu'une institution fédérale doit :

> 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[6].

Une autre exigence de la *Politique sur la protection de la vie privée*, est d'assurer, lorsqu'approprié, la réalisation, la mise à jour et la publication d'ÉFVP pertinentes[7].

Directive sur l'évaluation des facteurs relatifs à la vie privée

La *Directive sur l'ÉFVP* du Conseil du Trésor a comme objectif de s'assurer qu'un examen prudent des risques liés à la vie privée dans le contexte de la création, de la collecte ou du traitement de renseignements personnels dans le cadre d'activités ou de programmes gouvernementaux est fait. Elle prévoit que les ÉFVP sont effectuées d'une

5 Conseil du Trésor du Canada, *Politique sur la protection de la vie privée*, art. 3.1.

6 *Ibid*., art. 4.2.2.

7 *Ibid*., art. 4.2.4.

manière proportionnée au niveau de risque déterminé avant l'établissement d'une activité ou d'un programme ou après des changements importants à ceux-ci[8].

M. Dufresne a expliqué que la *Directive sur l'ÉFVP* prévoit que les institutions fédérales doivent effectuer une ÉFVP lorsque :

- des renseignements personnels peuvent être utilisés dans le cadre d'un processus décisionnel touchant directement un individu;
- 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 administratives;
- 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
- 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[9].

M. Dufresne a noté que lorsque le Commissariat à la protection de la vie privée du Canada (Commissariat) a des entretiens avec les institutions fédérales, les ÉFVP sont présentées comme un processus efficace de gestion des risques. Elles permettent de cerner et d'atténuer les risques qui pèsent sur la vie privée dans l'ensemble des programmes et des services à l'intérieur desquels des renseignements personnels sont recueillis et utilisés.

En ce qui concerne la décision de réaliser une ÉFVP, M. Dufresne a noté que dans une ère où la technologie change de plus en plus la manière dont les renseignements personnels sont recueillis, utilisés et communiqués, les institutions fédérales doivent porter une attention particulière aux répercussions de leurs activités sur la vie privée et les évaluer soigneusement afin d'établir si une ÉFVP est nécessaire et à quel moment. Il a reconnu que l'utilisation d'un nouvel outil n'entraîne pas toujours le besoin de réaliser une ÉFVP. Cela dépend de la manière dont le nouvel outil sera utilisé et de l'usage qui sera fait des renseignements recueillis.

8 Conseil du Trésor du Canada, *Directive sur l'évaluation des facteurs relatifs à la vie privée*, arts. 5.1 et 5.2.

9 *Ibid*., art. 6.3.1 et 6.3.2.

La *Directive sur l'ÉFVP* indique à l'article 3.3 que « 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 ». M. Dufresne a concédé qu'il faut de la discipline pour faire une ÉFVP. Il faut étudier le programme et répondre à certaines questions. Il pense donc qu'il est tout à fait légitime que des critères permettent de déterminer si elle est nécessaire ou non. Toutefois, il estime qu'elles ne sont pas « gourmandes en ressources au point de ne pas valoir la peine d'être faites ».

Enfin, M. Dufresne a rappelé que les ÉFVP sont obligatoires selon les politiques du Conseil du Trésor, mais pas une obligation prévue dans la LPRP. Il a toutefois reconnu qu'une directive est plus qu'un simple encouragement.

Directive sur les pratiques relatives à la protection de la vie privée

La *Directive sur les pratiques relatives à la protection de la vie privée* fournit une orientation aux institutions fédérales sur la façon de mettre en œuvre des pratiques efficaces de protection de la vie privée. Elle a comme objectif de faciliter la mise en œuvre et la publication de pratiques solides et uniformes en matière de gestion de la vie privée et de protection des renseignements personnels tout au long de leur cycle de vie. Par exemple, elle impose des exigences en matière de formation des employés des institutions fédérales sur la protection des renseignements personnels ou à l'égard du processus de création des fichiers de renseignements personnels[10].

Fichiers de renseignements personnels

Certains témoins ont fait référence aux fichiers de renseignements personnels (FRP)[11]. Les FRP sont des descriptions de renseignements personnels relevant d'une institution fédérale, qui décrivent la manière dont ils sont recueillis, utilisés, divulgués, conservés ou éliminés dans le cadre de l'administration d'un programme ou d'une activité de cette institution[12].

10 Conseil du Trésor du Canada, *Directive sur les pratiques relatives à la protection de la vie privée*, art. 4.

11 Chambre des communes, Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (ETHI), *Témoignages*, 44e législature, 1e session : Aaron McCrorie (vice-président, Renseignement et exécution de la loi, Agence des services frontaliers du Canada [ASFC]); Pierre Pelletier (dirigeant principal de l'information, ministère des Ressources naturelles [RNCan]).

12 Conseil du Trésor du Canada, *Fichiers de renseignements personnels ordinaires*.

Au terme du paragraphe 10(1) de la LPRP, le responsable d'une institution fédérale doit veiller à ce que tous les renseignements personnels qui relèvent de son institution et qui sont ou ont été utilisés à des fins administratives soient versés dans des FRP.

M. Dufresne a spécifié que les FRP indiquent ce que l'institution fédérale en question possède comme information et les raisons et objectifs associés à cette collecte d'information. Cela représente une sorte de divulgation proactive.

CHAPITRE 2 : UTILISATION D'OUTILS DE CRIMINALISTIQUE NUMÉRIQUE PAR DES INSTITUTIONS FÉDÉRALES

Distinction entre logiciel espion et outil de criminalistique numérique

M. Dufresne a expliqué que les outils de criminalistique numérique servent à extraire et à examiner un grand nombre de fichiers stockés sur des ordinateurs portables, des disques durs ou des appareils mobiles. Ces outils sont généralement utilisés dans le cadre d'enquêtes ou d'analyses techniques, qui requièrent un accès physique à l'appareil, et qui sont habituellement utilisés dans des circonstances où le propriétaire de l'appareil est informé[13].

En ce qui concerne les logiciels espions, M. Dufresne a rappelé que, contrairement aux outils de criminalistique numérique, ils sont généralement installés à distance sur l'appareil d'une personne et à l'insu de celle-ci. De tels logiciels peuvent recueillir secrètement des renseignements personnels, comme les touches utilisées sur le clavier d'un ordinateur ou l'historique de navigation sur le Web. Ils sont souvent utilisés de façon illégale ou non autorisée.

À l'égard des capacités des outils de criminalistique numérique, M. Dufresne a indiqué qu'ils peuvent, dans certains cas, déverrouiller un téléphone intelligent ou accéder au contenu d'ordinateurs portables ou tablettes protégés par des mots de passe. Toutefois, il a réitéré le fait que ces outils ne sont pas utilisés à distance, c'est-à-dire que l'enquêteur doit avoir l'appareil en main. C'est de cette manière qu'ils se distinguent des logiciels espions[14].

13 ETHI, *Témoignages*, Philippe Dufresne (commissaire à la protection de la vie privée, Commissariat à la protection de la vie privée du Canada).

14 ETHI, *Témoignages*, Dufresne.

M. Dufresne a aussi expliqué que les outils de criminalistique numérique peuvent être utilisés à plusieurs fins, comme pour faire une analyse de métadonnées d'un fichier, déterminer quand un système d'exploitation a été modifié où récupérer des données supprimées. Selon lui, ces outils d'enquête sont utiles et peuvent contribuer à la préservation de l'intégrité d'une chaîne de preuves[15].

M. Dufresne a d'ailleurs affirmé que le Commissariat lui-même a déjà utilisé des outils de criminalistique numérique dans le cadre d'enquêtes sur certaines allégations d'atteinte à la vie privée pour établir la nature, l'envergure et la portée d'un incident. Il ne considère donc pas que leur utilisation est complètement inacceptable et qu'il faudrait y mettre un terme. Il faut toutefois tenir compte des considérations en matière de protection de la vie privée afin de tirer les bénéfices d'un tel outil tout en protégeant nos droits fondamentaux.

Parmi les représentants d'institutions fédérales qui ont comparu devant le Comité, seuls ceux de la Gendarmerie royale du Canada (GRC) ont dit utiliser des outils d'enquête sur appareil ou « outils d'enquête embarquée » (OEE), dans certaines circonstances, dans le cadre d'enquêtes criminelles. Les OEE permettent d'intercepter des renseignements sur un appareil à l'insu de son propriétaire. Le logiciel peut être déployé sur des dispositifs ou des réseaux informatiques par un accès à distance, proche ou rapproché, permettant ainsi la surveillance électronique[16]. Les OEE diffèrent des outils de criminalistique numérique faisant l'objet de l'étude du Comité.

En effet, M. Dufresne a noté que les outils d'enquête sur appareil, qui sont utilisés pour obtenir des données secrètement et à distance à partir d'appareils ciblés, sont un exemple de logiciel espion. Toutefois, il a rappelé que dans le contexte de l'application de la loi, une autorisation judiciaire est requise avant de pouvoir utiliser des outils d'enquête sur appareil. Ainsi, dans ce cas, ces outils sont légaux et appropriés[17]. Ils ne sont pas utilisés de façon illégale ou non autorisée. Par ailleurs, Bryan Larkin, sous commissaire, Services de police spécialisés, Gendarmerie royale du Canada, a confirmé qu'en ce qui concerne les OEE, une ÉFVP a été complétée par la GRC en septembre 2023 et soumise au commissaire à la protection de la vie privée et au Conseil du Trésor[18].

---

15 ETHI, *Témoignages*, Dufresne.

16 ETHI, *Outils d'enquête sur appareil utilisés par la Gendarmerie royale du Canada et enjeux liés*, rapport, 44e législature, 1e session, novembre 2022, pp. 20-21; Gendarmerie royale du Canada (GRC), *Entrevue avec un expert en surveillance électronique sur les défis liés à la collecte de preuves*, 27 juillet 2022.

17 ETHI, *Témoignages*, Dufresne.

18 GRC, *Lettre au Comité*, 21 décembre 2023; GRC, *Évaluation des facteurs relatifs à la vie privée de l'Équipe d'accès secret et d'interception*.

À noter que le Comité a mené une étude sur les outils d'enquête sur appareil utilisés par la Gendarmerie royale du Canada en 2022 et qu'il a présenté un rapport à la Chambre des communes. Le présent rapport se concentre sur les outils de criminalistique numérique et non pas sur les OEE.

Faits saillants concernant l'utilisation d'outils de criminalistique numérique par des institutions fédérales

Les représentants de douze des treize institutions fédérales identifiées dans le reportage qui a motivé l'étude du Comité ont comparu durant l'étude[19].

Achat d'outils de criminalistique numérique

De façon générale, les représentants d'institutions fédérales qui ont comparu devant le Comité ont indiqué que l'achat d'outils de criminalistique numérique a été nécessaire pour faire face aux changements technologiques des dernières années. Les preuves qu'ils doivent obtenir pour s'acquitter de leur mandat ne se trouvent plus toujours dans des endroits physiques, mais plutôt sur des appareils mobiles ou ordinateurs.

Par exemple, Brent Napier, directeur général par intérim, Conservation et Protection, ministère des Pêches et Océans (Pêches et Océans Canada), a indiqué qu'auparavant, la récolte et la déclaration des ressources halieutiques s'effectuaient sous format papier. Aujourd'hui, les pêcheurs ont intégré de nouvelles technologies à leurs opérations de pêches, comme les traceurs de cartes et les journaux de bord électroniques. Il a dit que les appareils électroniques sont les classeurs des temps modernes et que pour y avoir accès, il faut des outils technologiques.

Donald Walker, responsable de la mise en application de la loi chez Environnement et Changement climatique Canada (ECCC), a noté que « pour récupérer l'information que nous pouvions auparavant trouver dans un classeur, nous devions dorénavant avoir accès à des appareils électroniques pour recueillir les preuves nécessaires à la poursuite d'une enquête ».

Aaron McCrorie, vice-président, Renseignement et exécution de la loi, de l'Agence des services frontaliers du Canada (ASFC), a noté qu'à une autre époque l'ASFC aurait demandé à un serrurier d'ouvrir une boîte contenant des reçus. Aujourd'hui, les reçus électroniques d'une affaire liée à la contrebande d'armes à feu entre les frontières se trouvent dans un téléphone cellulaire ou un ordinateur. Il faut donc un autre moyen

19 Affaires mondiales Canada a été invitée, mais n'a pas comparu.

d'avoir accès à cette information et la traduire sous une forme qui peut être utilisée devant un tribunal.

À la question de savoir si l'utilisation de ces outils est vraiment nécessaire et proportionnelle aux objectifs poursuivis, plusieurs témoins ont dit que sans ces outils, ils ne seraient pas en mesure d'avoir accès aux preuves nécessaires pour remplir leur mandat[20]. Ils les considèrent donc nécessaires.

Utilisation des outils de criminalistique numérique

M. Dufresne a confirmé ne pas avoir vu, dans les réponses des treize institutions fédérales avec qui il a communiqué, un objectif inapproprié ou une utilisation inappropriée des outils de criminalistique numérique qui pourrait soulever des inquiétudes[21]. Elles semblent toutes utiliser ces outils pour remplir leur mandat, appliquer leur loi habilitante ou mener des enquêtes. Il a précisé que certains ministères peuvent utiliser des outils de criminalistique numérique pour mener des enquêtes sur les infractions à la loi commise par des Canadiens ou Canadiennes[22].

Les représentants d'institutions fédérales ont indiqué que les appareils mobiles ou ordinateurs doivent être physiquement en leur possession pour qu'un outil de criminalistique numérique puisse être utilisé sur eux[23]. Plusieurs ont confirmé qu'un accès physique aux appareils technologiques est obtenu dans le cadre d'une enquête, par l'entremise d'une ordonnance judiciaire ou d'un mandat de perquisition, qui circonscrit quels renseignements peuvent être recueillis, ou en vertu des pouvoirs

20 ETHI, *Témoignages* : Steven Harroun (chef de l'application de la Conformité et enquêtes, Conseil de la radiodiffusion et des télécommunications canadiennes [CRTC]); McCrorie (ASFC); France Gratton (commissaire adjointe, Opérations et programmes correctionnels, Service correctionnel du Canada [SCC]); Nicolas Gagné (surintendant, GRC); Bryan Larkin (sous-commissaire, Services de police spécialisés, GRC); Donald Walker (responsable de la mise en application de la loi, ministère de l'Environnement [ECCC]); Hannah Rogers (directrice générale, Application de la loi en environnement, ECCC); Kathy Fox (présidente, Bureau de la Sécurité des transports du Canada [BST]); Eric Ferron (directeur général, Direction des enquêtes criminelles, Direction générale des programmes d'observation, Agence du revenu du Canada [ARC]).

21 ETHI, *Témoignages*, Dufresne.

22 ETHI, *Témoignages*, Dufresne.

23 ETHI, *Témoignages* : Gagné (GRC); McCrorie (ASFC); Gratton (SCC); Ferron (ARC); Harroun (CRTC); Larkin (GRC); Scott Jones (président, Services partagés Canada [SPC]); Fox (BST).

conférés par une loi[24]. Certains ont rappelé au Comité que seuls les renseignements expressément visés par l'ordonnance judiciaire ou le mandat de perquisition sont communiqués à l'enquêteur par l'expert en criminalistique numérique[25].

Les représentants des institutions fédérales ont aussi confirmé que leurs institutions n'utilisent pas de logiciel espion sur la population canadienne en général ni n'effectuent de surveillance de masse[26]. Plusieurs témoins ont spécifié qu'aucun outil technologique n'est laissé sur l'appareil pour faire de la surveillance à long terme une fois l'enquête de l'institution fédérale terminée et que l'appareil est retourné à son propriétaire[27].

Plusieurs représentants d'institutions fédérales ont aussi expliqué que les outils de criminalistique numérique ne sont utilisés que par un nombre limité d'analystes en matière d'informatique judiciaire au sein de leur institution[28]. Un grand nombre d'entre eux ont soulevé le fait que les données recueillies sur des appareils technologiques saisis sont conservées dans des endroits sécurisés, par exemple dans des laboratoires spécialisés et sur des ordinateurs qui ne sont pas connectés au réseau ou à l'Internet[29].

En ce qui concerne l'utilisation potentielle d'outils de criminalistique numérique sur les appareils mobiles ou ordinateurs fournis aux employés gouvernementaux, quelques représentants d'institutions fédérales ont confirmé qu'ils peuvent le faire dans le cadre

---

24 ETHI, *Témoignages* : McCrorie (ASFC); Larkin (GRC); Ferron (ARC); Ferron (ARC); Harroun (CRTC); Harroun (CRTC); Harroun (CRTC); Brett Napier (directeur général par intérim, Conservation et Protection, ministère des Pêches et Océans [MPO]); Walker (ECCC); Walker (ECCC); Gratton (SCC); Larkin (GRC); Mario Mainville (dirigeant principal de l'application numérique, Bureau de la concurrence du Canada [BC]); Jones (SPC); Fox (BST); Commissariat à la protection de la vie privée, *Lettre au Comité*, 8 mars 2024. M. Larkin a mentionné la possibilité d'une utilisation par la GRC dans des cas urgents ou il n'est pas possible d'obtenir un mandat, mais dans ce cas, l'utilisation serait faite conformément au *Code Criminel*. Service correctionnel du Canada, le Bureau de la Sécurité du Transport et Services partagés Canada s'appuient sur leurs pouvoirs statutaires pour utiliser ces outils.

25 ETHI, *Témoignages* : Rodgers (ECCC); Larkin (GRC); Gagné (GRC); Mainville (BC).

26 ETHI, *Témoignages* : Francis Brisson (sous-ministre adjoint et dirigeant principal des finances, RNCan); Dave Yarker (directeur général, Cybersécurité et commandement et contrôle des opérations des systèmes d'information, ministère de la Défense nationale [MDN]); Sophie Martel (dirigeante principale de l'information par intérim, MDN); Walker (ECCC); Larkin (GRC); Ferron (ARC); Napier (MPO); Harroun (CRTC); Harroun (CRTC); Napier (MPO); Walker (ECCC); Larkin (GRC); Jones (SPC); Fox (BST); Mainville (BC).

27 ETHI, *Témoignages* : Fox (BST); Gagné (GRC); McCrorie (ASFC) Gratton (SCC); Mainville (BC). Dans le cas de Service correctionnel du Canada, les appareils saisis sont des objets interdits et ne sont donc pas retournés à leurs propriétaires.

28 ETHI, *Témoignages* : Ferron (ARC) Walker (ECCC); Walker (ECCC); Rogers (ECCC); Napier (MPO); Gratton (SCC); Fox (BST); Mainville (BC).

29 ETHI, *Témoignages* : Gratton (SCC); Pelletier (RNCan); McCrorie (ASFC); McCrorie (ASFC); Napier (MPO); Mainville (BC); Jones (SPC); Mainville (BC).

d'enquêtes administratives internes. Les questions relatives à un tel usage sont abordées dans le chapitre 3.

Le tableau qui se trouve à l'Annexe A du rapport fournit quelques détails additionnels concernant l'utilisation d'outils de criminalistique numériques par les douze institutions fédérales dont les représentants ont comparu devant le Comité. Le tableau qui se trouve à l'Annexe B indique si d'autres institutions fédérales ont fait l'achat ou ont accès à des logiciels qui permettent d'extraire de l'information d'appareils électroniques.

Évaluation des facteurs relatifs à la vie privée

Alors que le reportage qui a mené à l'étude indiquait qu'aucune des institutions identifiées n'avait fait d'ÉFVP concernant l'utilisation d'outils de criminalistique numérique, certains représentants d'institutions fédérales ont clarifié devant le Comité qu'une ÉFVP au niveau du programme gouvernemental a bel et bien été faite. C'est une ÉFVP de l'outil de criminalistique numérique distinct qui n'a pas été faite.

D'autres représentants d'institutions fédérales ont indiqué soit qu'une ÉFVP relative à l'utilisation de ces outils était en cours, soit qu'ils s'étaient déjà engagés à en faire une prochainement, ou encore qu'ils étaient en train d'étudier la possibilité de procéder à une telle évaluation. Un représentant d'une institution fédérale a dit que cette institution ferait une ÉFVP si elle décidait d'utiliser l'outil de criminalistique numérique acheté.

M. Dufresne a reconnu que dans un certain nombre de cas, les institutions fédérales qui n'ont pas fait d'ÉFVP en lien avec leur utilisation d'outils de criminalistique numérique ne se sont pas conformées à la *Directive sur l'ÉFVP* du Conseil du Trésor.

Évaluation des facteurs relatifs à la vie privée au niveau du programme

En ce qui concerne l'Agence du Revenu du Canada (ARC), M. Ferron, directeur général, Direction des enquêtes criminelles, Direction générale des programmes d'observation, a indiqué que l'ensemble du Programme des enquêtes criminelles de l'ARC a fait l'objet d'une ÉFVP en 2016[30]. Une mise à jour a été faite récemment. Il a confirmé que cette ÉFVP vise le programme et non les outils utilisés. Il a dit que l'ÉFVP menée par l'ARC indique que les experts de l'ARC utilisent des outils au moment de faire la saisie d'objets électroniques afin d'en extraire de l'information.

30 ETHI, *Témoignages* : Ferron (ARC) et Ferron (ARC)

Anne-Marie Laurin, directrice générale par intérim et chef adjointe de la protection des renseignements personnels de l'ARC, a ajouté que l'ÉFVP en question a été remise au commissaire à la protection de la vie privée à l'époque et n'a fait l'objet d'aucun commentaire.

Pour le CRTC, M. Harroun a indiqué que lorsque la Loi canadienne antipourriel (LCAP) est entrée en vigueur en 2014, trois ÉFVP ont été effectuées[31]. L'une d'entre elles fait spécifiquement référence à l'article 19 de la LCAP, qui traite des mandats de perquisition et de l'utilisation d'outils d'investigation numérique. Il a donc affirmé qu'une ÉFVP valide existe depuis 2014 pour les outils que le CRTC utilise présentement[32]. M. Harroun a confirmé que l'ÉFVP a été faite au niveau du programme et non au niveau d'un outil spécifique. Selon lui, l'ÉFVP au niveau du programme est suffisante, puisque le programme est très précis quant à l'utilisation d'outils de criminalistique numérique et de collecte de preuves.

Dans le cas de Pêches et Océans Canada, Sam Ryan, directeur général, Opérations de technologie de l'information, a indiqué qu'une ÉFVP a été effectuée au niveau du programme de Conservation et Protection autour de 2010. Aucune ÉFVP n'a été faite au niveau de l'outil de criminalistique numérique spécifique[33]. Il a souligné que l'outil n'est qu'une composante du programme et qu'au moment de l'achat d'outils de criminalistique numérique, on considérait qu'il s'agissait d'une continuité de programmes existants. Toutefois, M. Napier a reconnu qu'à ce stade, il est justifié pour Pêches et Océans Canada de revoir ces processus pour s'assurer que le ministère protège bien la vie privée. Le ministère s'est donc engagé à faire une mise à jour de l'ÉFVP du programme susmentionné auprès du commissaire à la protection de la vie privée en décembre 2023[34].

Luc Casault, directeur général, Services intégrés, Bureau de la Sécurité des Transports du Canada (BST), a précisé qu'une ÉFVP existe pour le programme d'enquête du BST depuis sa création, mais qu'une évaluation n'a pas été faite pour l'outil de criminalistique numérique lui-même. Kathy Fox, présidente du BST, a indiqué, comme Pêches et Océans Canada, que puisque ce genre d'extraction de données est faite depuis longtemps, et

---

31 *Loi visant à promouvoir l'efficacité et la capacité d'adaptation de l'économie canadienne par la réglementation de certaines pratiques qui découragent l'exercice des activités commerciales par voie électronique et modifiant la Loi sur le Conseil de la radiodiffusion et des télécommunications canadiennes, la Loi sur la concurrence, la Loi sur la protection des renseignements personnels et les documents électroniques et la Loi sur les télécommunications*, S.C. 2010, c. 23.

32 ETHI, *Témoignages*, Harroun.

33 ETHI, *Témoignages* : Sam Ryan (directeur général, Opérations de technologie de l'information, MPO) et Napier (MPO).

34 ETHI, *Témoignages*, Sam Ryan (MPO).

qu'une ÉFVP du programme a déjà été faite, le BST n'a pas senti le besoin de faire une ÉFVP distincte pour l'outil de criminalistique numérique lui-même.

Toutefois, elle a dit qu'à la suite d'une discussion avec le commissaire à la protection de la vie privée, le BST est résolu à mettre à jour l'ÉFVP de son programme d'enquête afin de s'assurer qu'il englobe toutes les technologies actuelles utilisées pour remplir son mandat. M. Casault a confirmé que « le commissaire a recommandé à coup sûr de mettre à jour l'évaluation de notre programme ».

Évaluation des facteurs relatifs à la vie privée déjà en cours, à venir, ou potentielle

En ce qui concerne la GRC, M. Larkin a indiqué qu'une ÉFVP relative aux outils de criminalistique numérique était en cours et serait terminée d'ici mi-2024.

Pour ce qui est de l'ASFC, M. McCrorie a noté qu'elle travaille avec ses partenaires internes à faire une ÉFVP de l'ensemble du Programme des enquêtes criminelles de l'agence depuis 2022[35]. L'ASFC continuera de mener cette évaluation, il espère, en collaboration avec le Commissariat[36]. Il a confirmé que l'ÉFVP de l'ASFC se fait à l'échelle du programme plutôt qu'au niveau des appareils utilisés. Il a expliqué que l'ASFC a déterminé qu'au lieu de faire une ÉFVP pour chaque appareil, elle doit mener une ÉFVP qui vise la façon dont les appareils sont utilisés dans le cadre du programme.

Dans le cas de Service correctionnel Canada (SCC), France Gratton, commissaire adjointe, Opérations et programmes correctionnels, a expliqué qu'en 2010, dès l'achat de l'outil de criminalistique numérique, on a effectué une série de vérifications permettant de déterminer si une ÉFVP était nécessaire. À l'époque, considérant le programme que SCC mettait en place, l'outil qui allait être utilisé et la façon dont l'information allait être gérée, on a déterminé qu'une ÉFVP n'était pas nécessaire. Elle a toutefois dit que « l'utilisation d'outils améliorés pour lutter contre les activités criminelles s'étant accrue au cours des dernières années, le SCC s'est engagé à renouveler l'évaluation initiale et à remplir une liste de vérification actualisée ».

En ce qui concerne le ministère de la Défense nationale, M. Yarker, directeur général, Cyber-opérations et systèmes d'information de commandement et de contrôle, a confirmé qu'aucune ÉFVP n'a été faite en ce qui concerne l'utilisation d'un outil de criminalistique numérique. Sophie Martel, dirigeante principale de l'information par

35 ETHI, *Témoignages*, McCrorie (ASFC).

36 ETHI, *Témoignages*, McCrorie (ASFC).

intérim, a toutefois noté qu'un certain nombre d'ÉFVP sont en cours au ministère de la Défense nationale, par exemple à l'égard de Microsoft 365. Elle a indiqué que le ministère étudie le besoin d'une ÉFVP en lien avec son utilisation d'outils de criminalistique numérique.

De son côté, ECCC a confirmé qu'aucune ÉFVP n'a été faite pour son utilisation de l'outil de criminalistique numérique[37]. M. Walker a expliqué que le ministère a mis sur pied son unité de criminalistique numérique en 2013, ce qui était considéré comme une évolution naturelle du processus relatif aux mandats de perquisition[38]. Il a rajouté qu'à l'époque de la création du programme, les personnes qui en étaient responsables semblent avoir considéré que comme son but n'était pas de recueillir des renseignements personnels, une ÉFVP n'était pas nécessaire[39].

Toutefois, M. Walker a dit que « dans le cadre d'un exercice de modernisation concernant la mise en œuvre d'une approche fondée sur le risque pour nos activités d'application de la loi et un examen périodique de nos directives » ECCC a déterminé qu'il était prudent de procéder à de nouvelles ÉFVP pour couvrir non seulement un outil précis, mais aussi les activités qu'ECCC entreprend afin de tenir compte du contexte dans lequel les différents outils sont utilisés[40].

M. Walker a indiqué qu'ECCC est en train d'effectuer de nouvelles ÉFVP, en donnant la priorité à celles qui portent sur ses activités opérationnelles. Cette intention aurait été communiquée au commissaire à la protection de la vie privée en juin 2022. Hannah Rodgers, directrice générale, Application de la loi en environnement, a confirmé que l'ÉFVP relative aux activités opérationnelles d'ECCC sera terminée au cours de la prochaine année.

Le président de Services partagés Canada (SPC), Scott Jones, a confirmé qu'aucune ÉFVP n'a été faite dans le cadre du programme élaboré lors de la création de SPC et en lien avec l'utilisation d'outils de criminalistique numérique de SPC, mais que l'institution fédérale avait commencé à en faire une[41]. Il a précisé que dans le cas où SPC ne fait qu'acheter un outil pour une autre institution fédérale, il ne relève pas de sa responsabilité d'évaluer l'utilisation qu'en fera l'institution concernée.

37 ETHI, *Témoignages*, Walker (ECCC).

38 ETHI, *Témoignages*, Walker (ECCC).

39 ETHI, *Témoignages*, Walker (ECCC).

40 ETHI, *Témoignages*, Walker (ECCC).

41 ETHI, *Témoignages*, Jones (SPC).

Pour ce qui est du Bureau de la Concurrence, Mario Mainville, dirigeant principal de l'application numérique, a confirmé qu'aucune ÉFVP relative au programme en vertu duquel l'outil de criminalistique numérique est utilisé n'a été faite. Il a expliqué que le programme a été mis en place avant que la *Directive sur l'ÉFVP* existe et que lorsqu'elle est entrée en vigueur, on a estimé que le programme n'avait pas subi de changements majeurs depuis sa création en 1996[42]. Selon le Bureau de la concurrence, l'ajout de nouveaux appareils plus évolués ne constituait pas un changement radical[43].

Cependant, M. Mainville a dit qu'après le témoignage du commissaire à la protection de la vie privée et la publication du reportage à la fin de 2023, le Bureau de la concurrence a contacté le Commissariat et entrepris des démarches concernant l'évaluation de son programme d'informatique judiciaire[44].

Évaluation des facteurs relatifs à la vie privée si l'outil est utilisé

Francis Brisson, sous-ministre adjoint et dirigeant principal des finances du ministère des Ressources naturelles (RNCan) a indiqué que l'outil de criminalistique numérique n'a jamais été utilisé par RNCan et donc qu'aucune ÉFVP n'a été faite[45]. Il a expliqué que RNCan a acheté l'outil pour l'avoir dans sa boîte à outils[46]. Il a expliqué que RNCan utilise des outils technologiques pour protéger ses actifs technologiques et ses données. M. Brisson a aussi affirmé qu'une ÉFVP sera faite si l'outil de criminalistique numérique acheté doit être utilisé pour une enquête. Néanmoins, il a semblé indiquer que RNCan pourrait envisager de faire une ÉFVP à la suite de sa comparution devant le Comité[47].

Constats du commissaire à la protection de la vie privée du Canada

Consultation préalable du commissaire

M. Dufresne a confirmé que le Commissariat a pris connaissance de l'utilisation d'outils de criminalistique numérique sur des appareils mobiles ou ordinateurs par treize institutions fédérales dans les médias. Il a précisé que le Commissariat était au courant

42 ETHI, *Témoignages*, Mainville (BC).

43 ETHI, *Témoignages*, Mainville (BC).

44 ETHI, *Témoignages*, Mainville (BC).

45 ETHI, *Témoignages*, Brisson (RNCan).

46 ETHI, *Témoignages*, Brisson (RNCan); Pelletier (RNCan).

47 ETHI, *Témoignages*, Brisson (RNCan).

de certains programmes gouvernementaux, mais pas de toutes les utilisations de ces outils. Il a dit :

> 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.

M. Dufresne a aussi noté que le Commissariat ne sait pas ce que fait un ministère si ce dernier ne l'informe pas ou ne le consulte pas. Il est donc toujours préférable qu'un ministère communique de façon proactive avec lui. Le Commissariat peut alors partager avec lui son point de vue sur la situation en question et signaler les risques, s'il y en a.

M. Dufresne a affirmé que lorsque le Commissariat est consulté en amont, ce dernier a la chance de poser le genre de questions permettant de déterminer si une certaine pratique est nécessaire et proportionnelle, et potentiellement de prévenir une situation où une pratique ne satisfait pas ces principes importants. Une telle consultation permet aussi de rassurer la population canadienne que le Commissariat a été consulté et a donné son avis sur une certaine pratique.

M. Dufresne a confirmé qu'il aimerait voir une prise de contact plus proactive de la part des ministères avec le Commissariat pour l'aviser de ce qu'ils envisagent de faire et demander si une ÉFVP est nécessaire. Cela permettrait au Commissariat de ne pas prendre connaissance de cette information dans les médias. Il a constaté que les ministères n'ont pas toujours le réflexe de vérifier si le Commissariat a été informé avant la mise sur pied d'un programme. Il y a selon lui des améliorations à apporter de ce côté.

M. Dufresne a rappelé que le Commissariat a une équipe consultative gouvernementale qui est toujours prête à entendre et fournir des conseils aux ministères. En ce qui concerne les ressources du Commissariat lui permettant de recevoir des ÉFVP et d'offrir des conseils aux ministères ou autres institutions fédérales qui pourraient utiliser des outils comme ceux faisant l'objet de l'étude du Comité, M. Dufresne a indiqué que le Commissariat détermine la priorité des demandes reçues en fonction de l'importance et des répercussions sur la vie privée[48].

48 ETHI, *Témoignages*, Dufresne.

En ce qui concerne la capacité du Commissariat d'évaluer les répercussions de l'IA sur la vie privée, M. Dufresne a expliqué qu'il est bien équipé pour le faire, avec un laboratoire technologique, qui s'informe pour rester à la fine pointe de la technologie[49].

Compréhension de la *Directive sur l'évaluation des facteurs relatifs à la vie privée*

M. Dufresne a expliqué que les institutions fédérales font la distinction entre une activité ou un programme nouveau et ceux qui existent déjà, mais estiment parfois que puisqu'elles ne font qu'utiliser un nouvel outil puissant, il ne s'agit pas d'un nouveau programme, car elles n'ont pas vraiment changé ce qu'elles font. Puisque le programme a déjà été évalué à l'égard des risques à la vie privée, elles ne soumettent pas l'outil lui-même à une ÉFVP. Il a reconnu que ce type de situation pourrait bien être conforme à la politique étant donné que la directive n'exige pas de nouvelle ÉFVP pour un programme existant. Toutefois, il a rappelé que lorsque nous parlons d'un outil très puissant – même dans le cadre d'un programme existant – ce dernier peut changer la donne et procurer une capacité additionnelle importante. Dans ces cas, il y a lieu de se demander si la population canadienne ne tirerait pas profit d'une plus grande transparence à l'égard de cet outil, même dans un programme existant.

Dans le cas de l'utilisation d'outils de criminalistique numérique, M. Dufresne a rappelé que ces outils peuvent être utilisés d'une manière qui soulève des risques importants sur le plan de la vie privée et qui mériteraient la tenue d'ÉFVP. Par exemple, il a suggéré que dans un cas où un tel outil est utilisé dans le contexte 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 dans le cadre d'une enquête sur des allégations d'activités criminelles ou illégales, une ÉFVP devrait être menée. Dans un tel cas, l'ÉFVP « 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 ».

M. Dufresne a aussi rappelé que les outils de criminalistique numérique permettent d'extraire des données supprimées ou non supprimées sur des appareils et des ordinateurs et, donc, des renseignements personnels. Ce faisant, lorsque l'utilisation de tels outils vise 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 ÉFVP doit être réalisée.

M. Dufresne a aussi indiqué que le Commissariat doit parfois rappeler aux ministères que, même s'ils font quelque chose sous le coup d'un mandat ou d'une autorité

49 ETHI, *Témoignages*, Dufresne.

juridique appropriée, l'ÉFVP est une question distincte. Il s'agit d'une étape supplémentaire[50]. Il a rappelé qu'un mandat de perquisition peut être fondé sur des critères distincts des considérations relatives à la vie privée qui sont au cœur des ÉFVP. Ainsi, même s'il y a un mandat de perquisition et un fondement juridique, il faut quand même se demander si une ÉFVP doit être faite[51].

Certains représentants d'institutions fédérales ont indiqué reconnaître que le fait que l'outil soit utilisé dans le cadre d'une enquête, avec une ordonnance judiciaire ou un mandat de perquisition, ne remplace pas une ÉFVP[52].

En somme, M. Dufresne a rappelé que « [c]ertains 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 ».

Suivi auprès des institutions fédérales et limites des pouvoirs du commissaire

M. Dufresne a indiqué que le Commissariat a fait un suivi auprès des treize institutions identifiées dans le reportage de Radio-Canada[53]. Il a précisé que certaines institutions semblent utiliser couramment l'outil dans le cadre de leurs activités alors que d'autres en font une utilisation plus restreinte. Il a rappelé que le Commissariat, que l'outil soit utilisé deux, trois ou quatre fois ou régulièrement, regarde la situation de la même façon : est-ce une utilisation convenable et le ministère doit-il ou non effectuer une ÉFVP?

M. Dufresne a aussi dit au Comité que le Commissariat va faire un suivi avec les treize institutions fédérales visées pour veiller à ce que les ÉFVP manquantes soient réalisées et insister sur la nécessité de se conformer aux directives du Conseil du Trésor[54].

Toutefois, il a rappelé que sans une obligation au titre de la LPRP, il y a des limites à ce que le Commissariat peut faire pour assurer la conformité. En effet, M. Dufresne a expliqué la différence importante entre une politique ou une directive du Conseil du Trésor et une obligation en vertu de la LPRP. La directive ou politique est une règle interne que le gouvernement s'impose à lui-même et qui énonce ce que l'on attend d'un ministère. Elle n'a pas de force contraignante et ne permet donc pas au commissaire à la

50 ETHI, *Témoignages*, Dufresne.

51 ETHI, *Témoignages*, Dufresne.

52 ETHI, *Témoignages* : Mainville (BC) Casault (BST); Fox (BST).

53 ETHI, *Témoignages* : Dufresne et Dufresne.

54 ETHI, *Témoignages*, Dufresne.

protection de la vie privée d'effectuer une enquête pour un manquement à cette règle. Les obligations que l'on trouve dans la LPRP sont contraignantes. Le Commissariat peut faire enquête s'il a un motif raisonnable de croire qu'il y a eu contravention d'une disposition de la LPRP.

Considérant ce qui précède, M. Dufresne a confirmé qu'aucune enquête du Commissariat n'est en cours à l'égard des institutions fédérales visées par le reportage concernant de possibles manquements à la *Directive sur l'ÉFVP*. Il a réitéré que puisqu'il n'y a pas d'obligation légale en vertu de la LPRP d'effectuer une ÉFVP, il n'a pas de raison d'enquêter sur le non-respect d'une directive.

CHAPITRE 3 : PROTECTION DE LA VIE PRIVÉE DES EMPLOYÉS D'INSTITUTIONS FÉDÉRALES

Utilisation d'outils de criminalistique numérique sur les appareils d'employés d'institutions fédérales

M. Dufresne a rappelé que lorsqu'une institution fédérale utilise des outils de criminalistique numérique pour surveiller des employés, elle doit prendre certaines mesures pour garantir le respect du droit fondamental à la vie privée. Des règles claires devraient régir quand et comment cette technologie est utilisée, selon lui. À cet égard, le Commissariat a publié un document d'orientation sur la protection des renseignements personnels au travail, en mai 2023, et une résolution conjointe – avec ses homologues provinciaux – sur la protection de la vie privée des employés sur les lieux de travail, en octobre 2023[55].

Dans un document qu'il a fait parvenir au Comité à la suite de sa comparution, M. Dufresne précise que le document d'orientation *La protection des renseignements personnels au travail* de mai 2023 présente les principaux facteurs à prendre en compte dans la gestion des renseignements personnels concernant les employés et traite de questions d'actualité comme la surveillance des employés.

55 Commissariat à la protection de la vie privée du Canada, *La protection des renseignements personnels au travail*, révisé le 29 mai 2023, et *La protection de la vie privée des employés sur les lieux de travail modernes*, Résolution des commissaires fédéral, provinciaux et territoriaux à la protection de la vie privée et des ombuds responsables de la protection de la vie privée, du 4 au 5 octobre 2023. Dans le cas d'organisations du secteur privé, la *Loi sur la protection des renseignements personnels et les documents électroniques* ne s'applique qu'à la protection des renseignements personnels des employés d'organisations de compétence fédérale. Autrement, ce sont les lois provinciales – ou la common law – qui s'appliquent.

En ce qui concerne la résolution conjointe d'octobre 2023, le document mentionne que les autorités de protection :

> [I]nvitent les gouvernements et les employeurs à fournir un effort collectif en vue de combler les lacunes dans les lois, de respecter et de protéger le droit à la vie privée et à la transparence des employés, et de garantir une utilisation juste et adéquate des outils de surveillance électronique et des technologies de l'IA dans le contexte moderne du travail[56].

Il est question de l'utilisation de l'IA dans le contexte du travail plus loin dans ce rapport.

M. Dufresne a également rappelé que pour respecter les droits des employés en matière de protection de la vie privée, les institutions doivent notamment veiller à ce que l'utilisation d'un outil technologique soit liée aux objectifs d'un projet, faire preuve de transparence, s'adapter aux différentes situations qui se présentent, en plus de réaliser une ÉFVP, au besoin. Selon lui, chaque institution devrait évaluer l'outil en question selon les principes de nécessité et de proportionnalité liés à son utilisation.

Comme le Commissariat l'a indiqué, les principes de nécessité et de proportionnalité « garantissent que les pratiques portant atteinte à la vie privée sont mises en œuvre pour un objectif suffisamment important et qu'elles sont rigoureusement adaptées afin de ne pas porter atteinte au droit à la vie privée autrement que si cela est nécessaire »[57].

M. Dufresne a donné l'exemple d'une enquête menée en vertu de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) à l'issue de laquelle le Commissariat a conclu qu'une entreprise de transport, dont la caméra-témoin faisait un enregistrement audio et vidéo continu dans la cabine de son camion, ne respectait pas ces principes. Le Commissariat a jugé que cette surveillance était seulement légitime lorsque les camionneurs conduisaient, pour des raisons de sécurité[58].

En ce qui concerne la consultation par l'employeur de renseignements personnels de ses employés, M. Dufresne a rappelé le principe de la limitation de la collecte, lui-même lié aux principes de nécessité et de proportionnalité. Selon ce principe, un employeur ne

---

56 Commissaire à la protection de la vie privée du Canada, *Lettre au Comité*, 23 février 2024, p. 3.

57 Commissaire à la protection de la vie privée du Canada, *Document d'orientation sur la protection de la vie privée à l'intention des services de police relativement au recours à la reconnaissance faciale*, mai 2022, para. 60.

58 Commissariat à la protection de la vie privée du Canada, *Enquête sur l'utilisation par Trimac d'un appareil de surveillance vidéo et audio dans les cabines de ses camions*, Conclusions en vertu de la LPRPDE no 2022-006, 27 juillet 2022.

doit recueillir que les renseignements qui sont nécessaires aux fins poursuivies. En consultant les renseignements de son employé sur un appareil électronique, un employeur doit faire preuve de transparence et s'assurer que l'employé est conscient qu'il s'agit de son appareil de travail. L'employeur doit aussi exposer la nature des renseignements auxquels il aura accès et expliquer la raison pour laquelle il doit accéder à ces renseignements[59]. À cet égard, M. Dufresne a fourni l'exemple de renseignements sur la santé d'un employé qui se trouveraient sur l'appareil mobile qu'il utilise pour le travail. L'employeur devrait alors se demander s'il a besoin d'accéder à ces renseignements avant de les consulter.

M. Dufresne a avancé qu'en règle générale, les outils de criminalistique numérique utilisés par les institutions fédérales pour des enquêtes administratives visant des employés sont uniquement utilisés sur les appareils fournis par l'employeur.

En outre, les représentants de SCC, de RNCan, de l'ASFC, de l'ARC, du CRTC, de Pêches et Océans Canada, d'ECCC, ainsi que de la GRC ont tous affirmé que les outils de criminalistique numérique ne sont pas utilisés pour surveiller les employés à leur insu[60]. Si ces outils sont utilisés pour des enquêtes internes, les employés concernés en sont nécessairement informés puisque l'utilisation de l'outil exige d'avoir l'appareil examiné en main.

En ce qui concerne SCC, Mme Gratton a précisé que ces outils ne sont utilisés que sur des téléphones cellulaires interdits qui ont été saisis après avoir été introduits illégalement dans un de ses établissements.

La situation des employés du ministère de la Défense nationale diffère de celle des autres fonctionnaires. En effet, l'attente en matière de protection de la vie privée par rapport à l'utilisation des systèmes de TI et des appareils mobiles du ministère de la Défense nationale est limitée, selon Mme Martel, car une surveillance est requise aux fins de l'administration, de la maintenance et de la sécurité du système, ainsi que pour assurer le respect des politiques en vigueur.

Mme Martel a précisé que lorsqu'un compte est créé sur le réseau du ministère de la Défense nationale, un employé doit signer pour confirmer qu'il utilisera l'appareil en question exclusivement pour faire du travail lié au gouvernement s'il veut accéder à ce

59 Voir : Commissariat à la protection de la vie privée du Canada, *La protection des renseignements personnels au travail*, 29 mai 2023.

60 ETHI, *Témoignages*, Gratton (SCC), Pelletier (RNCan), McCrorie (ASFC), Ferron (ARC), Harroun (CRTC), Ryan (MPO), Walker (ECCC), Larkin (GRC).

compte. Elle a toutefois reconnu que certains employés utilisent ces appareils pour un usage personnel.

Quant à l'utilisation de ces outils par la police fédérale à l'égard de ses propres employés, M. Larkin a noté que le recours au programme de criminalistique numérique de la GRC dans le cadre d'enquêtes administratives est régi par des dispositions législatives et des politiques. Selon lui, la collecte d'éléments de preuves au moyen de ces outils est fondée sur la nécessité et la proportionnalité par rapport aux allégations à l'origine d'une enquête déontologique interne. Il a précisé que la GRC n'effectuerait ce genre d'examen que sur un appareil appartenant à la GRC, et que pour tout appareil personnel, un mandat judiciaire serait requis.

M. Larkin a indiqué que la GRC utilise des outils de criminalistique numérique sur les téléphones de ses employés seulement lorsqu'une allégation relative à un code de déontologie a été faite et qu'une enquête interne a lieu, ou encore dans le cadre d'une enquête criminelle impliquant un employé. Dans ce dernier cas, la GRC demanderait une autorisation judiciaire. Dans le cas d'une méconduite interne, l'enquêteur consulterait plutôt les spécialistes de la criminalistique numérique de la GRC et déciderait s'il est nécessaire d'utiliser l'outil en question.

M. Larkin a précisé que la GRC a utilisé un outil de criminalistique numérique dans le cadre d'une affaire interne à une seule occasion. Il s'agissait d'une enquête de sécurité ministérielle et cet outil a été utilisé avec le consentement de l'employé de la GRC[61].

En ce qui concerne le Programme des enquêtes criminelles de l'ARC, il limite l'utilisation des outils de criminalistique numérique aux enquêtes externes, ce qui signifie qu'ils ne pourraient être utilisés dans le cadre d'enquêtes internes sur les employés de l'Agence, selon M. Ferron.

Quant à Pêches et Océans Canada, M. Napier et M. Ryan ont confirmé qu'un outil de criminalistique numérique peut être utilisé dans le cadre d'enquêtes administratives internes, par exemple des enquêtes sur les violations des politiques du gouvernement du Canada et les incidents de cybersécurité.

M. Pelletier a indiqué qu'il est possible que des logiciels semblables à ceux faisant l'objet de l'étude du Comité aient été utilisés pour une enquête de RNCan relative à l'inconduite d'un employé par le passé, mais qu'ils n'en ont pas nécessairement besoin. M. Brisson a confirmé que si l'outil de criminalistique numérique devait être utilisé, ce serait pour une enquête interne. Il a noté que tous les systèmes de surveillance dont se dote RNCan sont

61 ETHI, *Témoignages*, Larkin.

utilisés pour des besoins internes et à des fins administratives, conformément aux exigences en matière de sécurité découlant d'un mandat de sécurité clair.

M. Jones, a affirmé que les institutions fédérales, y compris SPC, utilisent des outils de criminalistique numérique dans le cadre d'enquêtes administratives qui ont lieu uniquement lorsqu'il y a une allégation crédible d'acte répréhensible commis par un employé et pour assurer la sécurité des réseaux gouvernementaux. Il a expliqué que ces enquêtes peuvent notamment porter sur des cas où l'on soupçonne un employé – en lien avec un appareil ou un réseau du gouvernement – d'avoir navigué sur des sites Web inappropriés ou d'avoir installé un logiciel malveillant, ou encore d'avoir utilisé des réseaux ou des dispositifs électroniques ministériels de façon inacceptable.

Mme Fox a affirmé que le BST n'utilise pas du tout les outils de criminalistique numérique sur les téléphones de ses employés, qu'ils soient fournis par le gouvernement ou non.

L'ASFC a confirmé, dans un document qu'elle a fait parvenir au Comité, qu'elle n'utilise pas d'outil ou de technologie pour surveiller activement l'utilisation de ses appareils par les employés[62]. Dans ce document, l'ASFC précise l'utilisation qu'elle en fait dans le cadre d'une enquête :

> […] les employés de la Division de l'intégrité professionnelle (DIP) sont habilités à accéder à tous les systèmes d'information, documents et dossiers pertinents de l'ASFC, dans la mesure où la loi le permet. S'il y a lieu dans le cadre d'une enquête, la DIP récupère des appareils de l'ASFC auprès d'employés, et extrait et examine les données, les fichiers et les informations stockés sur ces appareils afin d'aider à déterminer dans quelle mesure les comportements ou les événements présumés se sont produits[63].

Cependant, dans un mémoire adressé au Comité, les représentants de l'Alliance de la Fonction publique du Canada (AFPC) affirment avoir

> plusieurs raisons de craindre l'utilisation d'outils capables d'extraire des données personnelles des appareils en l'absence de processus solides d'encadrement de leur

62 Agence des services frontaliers du Canada, *Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (ETHI) – Utilisation d'outils permettant d'extraire des données sur des appareils mobiles et ordinateurs – Le 6 février 2024*, p. 2.

63 *Ibid*.

utilisation, de protection des renseignements personnels concernant les employés et d'explication des motifs de leur déploiement[64].

Leur plus grande préoccupation découle du fait qu'un grand nombre de ministères ont failli à leur responsabilité de mener des ÉFVP, selon eux. Cette préoccupation a été partagée par Nathan Prier, président de l'Association canadienne des employés professionnels (ACEP), et par Jennifer Carr, présidente de l'Institut professionnel de la fonction publique du Canada (IPFPC).

La question du consentement des employés

Certains représentants d'institutions fédérales ont insisté sur le fait que les employés visés par une enquête interne consentaient à ce que leurs renseignements personnels soient vérifiés à l'aide d'outils de criminalistique numérique. M. Jones a affirmé que les employés de SPC concernés sont toujours informés du déroulement des enquêtes administratives menées par les institutions fédérales et que l'équité procédurale est respectée.

En ce qui concerne la GRC, M. Larkin a rappelé que chaque employé signe un formulaire de consentement quant à l'utilisation de l'appareil qu'il reçoit. Comme indiqué ci-dessus, dans le seul cas où un outil de criminalistique numérique a été utilisé sur l'appareil d'un employé dans le cadre d'une enquête administrative interne, c'était avec le consentement de l'individu concerné.

Quant à Mme Martel, elle a expliqué que pour utiliser un appareil gouvernemental et avoir un compte sur le réseau du ministère de la Défense nationale, un employé doit remplir un questionnaire et est informé qu'il sera surveillé pour des raisons de sécurité du réseau.

Selon M. Pelletier, de RNCan, un employé qui utilise les réseaux d'une institution gouvernementale a l'obligation de s'assurer que cette utilisation est conforme aux politiques gouvernementales. Il a rajouté que RNCan remet régulièrement en évidence cette obligation et qu'un rappel est fait automatiquement chaque fois qu'un employé accède au réseau privé virtuel du ministère.

64 Alliance de la Fonction publique du Canada [AFPC], *Mémoire à l'intention du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique – Au sujet de – l'étude sur l'utilisation par le gouvernement fédéral d'outils technologiques permettant d'extraire des renseignements personnels des appareils mobiles et des ordinateurs*, 3 mars 2024, p. 1.

Dans la même veine, M. Ryan a indiqué que la politique du gouvernement du Canada d'utilisation acceptable d'appareils gouvernementaux s'affiche à chaque connexion au réseau de Pêches et Océans Canada. Les employés acceptent ainsi de se conformer à cette politique, selon lui. M. Ryan a également indiqué que les employés de Pêches et Océans Canada qui sont visés par une enquête administrative interne sont pleinement conscients du processus et sont informés de la portée de l'enquête.

Mme Fox a affirmé que même s'il est possible pour le BST d'émettre un mandat à la suite d'une demande faite à un juge de paix pour utiliser un outil de criminalistique numérique, cela n'a jamais été fait parce que les appareils visés sont habituellement obtenus par consentement, sur place, ou par l'intermédiaire des premiers intervenants.

Dans le même ordre d'idées, M. Mainville a affirmé que le Bureau de la concurrence n'utilise ces outils qu'avec un mandat de perquisition autorisé par un juge, à l'exception d'un seul cas où il y a eu consentement de la personne visée et où une entente de consentement a été conclue.

Evan Light, professeur agrégé de la Toronto Metropolitan University, a offert un point de vue différent sur la question du consentement. Selon lui, il est difficile – voire impossible – pour les employés qui font l'objet d'une enquête interne de donner un consentement éclairé dans ces situations, car « il y a un déséquilibre des pouvoirs ainsi qu'un déséquilibre des connaissances ».

Dans un document qu'il a fait parvenir au Comité, M. Light présente deux facteurs qui doivent être pris en compte dans les discussions sur le consentement, selon lui : « 1) la question de savoir si le sujet est capable d'obtenir un consentement éclairé en fonction des informations qui lui sont fournies, et 2) s'il est capable d'obtenir un consentement éclairé compte tenu de la dynamique de pouvoir en jeu[65] ».

Selon M. Light, le consentement n'est pas suffisant à lui seul parce que les personnes ne savent pas nécessairement à quoi ils consentent et parce que les ÉFVP ne sont pas efficaces en tant qu'outils d'autoréglementation. Selon lui, un organisme externe, comme le Commissariat, devrait décider si un outil doit être utilisé ou non et quel type de processus doit être mis en place pour qu'une personne soit en mesure de donner un consentement éclairé à l'examen de son appareil.

M. Light a avancé qu'un fonctionnaire a une attente raisonnable en matière de protection de la vie privée sur le téléphone que lui fournit le gouvernement. Selon lui,

65 Evan Light, *Au Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique*, Document de référence soumis au Comité, 5 février 2024, p. 4.

les ÉFVP ne sont pas nécessairement la norme en matière de gestion des relations entre les institutions et leurs employés. Les ÉFVP poussent une institution à poser des questions qui l'aident à réfléchir à la manière de trouver un équilibre entre les violations et les protections de la vie privée, mais ce processus n'est pas forcément clair pour les employés, selon M. Light. Il a résumé sa position en affirmant qu'il existe des directives à un haut niveau, mais qu'on ne comprend pas ce qui doit être fait sur le terrain.

Mme Carr a rappelé quant à elle que les politiques applicables ont été élaborées à une époque où les activités infonuagiques et les données chiffrées n'existaient pas, ce qui ferait en sorte que le consentement donné en fonction de ces politiques – qui doivent être mises à jour, selon elle – ne correspond pas à la réalité d'aujourd'hui.

En ce qui concerne la façon pour un fonctionnaire de donner son consentement et la formation reçue au moment où un appareil lui est fourni par le gouvernement, Mme Carr et M. Prier ont noté que différentes règles s'appliquent, selon l'institution pour laquelle le fonctionnaire travaille. On l'informerait généralement des valeurs et des règles d'éthique à respecter tout en exigeant sa signature, mais la décentralisation des responsabilités confiées aux institutions est telle qu'on leur permet d'adopter leurs propres politiques, selon Mme Carr.

Utilisation de l'intelligence artificielle dans le domaine de l'emploi

Partant de la prémisse que les avancées technologiques renforcent la recommandation de faire de la réalisation des ÉFVP une obligation juridique – dont il est question dans le chapitre 4 du présent rapport – M. Dufresne a noté sur un sujet connexe que, lors de la conférence de l'Assemblée mondiale pour la protection de la vie privée (AMVP), des autorités chargées de la protection de la vie privée de partout dans le monde ont adopté une résolution sur l'intelligence artificielle (IA) dans le domaine de l'emploi[66].

Cette résolution appelle les gouvernements et les parlementaires à prendre conscience de la nécessité de baliser cette utilisation et demande à l'AMVP de collaborer avec les organisations qui élaborent ou mettent en œuvre des outils d'IA dans un contexte d'emploi, comme à des fins de surveillance ou de collecte et de conservation de données, afin de garantir que la protection de la vie privée des employés est prise en compte à toutes les étapes[67].

66 Global Privacy Assembly, *Resolution on AI and Employment*, Adopted Resolutions, 45th Global Privacy Assembly, Hamilton, Bermuda, 2023 [DISPONIBLE EN ANGLAIS SEULEMENT].

67 Commissaire à la protection de la vie privée du Canada, *Lettre au Comité*, 23 février 2024, p. 4.

Considérant ce qui précède, le Comité fait la recommandation suivante.

Recommandation 1

Que le gouvernement du Canada s'assure que les institutions et organisations sous réglementation fédérale qui élaborent ou utilisent des outils d'intelligence artificielle dans un contexte d'emploi garantissent que la protection de la vie privée des employés est prise en compte à toutes les étapes de l'élaboration ou de l'utilisation de ces outils.

CHAPITRE 4 : AMÉLIORATIONS LÉGISLATIVES ET AUTRES MESURES PROPOSÉES

Certains témoins ont recommandé de modifier la LPRP afin d'assurer une plus grande transparence dans les pratiques des institutions fédérales et d'accroitre leur conformité à l'obligation de mener des ÉFVP, tout en étayant les principes de nécessité et de proportionnalité. D'autres recommandations ont aussi été faites, notamment sur des modifications potentielles aux directives du Conseil du Trésor.

Améliorations législatives proposées

M. Dufresne a rappelé au Comité la recommandation qu'il lui a faite en 2022 lors de son étude de l'utilisation des outils d'enquête sur appareil par la GRC – à laquelle le Comité a souscrit – d'imposer aux institutions fédérales l'obligation explicite de faire des ÉFVP en vertu de la LPRP[68]. M. Light a abondé dans le même sens, en précisant que les ÉFVP devraient être effectuées avant tout achat d'outil technologique, selon lui. Mme Carr, de l'IPFPC, a également fait une recommandation dans le même sens.

M. Dufresne a expliqué les raisons pour lesquelles cet ajout est important, selon lui, de la manière suivante :

> 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 ÉFVP 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

68 ETHI, *Outils d'enquête sur appareil utilisés par la Gendarmerie royale du Canada et enjeux liés*, novembre 2022.

loi de procéder ainsi; il devrait s'agir d'une obligation au titre de la *Loi sur la protection des renseignements personnels*.

Selon M. Dufresne, cet ajout devrait également être fait dans la LPRPDE, pour que l'obligation de réaliser une ÉFVP s'applique aux organisations du secteur privé[69]. Pour appuyer cette recommandation, M. Dufresne a également recommandé de donner au commissaire à la protection de la vie privée le mandat et le pouvoir de s'assurer que les institutions respectent leur obligation de réaliser une ÉFVP lorsque la situation l'exige.

M. Dufresne a également recommandé que le concept de la protection de la vie privée dès la conception soit inclus dès le début d'un processus où une nouvelle technologie est utilisée. Il a noté qu'une ÉFVP est souvent réalisée après qu'un outil soit développé et utilisé et a avancé qu'il serait toujours plus rentable et prudent d'intégrer la protection de la vie privée dès le départ. Ce constat est à la base de sa recommandation de rendre la réalisation des ÉFVP obligatoire en vertu de la LPRP.

M. Dufresne a rappelé au Comité que la réalisation d'une ÉFVP est prévue dans une directive gouvernementale. N'étant pas une obligation légale, le commissaire n'a pas l'autorité d'empêcher une institution de mettre en œuvre un outil technologique quelconque. Son rôle se limite à signaler au Conseil du Trésor que l'utilisation d'un certain outil ne serait pas conforme à la LPRP.

Qui plus est, rendre la réalisation d'une ÉFVP obligatoire en vertu de la LPRP pourrait mener à une conformité accrue et éviter des situations comme celle ayant mené à l'étude du Comité, où la population découvre les outils utilisés par des institutions fédérales par l'entremise des médias, selon M. Dufresne. À son avis, l'assurance de savoir que les institutions fédérales font des ÉFVP renforcerait la confiance de la population envers ces institutions.

La *Directive sur l'ÉFVP* établit des distinctions entre un nouveau programme et la mise à jour d'un programme existant, et entre l'évaluation d'un programme et l'évaluation d'un outil en particulier, comme l'a rappelé M. Dufresne. Ces distinctions permettent à une institution d'affirmer – de bonne foi – qu'une ÉFVP n'est pas nécessaire, puisque la directive ne l'exige pas. Pourtant, selon lui, avec la technologie qui devient de plus en plus puissante, il faudrait exiger une ÉFVP lorsque de nouveaux outils peuvent avoir une

69 Le projet de loi C-27, Loi édictant la Loi sur la protection de la vie privée des consommateurs, la Loi sur le Tribunal de la protection des renseignements personnels et des données et la Loi sur l'intelligence artificielle et les données et apportant des modifications corrélatives et connexes à d'autres lois, présenté au Parlement en juin 2022, est présentement à l'étape de l'étude en Comité. Il vise entre autres à remplacer la partie 1 de la *Loi sur la protection des renseignements personnels et les documents électroniques* par une nouvelle loi : la Loi sur la protection de la vie privée des consommateurs.

incidence sur la vie privée afin de rassurer la population en lui montrant que ces évaluations sont faites d'une façon encore plus proactive.

En effet, selon M. Dufresne, si on s'éloigne de la notion même de programme, si un nouvel outil modifie le contexte, une ÉFVP doit être envisagée. Il a noté à ce propos que le contexte de l'utilisation et les mesures de protection en place sont des éléments importants à examiner dans le cadre d'une ÉFVP. Pour toutes ces raisons, il serait préférable de rendre la réalisation d'une ÉFVP obligatoire en vertu de la LPRP, selon lui.

En ce qui concerne le contenu de cette obligation proposée, M. Dufresne a recommandé que la LPRP impose – avant la mise sur pied d'un programme – l'obligation pour une institution de fournir au Commissariat les détails pertinents de ce programme dans un délai prescrit. Ces détails pourraient être précisés dans la LPRP ou dans le règlement pris en vertu de la LPRP, selon lui.

M. Dufresne a aussi recommandé que les concepts de nécessité et de proportionnalité soient inclus dans la LPRP[70]. En ce qui concerne la nécessité, il a indiqué que la LPRP exige simplement que l'utilisation soit liée au mandat de l'institution fédérale, alors que la directive du Conseil du Trésor prévoit que l'utilisation doit être nécessaire pour atteindre l'objectif visé[71]. Selon lui, même si un objectif est légitime, la question à se poser est si l'on va trop loin dans la manière de l'atteindre.

Quant à la proportionnalité, M. Dufresne a expliqué que plus une 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. En d'autres termes, lorsqu'on dispose d'un outil plus intrusif, il est nécessaire de mettre en place un mécanisme de protection plus rigoureux.

M. Dufresne a rappelé que l'innovation et la technologie apportent beaucoup d'avantages dans de nombreux domaines et qu'il ne s'agit pas de refuser de l'utiliser. Il s'agit plutôt de s'assurer que la population n'ait pas à choisir entre la technologie et leur vie privée et qu'elle sache que les institutions sont en mesure de les protéger et les conseiller.

M. Dufresne a également recommandé d'octroyer au commissaire à la protection de la vie privée le pouvoir d'émettre des ordonnances et la possibilité d'imposer des sanctions

---

70 ETHI, *Témoignages*, 1er février 2024, Dufresne.

71 LPRP, art. 4. Cet article prévoit que « les seuls renseignements personnels que peut recueillir une institution fédérale sont ceux qui ont un lien direct avec ses programmes ou ses activités »; Secrétariat du Conseil du Trésor, *Directive sur les pratiques relatives à la protection de la vie privée*, art. 4.2.9 prévoit qu'une institution fédérale doit « limiter la collecte de renseignements personnels à ceux qui sont directement liés et manifestement nécessaires aux programmes ou aux activités de l'institution fédérale ».

pécuniaires administratives dans la LPRP, comme c'est le cas pour la Commission d'accès à l'information du Québec en vertu de la Loi 25, par exemple[72].

Autres mesures proposées

Dans un document qu'il a fait parvenir au Comité à la suite de sa comparution, M. Light fait une série de recommandations regroupées sous quatre thèmes : la préservation du droit fondamental à la protection de la vie privée, l'accès à l'information et la divulgation proactive, la souveraineté des données et la préservation des institutions démocratiques, ainsi que l'approvisionnement[73].

M. Light a recommandé notamment d'accorder au commissaire à la protection de la vie privée du Canada des pouvoirs judiciaires et au Commissariat « le mandat d'un organisme de réglementation proactif chargé de préserver le droit fondamental à la protection de la vie privée à l'endroit du gouvernement fédéral autant que du secteur privé » en même temps que les ressources nécessaires pour s'acquitter de ce mandat.

En ce qui concerne l'approvisionnement, il a recommandé de le placer au cœur du mandat du Commissariat à la protection de la vie privée du Canada et d'accorder à ce dernier un droit de veto en la matière. Selon M. Light, le Commissariat devrait approuver tous les achats de nature technologique, qu'il s'agisse de matériel informatique ou de logiciels. De plus, pour être approuvées, les technologies en question devraient faire l'objet d'une ÉFVP de la part du Commissariat et non des institutions qui ont l'intention de les utiliser. M. Light a recommandé également, « [d]ans une optique d'ouverture, de transparence et de responsabilité gouvernementales », que le gouvernement du Canada procède à un examen complet de ses processus d'approvisionnement et de reddition de comptes.

Dans leur mémoire, les représentants de l'AFPC recommandent au Conseil du Trésor de mettre en place une directive qui établirait des mesures correctives pour les cas où les hauts fonctionnaires n'effectuent pas les ÉFVP appropriées ou utilisent les outils technologiques de façon inappropriée, et que les mesures en question soient assez

72 ETHI, *Témoignages*, 1er février 2024, Dufresne. Le projet de loi C-27, si adopté, donnerait au commissaire à la protection de la vie privée des pouvoirs d'ordonnance sous la nouvelle Loi sur la protection de la vie privée des consommateurs, mais pas le pouvoir d'imposer des sanctions administratives.

73 Evan Light, *Au Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique*, Document de référence soumis au Comité, 22 février 2024.

sévères pour décourager ces comportements[74]. Mme Carr et M. Prier ont abondé dans le même sens en recommandant qu'il y ait des répercussions en cas de non-respect des directives du Conseil du Trésor et des mesures claires pour veiller à ce que les institutions fédérales s'y conforment davantage à l'avenir.

M. Prier, de l'ACEP, a présenté les trois demandes suivantes au Comité :

> Premièrement, nous demandons au gouvernement de mettre fin à l'utilisation de logiciels espions sur les appareils fédéraux allant à l'encontre de ses propres règles et d'utiliser les mesures les moins invasives qui soient. Tous les fonctionnaires ont droit à l'application régulière de la loi pendant les enquêtes.
>
> Deuxièmement, nous voulons savoir quand le gouvernement prévoit d'effectuer des évaluations des facteurs relatifs à la vie privée dans tous les ministères touchés et de rendre publics les résultats de ces évaluations afin d'aider les fonctionnaires à rétablir la confiance envers leur employeur après ces violations. L'utilisation de logiciels espions entraîne une érosion du droit à la vie privée qu'aucun fonctionnaire ne devrait accepter au premier abord.
>
> Enfin, nous demandons au gouvernement de procéder à un examen approfondi de toutes ses politiques numériques afin de s'assurer que le cadre stratégique actuel est suffisamment robuste pour protéger les droits numériques des employés, y compris leur droit à une protection raisonnable de leur vie privée, leur droit d'être informés de tout outil de surveillance numérique utilisé en milieu de travail et leur droit de se déconnecter du travail après les heures travaillées.

Le Comité note que les représentants des institutions fédérales qui ont comparu devant le Comité ont insisté sur le fait que leur institution utilise des outils de criminalistique numérique et non des logiciels espions.

Pour sa part, Mme Carr, de l'IPFPC, a recommandé au gouvernement de fournir des lignes directrices plus claires sur les programmes, nouveaux ou modifiés, qui nécessiteront de nouvelles ÉFVP et de mettre à jour les lignes directrices actuelles. « La technologie évolue rapidement, et nos pratiques doivent refléter cette réalité », a-t-elle noté.

Mme Carr a également demandé au gouvernement de reconnaître qu'il ne détient pas les renseignements personnels se trouvant sur les appareils utilisés par les employés et a plaidé en faveur d'un renforcement des mesures de protection de la vie privée, à mesure

74 AFPC, *Mémoire à l'intention du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique – Au sujet de – l'étude sur l'utilisation par le gouvernement fédéral d'outils technologiques permettant d'extraire des renseignements personnels des appareils mobiles et des ordinateurs*, 3 mars 2024, p. 1.

que les outils technologiques utilisés par les institutions fédérales deviennent plus puissants et intrusifs.

En ce qui concerne la mise à jour des politiques applicables, la présidente du Conseil du Trésor, l'honorable Anita Anand a annoncé que le Conseil du Trésor s'engage à renouveler les politiques de confidentialité et à mettre à jour la *Directive sur l'ÉFVP*, ce qui comprendrait la rationalisation des ÉFVP et la recherche de façons d'améliorer la directive. Elle a affirmé ce qui suit :

> Nous avons entrepris une action à l'échelle du gouvernement, nous avons consulté des experts en protection de la vie privée au sujet des modifications à apporter à la Directive sur l'évaluation des facteurs relatifs à la protection de la vie privée et nous dialoguons avec le Commissariat à la protection de la vie privée du Canada. Nous avons l'intention de publier la directive à jour cet été[75].

Dominic Rochon, sous-ministre et dirigeant principal de l'information du Canada, du Secrétariat du Conseil du Trésor, a reconnu quant à lui que la version actuelle de la *Directive sur l'ÉFVP* laisse aux ministères une certaine marge de manœuvre pour décider s'il faut ou non mettre à jour les ÉFVP lorsque de nouveaux outils technologiques sont utilisés, ce qui laisse place à l'interprétation. Il a précisé que, dans le cadre de la mise à jour de la directive, certains éléments seront mis en place pour expliquer précisément que l'utilisation de nouveaux outils technologiques requiert une mise à jour des ÉFVP.

Mme Anand a offert l'exemple suivant de ce qui pourrait être clarifié dans le cadre de la mise à jour de la directive :

> Nous voulons préciser que, si vous changez votre logiciel, par exemple, vous aurez besoin d'une ÉFVP dans l'avenir. Vous ne pouvez pas vous fonder sur vos ÉFVP précédentes une fois qu'un nouveau logiciel ou que de nouveaux outils sont utilisés. C'est ce type de clarification que nous voulons apporter.

Dans un document que le Secrétariat du Conseil du Trésor du Canada a fait parvenir au Comité avant la comparution de Mme Anand, il est écrit que la *Directive sur l'ÉFVP* modernisée clarifiera les exigences en matière d'ÉFVP tout en élargissant son champ d'application à un plus grand nombre d'initiatives et qu'elle cherchera, de manière

75 Au moment de l'adoption du présent rapport, le 24 septembre 2024, une *Directive sur l'évaluation des facteurs relatifs à la vie privée* mise à jour n'avait pas été publiée.

générale, à rationaliser et à normaliser le processus d'évaluation parmi les institutions afin de faciliter la soumission des ÉFVP par les institutions[76].

Ce document précise également que les modifications proposées à la *Directive sur l'ÉFVP* favoriseront une plus grande responsabilité et une plus grande transparence et qu'en étendant les exigences en matière d'ÉFVP aux systèmes et aux logiciels, la directive actuelle sera renforcée et la conformité des institutions par rapport aux articles 4 à 8 de la LPRP sera accrue[77].

Questionnée sur la possibilité d'ajouter l'obligation de mener une ÉFVP dans la LPRP, Mme Anand a répondu ce qui suit :

> J'ai parlé avec le ministre Virani hier soir. Je sais qu'il est en train d'examiner la *Loi sur la protection des renseignements personnels* dans son ensemble en adoptant le point de vue d'un ministre de la Justice. Nous mettons actuellement à jour notre propre directive, ce qui relève exclusivement de la compétence du Conseil du Trésor. C'est mon domaine, et je vais donc m'assurer que la liste de contrôle des points... que les ÉFVP et l'analyse des risques qui seront effectuées par les ministères se produiront. Des consultations sont en cours. Nous devons nous assurer de bien faire les choses. C'est un processus systématique, et je reviendrai cet été avec plus d'information sur une directive actualisée.

Mme Anand a rajouté qu'elle coordonne ses efforts avec le ministre de la Justice et le commissaire à la protection de la vie privée pour s'assurer qu'il y a conformité, dans le cadre de la révision de la LPRP qui est en cours, et qu'elle ne souhaite pas précipiter l'adoption de changements majeurs de la *Directive sur l'ÉFVP* ou de la LPRP, à quelques mois de la publication d'une directive révisée.

Selon elle, l'ajout d'une obligation concernant les ÉFVP dans la LPRP est une question qui ne relève pas de son ministère, mais qui relève plutôt du ministre de la Justice. Elle s'est engagée à lui mentionner la possibilité d'inclure cet élément dans un projet de loi qui modifierait la LPRP, en même temps que les considérations nécessaires sur cette question.

Dans le document que le Secrétariat du Conseil du Trésor du Canada a fait parvenir au Comité, il est écrit ce qui suit :

> Le ministère de la Justice mène actuellement un examen de la [*Loi sur la protection des renseignements personnels*] dans le but de la moderniser pour qu'elle réponde aux

76 Secrétariat du Conseil du Trésor du Canada, *Brief : Description du rôle de la présidente du Conseil du Trésor concernant l'utilisation d'outils permettant d'extraire des données à caractère personnel de dispositifs mobiles et d'ordinateurs*, Document de référence soumis au Comité, p. 1 (Document de référence du SCT).

77 *Document de référence du SCT*, p. 2.

> exigences de l'ère numérique et aux attentes des personnes en matière de protection de la vie privée. Cet examen envisage notamment la possibilité de conférer un caractère législatif à l'obligation d'effectuer des évaluations des facteurs relatifs à la vie privée. D'importants travaux d'élaboration de politiques et d'engagement ont été menés à l'appui de l'initiative du ministère de la Justice[78].

Aucun projet de loi visant à modifier la LPRP de façon substantielle n'a été présenté au Parlement depuis son entrée en vigueur en 1983.

Conclusions et recommandations

Le Comité retient la suggestion que lui a faite M. Dufresne de réitérer les recommandations de son rapport de 2022 sur les outils d'enquêtes sur appareil utilisés par la GRC, qui visent notamment à modifier le préambule de la LPRP pour reconnaître le droit à la vie privée comme un droit fondamental, à y inclure le concept de protection de la vie privée dès la conception et à y ajouter des obligations de transparence pour les institutions fédérales.

Dans le document qu'il a fait parvenir au Comité à la suite de sa comparution, M. Dufresne – à l'invitation du Comité – a formulé des recommandations de modifications législatives et a réitéré les recommandations faites lors de sa comparution[79]. Le Comité en a tenu compte dans le libellé des nouvelles recommandations qu'il fait dans le présent rapport.

À la lumière de ce qui précède, le Comité réitère les recommandations suivantes, formulées dans son rapport de 2022 sur l'utilisation des outils d'enquête sur appareil par la GRC, qu'il considère toujours pertinentes dans le cadre de la présente étude[80].

78 *Document de référence du SCT*, p. 1.

79 Commissaire à la protection de la vie privée du Canada, *Lettre au Comité*, 23 février 2024, pp. 1-2.

80 ETHI, *Outils d'enquête sur appareil utilisés par la Gendarmerie royale du Canada et enjeux liés*, rapport, 44e législature, 1e session, novembre 2022. Les recommandations 2, 3, 4, 5 et 6 du présent rapport étaient respectivement les recommandations 1, 4, 6, 7 et 9 du rapport de 2022.

Recommandation 2

Que le gouvernement du Canada modifie la *Loi sur la protection des renseignements personnels* afin d'y inclure une obligation explicite pour les institutions fédérales de faire des évaluations des facteurs relatifs à la vie privée avant d'adopter des outils technologiques à haut risque qui font la collecte de renseignements personnels et de les soumettre au Commissariat à la protection de la vie privée du Canada pour évaluation.

Recommandation 3

Que le gouvernement du Canada modifie le préambule de la *Loi sur la protection des renseignements personnels* et de la *Loi sur la protection des renseignements personnels et les documents électroniques* afin d'indiquer que le droit à la vie privée est un droit fondamental.

Recommandation 4

Que le gouvernement du Canada accorde au Commissariat à la protection de la vie privée du Canada le pouvoir de faire des recommandations et de rendre des ordonnances, tant dans le secteur public que le secteur privé, lorsqu'il constate des violations des lois dont il est responsable.

Recommandation 5

Que le gouvernement du Canada modifie la *Loi sur la protection des renseignements personnels* afin d'inclure le concept de protection de la vie privée dès la conception et une obligation pour les institutions fédérales qui y sont assujetties de respecter cette norme lorsqu'elles développent et utilisent de nouvelles technologies.

Recommandation 6

Que le gouvernement du Canada modifie la *Loi sur la protection des renseignements personnels* afin d'y inclure des exigences explicites en matière de transparence pour les institutions fédérales, sauf lorsque la confidentialité est nécessaire pour protéger les méthodes utilisées par les autorités d'application de la loi et assurer l'intégrité de leurs enquêtes.

Le Comité formule également les nouvelles recommandations suivantes :

Recommandation 7

Que l'obligation pour les institutions fédérales de faire des évaluations des facteurs relatifs à la vie privée en vertu de la *Loi sur la protection des renseignements personnels*, prévue dans la recommandation 2, s'applique notamment lorsqu'une institution fédérale prévoit utiliser un nouvel outil technologique puissant, capable d'avoir une incidence sur la vie privée.

Recommandation 8

Que le gouvernement du Canada modifie la *Loi sur la protection des renseignements personnels* afin d'imposer aux institutions fédérales l'obligation – avant le lancement d'une initiative, d'une activité ou d'un programme qui pourrait avoir une incidence sur la vie privée – de consulter le Commissariat à la protection de la vie privée du Canada, de lui fournir les détails pertinents de cette initiative, de cette activité ou de ce programme dans un délai prescrit et de tenir compte de l'avis du Commissariat à l'issue de cette consultation.

Recommandation 9

Que le gouvernement du Canada modifie la *Loi sur la protection des renseignements personnels* afin d'y inclure les concepts de nécessité et de proportionnalité en imposant aux institutions fédérales l'obligation de démontrer que les activités qu'elles mènent et les programmes qu'elles exécutent qui ont une incidence sur la vie privée sont nécessaires pour atteindre un objectif urgent et important, et que l'atteinte à la vie privée qui en résulte est proportionnelle aux avantages escomptés.

Recommandation 10

Que le gouvernement du Canada mette à jour la *Directive sur l'évaluation des facteurs relatifs à la vie privée* afin d'y assurer la conformité.

Recommandation 11

Que le gouvernement du Canada impose aux institutions fédérales une obligation de consulter le Commissariat à la protection de la vie privée du Canada lorsqu'ils procèdent à l'évaluation des risques d'atteinte à la vie privée de leurs programmes et outils.

Recommandation 12

Que le gouvernement du Canada impose aux institutions fédérales une obligation de procéder à des examens réguliers des évaluations des facteurs relatifs à la vie privée existantes.

Recommandation 13

Que le gouvernement du Canada impose aux institutions fédérales une obligation de rappeler régulièrement à leurs employés leurs obligations concernant la sécurité des appareils et de les tenir au courant à cet égard.

Recommandation 14

Que le gouvernement du Canada examine et mette en œuvre des mesures de protection plus strictes afin de limiter tout accès non nécessaire à des données extraites.

CONCLUSION

Bien que les représentants d'institutions fédérales qui se sont présentés devant le Comité ont indiqué que leur institution accorde beaucoup d'importance à la protection de la vie privée et estime que l'utilisation d'outils de criminalistique numérique se fait en suivant les règles applicables et l'autorité que leur confèrent certaines lois applicables, il ressort de l'étude du Comité que leurs obligations en vertu de la *Directive sur l'ÉFVP* pourraient être plus claires et mieux respectées.

La présidente du Conseil du Trésor a déjà indiqué qu'une mise à jour de cette directive est en cours. Le Comité espère que cette mise à jour renforcera l'obligation pour les institutions fédérales de mener une ÉFVP en temps opportun.

La modernisation de la LPRP pourrait aussi permettre d'ajouter dans la LPRP l'obligation de mener une ÉFVP. Elle pourrait aussi clarifier le besoin de considérer la nécessité et la proportionnalité de toute collecte de renseignements personnels, afin de limiter le nombre de données recueillies par les institutions fédérales à ce qui est absolument nécessaire pour atteindre leurs objectifs.

Le Comité estime que la mise en œuvre des recommandations qu'il présente servirait à améliorer la confiance de la population canadienne envers les institutions fédérales en ce qui concerne la protection de ses renseignements personnels.

ANNEXE A : UTILISATION D'OUTILS DE CRIMINALISTIQUE NUMÉRIQUE PAR LES INSTITUTIONS FÉDÉRALES QUI ONT COMPARU

Le tableau 1 présente quelques détails concernant l'utilisation d'outils de criminalistique numérique des douze institutions fédérales qui ont comparu devant le Comité dans le cadre de cette étude : le programme gouvernemental dans le cadre duquel elle utilise ces outils ou le contexte de l'utilisation; les lois pertinentes au terme desquelles elles mènent des enquêtes et peuvent saisir des appareils électroniques; et l'année d'achat de l'outil, lorsque disponible.

Tableau 1 — Faits saillants concernant l'utilisation d'outils de criminalistique numérique par 12 institutions fédérales

Institution fédérale	Question	Réponse
Agence du revenu du Canada	Programme gouvernemental dans le cadre duquel les outils sont utilisés ou contexte d'utilisation	Programme des enquêtes criminelles de l'Agence de Revenu du Canada.
Agence du revenu du Canada	Lois pertinentes	*Code Criminel* (articles 2 et 487) et pouvoirs de perquisition en vertu des lois dont elle est responsable de l'application.
Agence du revenu du Canada	Année d'achat du ou des outils de criminalistique numérique	2012.
Agence des services frontaliers du Canada	Programme gouvernemental dans le cadre duquel les outils sont utilisés ou contexte d'utilisation	L'Agence des services frontaliers du Canada a la responsabilité de conduire des enquêtes criminelles sur des infractions présumées au titre des lois frontalières.

Institution fédérale	Question	Réponse
Agence des services frontaliers du Canada	Lois pertinentes	Les lois en vertu desquelles elle peut mener des enquêtes incluent la *Loi sur les douanes* et la *Loi sur l'immigration et la protection des réfugiés*.
Agence des services frontaliers du Canada	Année d'achat du ou des outils de criminalistique numérique	2019 (Graykey maintenant connu sous le nom de Magnet Axiom). 2021 (Cellebrite Premium).
Bureau de la Concurrence	Programme gouvernemental dans le cadre duquel les outils sont utilisés ou contexte d'utilisation	Programme d'informatique judiciaire du Bureau de la concurrence.
Bureau de la Concurrence	Lois pertinentes	*Loi sur la concurrence*.
Bureau de la Concurrence	Année d'achat du ou des outils de criminalistique numérique	Pas spécifié.
Bureau de la Sécurité du Transport du Canada	Programme gouvernemental dans le cadre duquel les outils sont utilisés ou contexte d'utilisation	Programme d'enquête du Bureau de la Sécurité du Transport du Canada.
Bureau de la Sécurité du Transport du Canada	Lois pertinentes	*Loi sur le Bureau canadien d'enquête sur les accidents de transport et de la sécurité des transports*.
Bureau de la Sécurité du Transport du Canada	Année d'achat du ou des outils de criminalistique numérique	Pas spécifié.
Conseil de la radiodiffusion et des télécommunications canadiennes	Programme gouvernemental dans le cadre duquel les outils sont utilisés ou contexte d'utilisation	Programme d'outils d'investigation numérique du CRTC.
Conseil de la radiodiffusion et des télécommunications canadiennes	Lois pertinentes	Loi canadienne antipourriel.

Institution fédérale	Question	Réponse
Conseil de la radiodiffusion et des télécommunications canadiennes	Année d'achat du ou des outils de criminalistique numérique	2014.
Gendarmerie royale du Canada	Programme gouvernemental dans le cadre duquel les outils sont utilisés ou contexte d'utilisation	Utilisés dans le cadre d'enquêtes criminelles ou d'enquêtes administratives internes.
Gendarmerie royale du Canada	Lois pertinentes	*Code criminel*.
Gendarmerie royale du Canada	Année d'achat du ou des outils de criminalistique numérique	Pas spécifié.
Ministère de la Défense nationale	Programme gouvernemental dans le cadre duquel les outils sont utilisés ou contexte d'utilisation	Programme ministériel des technologies de l'information et de la communication.
Ministère de la Défense nationale	Lois pertinentes	*Loi sur la gestion des finances publiques*.
Ministère de la Défense nationale	Année d'achat du ou des outils de criminalistique numérique	Pas spécifié.
Environnement et Changement climatique Canada	Programme gouvernemental dans le cadre duquel les outils sont utilisés ou contexte d'utilisation	Programme de criminalistique judiciaire de la Direction générale de l'application de la loi d'Environnement et Changement climatique Canada.
Environnement et Changement climatique Canada	Lois pertinentes	Les lois en vertu desquelles elle peut mener des enquêtes incluent la *Loi canadienne sur la protection de l'environnement*, les dispositions relatives à la prévention de la pollution de la *Loi sur les pêches*, ainsi que la *Loi sur la tarification de la pollution causée par les gaz à effet de serre*.

Institution fédérale	Question	Réponse
Environnement et Changement climatique Canada	Année d'achat du ou des outils de criminalistique numérique	2013
Ministère des Pêches et des Océans	Programme gouvernemental dans le cadre duquel les outils sont utilisés ou contexte d'utilisation	Le Programme de Conservation et Protection de Pêches et Océans Canada a un Service national d'informatique judiciaire et un Service d'enquêteur en criminalistique numérique et pour la cybersécurité.
Ministère des Pêches et des Océans	Lois pertinentes	Les lois en vertu desquelles elle peut mener des enquêtes incluent la *Loi sur les pêches* et la *Loi sur les espèces en péril*.
Ministère des Pêches et des Océans	Année d'achat du ou des outils de criminalistique numérique	2013.
Ministère des Ressources naturelles	Programme gouvernemental dans le cadre duquel les outils sont utilisés ou contexte d'utilisation	s/o
Ministère des Ressources naturelles	Lois pertinentes	s/o
Ministère des Ressources naturelles	Année d'achat du ou des outils de criminalistique numérique	2018 (acheté, mais jamais utilisé)
Service correctionnel Canada	Programme gouvernemental dans le cadre duquel les outils sont utilisés ou contexte d'utilisation	Saisie d'objet interdits (objets de contrebande dans les établissements de correction) en vertu de sa loi habilitante.
Service correctionnel Canada	Lois pertinentes	*Loi sur le système correctionnel et la mise en liberté sous condition*.
Service correctionnel Canada	Année d'achat du ou des outils de criminalistique numérique	2010

Institution fédérale	Question	Réponse
Services partagés Canada	Programme gouvernemental dans le cadre duquel les outils sont utilisés ou contexte d'utilisation	Programme d'enquêtes administratives de Services partagés Canada.
Services partagés Canada	Lois pertinentes	*Loi sur la gestion des finances publiques*.
Services partagés Canada	Année d'achat du ou des outils de criminalistique numérique	Outils obtenus par Services partagés Canada au moment de sa création en 2011.

Source : Comité permanent de la Chambre des communes sur l'accès à l'information, la protection des renseignements personnels et l'éthique (ETHI), *Témoignages*, 1er février 2024; (ETHI), *Témoignages*, 6 février 2024; (ETHI), *Témoignages*, 8 février 2024; (ETHI), *Témoignages*, 13 février 2024; (ETHI); Services partagés Canada, *Réponse écrite au Comité*, 23 avril 2024 [HYPERLIEN NON DISPONIBLE].

ANNEXE B : ACCÈS PAR D'AUTRES INSTITUTIONS FÉDÉRALES À DES LOGICIELS UTILISÉS POUR EXTRAIRE DES INFORMATIONS DE DISPOSITIFS ÉLECTRONIQUES

Le 1er février 2024, le Comité a adopté la motion suivante :

> 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.

Le tableau suivant résume les réponses que le Comité a reçues de la part de 54 institutions fédérales, certaines répondant pour un ministère et ses agences. Parmi ces institutions fédérales, 17 ont répondu par l'affirmative à la question de savoir si elles ont acheté un logiciel permettant d'extraire des informations de dispositifs électroniques ou ont accès à un tel logiciel.

Il est important de noter que le logiciel acheté ou auquel une institution a rapporté avoir accès ne correspond pas nécessairement aux outils de criminalistique numériques précis dont ont parlé les représentants d'institutions fédérales qui ont comparu devant le Comité pendant l'étude, les plus mentionnés étant Cellebrite et Magnet Axiom/GrayKey.

Parmi les 17 institutions qui ont répondu par l'affirmative, seuls le Commissariat à la protection de la vie privée du Canada, les Services administratifs des tribunaux judiciaires et Emploi et Développement social Canada (EDSC) ont acheté Magnet Axiom. EDSC a indiqué avoir acheté ce logiciel, mais ne l'avoir jamais utilisé. Le ministère de la Justice et EDSC ont indiqué avoir acheté Cellebrite, mais comme pour Magnet Axiom, EDSC a indiqué ne l'avoir jamais utilisé. Les autres logiciels auxquels ces institutions ont rapporté avoir accès incluent X-Ways, EnCase, FTK and RECON *ITR*.

Tableau 1 — Accès à un outil de criminalistique numérique

Institution fédérale	**Achat ou accès à des logiciels utilisés pour extraire des informations de dispositifs électroniques**
Agence de promotion économique du Canada atlantique (APECA)	Non
Banque du Canada	Oui
Société d'assurance-dépôts du Canada (SADC)	
Développement économique Canada pour les régions du Québec	Non
Agence canadienne d'inspection des aliments	Non
Instituts de recherche en santé du Canada (IRSC)	Oui
Agence canadienne de développement économique du Nord	Non
Service canadien du renseignement de sécurité (SCRS)	Ne peut répondre
Agriculture et agroalimentaire Canada	Oui
Financement agricole Canada	Oui
Commission canadienne du lait	Non
Commission canadienne des grains	Non
Conseil des produits agricoles du Canada	Non
Ministère du Patrimoine canadien et ses entités (excepté CRTC)	Non
Immigration, Réfugiés et Citoyenneté Canada	Oui
Services aux Autochtones Canada	Oui
Relations Couronne-Autochtones et Affaires du nord	Oui
Emploi et Développement social Canada (EDSC)	Oui
Santé Canada	Oui

Innovation, Sciences et Développement économique Canada (ISDE) et ses organismes	Oui
Ministère de la Justice	Oui
Service administratif des tribunaux judiciaires	Oui
Commissariat à l'information du Canada	Oui
Commissariat à la protection de la vie privée du Canada	Oui
Comité externe d'examen des griefs militaires	Non
Commission d'examen des plaintes concernant la police militaire du Canada	Non
Ombudsman de la Défense nationale et des Forces armées canadiennes	Non
Services publics et Approvisionnement Canada (SPAC)	Oui
Transport Canada	Non
Anciens Combattants Canada	Oui
Surintendant des institutions financières	Non
Bureau du Conseil Privé	Non
Agence de la santé publique du Canada	Oui
Monnaie royale canadienne	Non
Secrétariat du Conseil du trésor	Non
École de la fonction publique du Canada	Non
Centre de la sécurité des télécommunications (CST)	Ne peut répondre
Agence fédérale de développement économique pour le Sud de l'Ontario	Non
Agence fédérale de développement économique pour le Nord de l'Ontario	Non
Ministère des Finances	Non
Infrastructure Canada	Non

Société canadienne d'hypothèques et de logement Canada	Non
Banque de l'infrastructure du Canada	Non
Autorité du pont Windsor-Détroit	Non
Ponts Jacques Cartier et Champlain Incorporée	Non
Poursuites pénales du Canada	Non
Agences sous le portfolio de Ressources naturelles Canada	Non
Développement économique Canada pour les Prairies	Non
Corporation de développement des investissements du Canada	Non
Femmes et Égalité des genres Canada	Non
Agence de la consommation en matière financière du Canada	Non
Centre d'analyse des opérations et déclarations financières du Canada - CANAFE	Non
Parcs Canada	Non
Agence d'évaluation d'impact du Canada	Non

Source: Tableau préparé par la Bibliothèque du Parlement en utilisant de l'information que le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes (ETHI) a obtenu de diverses institutions fédérales et de Services partagés Canada.

ANNEXE C :
LISTE DES TÉMOINS

Le tableau ci-dessous présente les témoins qui ont comparu devant le Comité lors des réunions se rapportant au présent rapport. Les transcriptions de toutes les séances publiques reliées à ce rapport sont affichées sur la page Web du Comité sur cette étude.

Organismes et individus	Date	Réunion
Commissariat à la protection de la vie privée du Canada	2024/02/01	100
Lara Ives, directrice exécutive, direction des politiques, de la recherche et des affaires parlementaires		
Commissariats à l'information et à la protection de la vie privée au Canada	2024/02/01	100
Philippe Dufresne, commissaire à la protection de la vie privée du canada		
Agence des services frontaliers du Canada	2024/02/06	101
Aaron McCrorie, vice-président, renseignement et exécution de la loi		
Gendarmerie royale du Canada	2024/02/06	101
Nicolas Gagné, surintendant		
Bryan Larkin, sous-commissaire, services de police spécialisés		
Ministère de la Défense nationale	2024/02/06	101
Sophie Martel, dirigeante principale de l'information par intérim		
Dave Yarker, directeur général, cybersécurité et commandement et contrôle des opérations des systèmes d'information		
Ministère des Ressources naturelles	2024/02/06	101
Francis Brisson, sous-ministre adjoint et dirigeant principal des finances		
Pierre Pelletier, dirigeant principal de l'information		

Organismes et individus	Date	Réunion
Service correctionnel du Canada	2024/02/06	101
France Gratton, commissaire adjointe, opérations et programmes correctionnels		
Tony Matson, commissaire adjoint et dirigeant principal des finances, services corporatifs		
Agence du revenu du Canada	2024/02/08	102
Eric Ferron, directeur général, direction des enquêtes criminelles, direction générale des programmes d'observation		
Anne Marie Laurin, directrice générale par intérim et chef adjointe de la protection des renseignements personnels, division de l'accès à l'information et protection des renseignements personnels, direction générale des affaires publiques		
Conseil de la radiodiffusion et des télécommunications canadiennes	2024/02/08	102
Steven Harroun, chef de l'application de la conformité et enquêtes		
Anthony McIntyre, avocat général et sous-directeur exécutif, services juridiques		
Ministère de l'Environnement	2024/02/08	102
Hannah Rogers, directrice générale, application de la loi en environnement		
Donald Walker, responsable de la mise en application de la loi		
Ministère des Pêches et des Océans	2024/02/08	102
Brent Napier, directeur général par intérim, conservation et protection		
Sam Ryan, directeur général, services techniques intégrés		
Bureau de la concurrence Canada	2024/02/13	103
Pierre-Yves Guay, commissaire délégué, direction des cartels		
Mario Mainville, dirigeant principal de l'application numérique		

Organismes et individus	Date	Réunion
Bureau de la sécurité des transpors du Canada	2024/02/13	103
Luc Casault, directeur général, services intégrés		
Kathy Fox, présidente		
Services partagés Canada	2024/02/13	103
Scott Jones, président		
Daniel Mills, sous-ministre adjoint, direction générale de l'approvisionnement en TI pour l'entreprise et des services ministériels		
À titre personnel	2024/02/15	104
Evan Light, professeur agrégé		
Association canadienne des employés professionnels	2024/02/15	104
Nathan Prier, président		
Laura Shantz, conseillère principale, défense des droits et campagnes		
L'Institut professionnel de la fonction publique du Canada	2024/02/15	104
Jennifer Carr, présidente		
Stéphanie Montreuil, gestionnaire, affaires publiques		
Secrétariat du Conseil du Trésor	2024/03/21	109
L'hon. Anita Anand, présidente du conseil du trésor		
Dominic Rochon, sous-ministre et dirigeant principal de l'information du canada		

ANNEXE D :
LISTE DES MÉMOIRES

Ce qui suit est une liste alphabétique des organisations et des personnes qui ont présenté au Comité des mémoires reliés au présent rapport. Pour obtenir de plus amples renseignements, veuillez consulter la page Web du Comité sur cette étude.

Alliance de la Fonction publique du Canada

DEMANDE DE RÉPONSE DU GOUVERNEMENT

Conformément à l'article 109 du Règlement, le Comité demande au gouvernement de déposer une réponse globale au présent rapport.

Un exemplaire des *procès-verbaux* pertinents (réunions nos 100, 101, 102, 103, 104, 109 et 128) est déposé.

Respectueusement soumis,

Le président,
John Brassard