



CHAMBRE DES COMMUNES  
HOUSE OF COMMONS  
CANADA

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

---

ETHI • NUMÉRO 018 • 2<sup>e</sup> SESSION • 41<sup>e</sup> LÉGISLATURE

---

TÉMOIGNAGES

**Le mardi 8 avril 2014**

—  
**Président**

**M. Pat Martin**



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

Le mardi 8 avril 2014

• (1100)

[Traduction]

**Le président (M. Pat Martin (Winnipeg-Centre, NPD)):** Bonjour, mesdames et messieurs. Commençons notre séance.

Bienvenue à la 18<sup>e</sup> séance du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique.

Nous poursuivons aujourd'hui notre étude du problème grandissant du vol d'identité et de ses répercussions économiques.

Nous avons le plaisir d'accueillir, en qualité de témoins et de conférenciers, M. Philippe Dufresne, directeur général et avocat général principal à la Commission canadienne des droits de la personne, ainsi que Mme Susan Gardner-Barclay, sous-commissaire et chef de la protection des renseignements personnels, Direction générale des affaires publiques, qui est accompagnée de Mme Helen Brown, directrice générale, Direction de la sécurité et des affaires internes, Direction générale des finances et de l'administration, toutes deux de l'Agence canadienne du revenu.

Nous entendrons d'abord les déclarations préliminaires de nos invités. Nous commencerons par M. Dufresne, de la Commission canadienne des droits de la personne.

Comme cela est d'usage, nous vous demandons de présenter un exposé d'environ 10 minutes, à la suite duquel nous inviterons les membres du comité à poser des questions.

Bienvenue, monsieur Dufresne. Vous avez la parole.

**M. Philippe Dufresne (directeur général et avocat général principal, Direction générale de la promotion des droits de la personne, Commission canadienne des droits de la personne):** Monsieur le président, je vous remercie d'inviter la Commission canadienne des droits de la personne (CCDP) à participer à votre étude du problème grandissant du vol d'identité et de ses répercussions économiques.

J'aimerais vous présenter mon collègue Maciej Karpinski, analyste principal de recherche à la Direction générale de la promotion des droits de la personne.

Aujourd'hui, j'aimerais traiter de trois questions importantes. Je commencerai par parler brièvement de la Commission canadienne des droits de la personne et de la façon dont nous assurons la promotion et la protection des droits de la personne, de même que l'égalité des chances. Je parlerai ensuite du rapport sur la certification de l'identité qu'a publié la Commission en 2010 et du fait qu'il est important de veiller à ce que les mesures utilisées pour certifier l'identité d'un individu soient conformes aux principes des droits de la personne. Enfin, je vous communiquerai nos recommandations sur la façon d'éviter la discrimination dans ce domaine.

[Français]

Je vais commencer par une brève description de la commission et de son mandat.

Nous avons reçu du Parlement le mandat de veiller à l'application de la Loi canadienne sur les droits de la personne et de vérifier la conformité des organisations fédérales à la Loi sur l'équité en matière d'emploi.

Nous recevons des plaintes de discrimination concernant l'emploi et les services offerts par les organisations relevant de la compétence fédérale. Cela comprend la fonction publique fédérale de même que les entreprises du secteur privé oeuvrant dans certaines industries, telles que les transports, les télécommunications et les services bancaires.

Nous participons également, comme partie, à des dossiers importants en matière de droits de la personne devant des tribunaux judiciaires et quasi judiciaires, incluant la Cour suprême du Canada.

La commission travaille également à prévenir la discrimination et à favoriser le développement d'une culture durable axée sur les droits de la personne. Nous y arrivons en fournissant aux organisations des recherches, des politiques et des outils qui contribuent à la compréhension et au respect de la Loi canadienne sur les droits de la personne.

L'un de ces outils est l'évaluation des répercussions des mesures de sécurité sur les droits de la personne, dont je parlerai plus tard dans mon allocution

[Traduction]

Le rapport dont vous nous avez demandé de parler aujourd'hui a été publié en 2010. Il faisait partie d'une initiative de recherche liée à la sécurité nationale et aux droits de la personne. Notre objectif était alors d'aider les organisations chargées de la sécurité nationale à renforcer leurs pratiques en matière de certification de l'identité d'une manière conforme aux droits de la personne.

Bien que notre rapport soit axé sur les organisations de sécurité nationale, ses conclusions, à notre avis, sont pertinentes pour toutes les organisations publiques et privées qui offrent des services nécessitant des renseignements sur l'identité. Nous espérons donc que l'information contenue dans notre rapport sera utile aux travaux de votre comité.

[Français]

Notre rapport a démontré que les formes de certification d'identité les plus fréquemment utilisées présentent le risque d'être discriminatoires en vertu des motifs de distinction illicites prévus dans la Loi canadienne sur les droits de la personne, et ce, pour deux raisons.

Premièrement, la méthode utilisée peut être inaccessible à une personne ou à un groupe de personnes. Deuxièmement, les décisions discrétionnaires prises par les agents concernant la validation de l'identité peuvent conduire à de la discrimination.

[Traduction]

Notre rapport a montré l'existence de deux grands systèmes de mesure pour l'établissement de l'identité. Le premier est unimodal, c'est-à-dire qu'il ne comporte qu'une seule mesure, tandis que l'autre est multimodal, et requiert deux mesures ou plus.

Par exemple, il est possible qu'un système unimodal n'utilise que les empreintes digitales. Ce système peut alors ne pas être accessible aux gens qui n'ont pas de doigts ou dont les empreintes digitales se sont partiellement dégradées en raison de leurs conditions de travail ou de leur âge. À l'inverse, notre étude a montré que les systèmes biométriques multimodaux offrent un degré d'inclusivité qui permet souvent de pallier les limites des systèmes unimodaux. Les systèmes multimodaux peuvent non seulement aider à protéger les droits de la personne, mais ils permettent également de bâtir un système de sécurité plus fort et plus fiable.

Lors de l'examen, la carte Personal Identity Certifier a été désignée comme système multimodal efficace aux États-Unis. Pour chaque employé fédéral ou entrepreneur inscrit, la carte enregistre à la fois les empreintes digitales et les données biométriques résultant d'un balayage du visage. Bien qu'on utilise principalement la biométrie des empreintes digitales, on a recours à la lecture numérique du visage lorsqu'il est impossible pour un employé fédéral ou un entrepreneur de fournir des empreintes digitales ou lorsqu'il y a des anomalies.

Lorsqu'il faut décider de ces questions importantes, les dispositions législatives sur les droits de la personne fournissent une orientation pour déterminer si une mesure qui serait autrement discriminatoire peut être justifiée. Il faut d'abord examiner à quel point la mesure est nécessaire, ensuite, déterminer s'il existe des moyens moins discriminatoires pour atteindre le même objectif et, enfin, établir à quel point l'atteinte aux droits de la personne l'emporte sur l'avantage offert par la mesure.

Il peut arriver également que certains utilisateurs aient besoin d'une exemption. Il faut donc prévoir, dans l'élaboration de toute mesure, des politiques et des pratiques acceptables permettant de répondre aux besoins de ces personnes. S'il n'existe aucune solution de rechange acceptable à une mesure biométrique particulière, il revient à l'organisation qui utilise la biométrie de démontrer que des efforts suffisants ont été déployés pour explorer d'autres moyens moins discriminatoires d'en arriver aux mêmes résultats.

En nous appuyant sur ces principes, nous avons élaboré l'Évaluation des impacts des mesures de sécurité sur les droits de la personne. Cet outil énonce les dispositions à prendre au cours du cycle de vie d'une mesure de sécurité pour que les normes de sécurité, les politiques et les pratiques soient à la fois efficaces et respectueuses des droits de la personne.

• (1105)

[Français]

Nous sommes d'avis que la conduite d'une évaluation des répercussions sur les droits de la personne avant la mise en oeuvre d'une mesure de sécurité permet non seulement d'améliorer l'efficacité et l'efficience de cette mesure, mais également de gagner du temps et de l'argent, tout en renforçant l'appui de la population aux initiatives de sécurité, qu'elles soient nouvelles ou actuelles.

Voilà ce que nous voulons dire quand nous demandons aux organisations d'analyser sous l'angle des droits de la personne les politiques ou les procédures proposées.

[Traduction]

Je vous remercie de votre attention. Nous serons heureux de répondre à vos questions.

**Le président:** Merci, monsieur Dufresne.

Je donne maintenant la parole à Mme Susan Gardner-Barclay, de l'Agence du revenu du Canada.

Vous disposez d'environ 10 minutes. Veuillez commencer, madame Gardner-Barclay.

**Mme Susan Gardner-Barclay (sous-commissaire et chef de la protection des renseignements personnels, Direction générale des affaires publiques, Agence du revenu du Canada):** Bonjour, monsieur le président, et merci beaucoup.

Bonjour aux membres du comité.

Je m'appelle Susan Gardner-Barclay, et je suis sous-commissaire de la Direction générale des affaires publiques et chef de la protection des renseignements personnels à l'Agence du revenu du Canada, ou ARC.

Je suis accompagnée aujourd'hui par Helen Brown, notre directrice générale de la Direction de la sécurité et des affaires internes à la Direction générale des finances et de l'administration.

[Français]

Nous sommes très heureuses de comparaître devant vous aujourd'hui afin de vous aider dans votre étude sur le problème croissant qu'est le vol d'identité en parlant des mesures que l'ARC a mises en place pour protéger les renseignements des contribuables.

[Traduction]

En tant qu'une des plus grandes institutions du gouvernement du Canada, l'ARC a plus d'interactions avec les Canadiens que tout autre ministère. En 2012-2013 seulement, plus de 27 millions de Canadiens et d'entreprises ont produit une déclaration de revenus ou une déclaration de revenus et de prestations. L'ARC perçoit environ 400 milliards de dollars par année en taxes, impôts et droits, et elle distribue 22 milliards de dollars en crédits et prestations aux Canadiens. Nos centres d'appels reçoivent 20 millions d'appels par année, et nous traitons plus de 150 millions de pièces de correspondance. Nous avons donc l'un des plus importants fonds de données de renseignements personnels du gouvernement du Canada.

La confiance que les Canadiens accordent à l'ARC pour ce qui est de protéger leurs renseignements est la pierre angulaire du régime canadien d'autocotisation volontaire. En outre, l'article 241 de la Loi de l'impôt sur le revenu et l'article 295 de la Loi sur la taxe d'accise interdisent à tout employé de l'ARC de divulguer des renseignements sur les contribuables, à moins d'y être spécifiquement autorisé en vertu de ces lois. La violation de ces dispositions est une infraction criminelle qui peut entraîner des pénalités sévères pouvant aller jusqu'à l'emprisonnement.

[Français]

C'est pourquoi l'ARC a mis en place un grand nombre de mesures de protection visant à protéger les renseignements personnels et, ainsi, à réduire les risques de vol d'identité.

D'abord et avant tout, l'agence a travaillé avec diligence pour promouvoir une solide culture d'intégrité parmi ses employés.

•(1110)

[Traduction]

Notre Code de déontologie et de conduite nous permet d'informer clairement les employés du fait que la protection des renseignements personnels des contribuables est au cœur de leurs responsabilités et que ces responsabilités demeurent même une fois qu'ils ont quitté l'ARC.

En 2012, l'ARC a lancé son Cadre d'intégrité, qui regroupe tous ses programmes, systèmes et politiques visant à protéger son intégrité. Grâce à ce cadre, les normes élevées établies pour protéger la vie privée des contribuables sont communiquées à tous les employés et gestionnaires et le rendement de l'Agence par rapport à ces normes fait l'objet d'une surveillance et de rapports minutieux.

De plus, l'ARC collabore très étroitement avec le commissaire à la protection de la vie privée du Canada pour veiller à ce que les mesures de protection soient solides et à ce que les améliorations requises soient apportées.

En 2009 et en 2013, la commissaire à la protection de la vie privée a réalisé des vérifications du système de gestion de la protection de la vie privée de l'ARC. Au cours de ces vérifications, la commissaire a reconnu la portée et la complexité immenses de l'environnement opérationnel de l'ARC, de même que la culture de sécurité et de confidentialité établie à l'ARC. Naturellement, la commissaire a aussi relevé des points à améliorer qui portaient sur l'exécution uniforme et opportune des évaluations des impacts sur la vie privée; la réalisation d'évaluations du risque pour tous les systèmes de la TI qui traitent des renseignements sur les contribuables; le renforcement de la surveillance de l'accès des employés aux systèmes informatiques et l'amélioration des processus d'échange internes de renseignements sur les atteintes à la vie privée. L'ARC a avalisé toutes les recommandations et elle a réalisé d'importants progrès pour y donner suite, beaucoup d'activités ayant déjà été menées à bonne fin pour cela.

[Français]

Cela comprend la création du rôle de chef de la protection des renseignements personnels en avril 2013. C'est un rôle que j'assume depuis qu'on m'a nommée en octobre dernier sous-commissaire de la Direction générale des affaires publiques et chef de la protection des renseignements personnels.

[Traduction]

En tant que chef de la protection des renseignements personnels, j'ai la responsabilité de superviser toutes les décisions liées à la protection de la vie privée à l'ARC, de promouvoir le respect des droits à la protection des renseignements personnels dans notre organisation et de rendre des comptes à ce sujet.

L'ARC cherche aussi à apporter de nombreux autres changements aux programmes, aux politiques et aux technologies pour mieux gérer la protection de la vie privée. Entre autres, nous misons sur nos contrôles de première ligne pour que les employés aient seulement accès aux systèmes informatiques de l'ARC dont ils ont besoin pour faire leur travail. Nous renforçons également nos contrôles secondaires en misant sur nos systèmes automatisés pour que l'ARC puisse mieux surveiller et analyser toutes les opérations effectuées par ses employés sur leurs ordinateurs.

De nouveaux protocoles de communication de renseignements ont été établis à l'agence pour que les questions relatives à la protection de la vie privée fassent l'objet d'une surveillance et de rapports exacts. Nous avons mis sur pied un Comité consultatif sur l'intégrité, qui est présidé par le commissaire de l'ARC et qui compte

parmi ses membres un conseiller en intégrité externe. Nous réalisons aussi un exercice à l'échelle de l'agence afin que les évaluations des facteurs relatifs à la vie privée soient à jour pour tous les programmes et toutes les initiatives qui en nécessitent une.

L'ARC sait très bien que, en raison de la nature des fonds de renseignements qu'elle détient, une atteinte à la sécurité des renseignements personnels peut représenter un risque que des renseignements servent au vol d'identité ou à d'autres activités criminelles.

La nature des atteintes à la sécurité des renseignements qui ont lieu à l'ARC est extrêmement variée. Elle peut aller d'un employé qui accède par erreur au dossier du mauvais contribuable dans l'exercice de ses fonctions, au courrier mal acheminé, qui constitue 95 p. 100 des atteintes à la sécurité de l'information et des données et à la vie privée de l'ARC, et à de rares cas où les renseignements personnels auxquels on accède pourraient servir à de la fraude ou à un gain financier.

Il est important de noter qu'un grand nombre des atteintes à la sécurité des données relevées par l'ARC ne constituent pas des atteintes à la vie privée, puisque aucun renseignement personnel n'a été divulgué. Toutefois, lorsque l'ARC découvre qu'une atteinte à la vie privée a eu lieu, la situation est évaluée en conformité avec la politique et les procédures du Conseil du Trésor, l'incident est donc consigné et tous les risques potentiels pour la personne touchée sont évalués.

Lorsqu'il y a un risque raisonnable que l'atteinte à la vie privée porte préjudice à une personne, cette dernière en est avisée. La commissaire à la protection de la vie privée en est aussi informée, en conformité avec les lignes directrices du Conseil du Trésor.

Avant de conclure, j'aimerais parler brièvement de ce que l'ARC fait pour mettre en garde les Canadiens contre les stratagèmes d'hameçonnage par des tiers qui tentent de se faire passer pour des représentants de l'ARC afin d'obtenir des renseignements personnels de nature délicate. Cette année, nous avons constaté une nette augmentation de ces stratagèmes au cours de la période de production des déclarations de revenus, et l'ARC continue de prendre diverses mesures pour mettre en garde les Canadiens à leur sujet. Notre site Web fournit des renseignements faciles à trouver sur la forme que prennent ces stratagèmes et sur ce qu'il faut faire pour réduire le risque de vol d'identité. Nous diffusons aussi des alertes fiscales et des communiqués de presse aux médias, et nous attirons fréquemment l'attention des Canadiens sur ces renseignements à l'aide du compte Twitter de notre organisation.

Pour entrer en contact avec certains groupes, par exemple les aînés et d'autres groupes vulnérables, qui peuvent ne pas avoir accès à Internet, nous avons adopté une stratégie média proactive dans laquelle nous offrons des entrevues aux médias spécialisés, et ce, en diverses langues, selon les régions, en punjabi, en hindi, en cantonais, en italien et en grec notamment. Nous avons aussi établi un solide réseau d'intermédiaires - des organismes d'aînés et de jeunes, des groupes multiculturels, des associations policiers, des spécialistes en déclarations de revenus, entre autres - qui communiquent nos renseignements à leurs clients et communautés. Et nous nous associons à d'autres organisations gouvernementales pour faire passer le message au cours d'événements comme le Mois de la prévention de la fraude. Lorsque le vol d'identité se produit malgré tout, l'ARC peut et pourra marquer les dossiers des contribuables pour les protéger contre les activités suspectes.

Bref, monsieur le président, l'ARC s'attache à mettre en place des mesures de contrôle, à les évaluer et à les améliorer.

• (1115)

[Français]

Notre responsabilité de protéger les renseignements des Canadiens est essentielle à notre raison d'être et à nos activités. Nous continuons de déployer beaucoup d'efforts afin de répondre aux attentes des Canadiens à cet égard.

[Traduction]

C'est avec plaisir que nous répondrons à vos questions.

**Le président:** Merci, Mme Gardner-Barclay

Nous allons procéder aux séries de questions.

Pour l'opposition officielle et la première série de questions de sept minutes, je donne la parole à Mme Charmaine Borg.

[Français]

**Mme Charmaine Borg (Terrebonne—Blainville, NPD):** Merci, monsieur le président.

J'aimerais tout d'abord remercier les témoins d'être présents parmi nous aujourd'hui. Vous avez sûrement un horaire chargé, mais vous avez pris le temps de venir nous parler d'un enjeu très important. C'est très apprécié.

J'aimerais commencer en posant une question aux représentants de l'Agence du revenu du Canada.

Dans votre présentation, vous avez mentionné qu'il y a eu plusieurs atteintes aux données. En réponse à une question écrite d'un de mes collègues, vous avez déclaré qu'au sein de votre ministère, il y a eu 2 983 atteintes ou pertes de données qui auraient affectées 2 249 personnes. Cela équivaut à plus de la moitié des pertes ou atteintes aux données si on tient compte la totalité des agences fédérales actives. C'est un taux extrêmement élevé d'atteintes aux données pour une seule année.

Avec un si grand nombre d'atteintes ou de pertes aux données, que planifiez-vous faire pour mieux gérer les renseignements personnels des Canadiens et diminuer les risques de vol d'identité qui pourraient découler de ces atteintes aux données?

[Traduction]

**Mme Susan Gardner-Barclay:** Permettez-moi de vous donner un peu de contexte au sujet des chiffres apparaissant à la question écrite 255, qui est, je crois, celle à laquelle vous vous reportez.

Dans cette réponse, il est indiqué que l'ARC a éprouvé environ 2 900 atteintes à la sécurité des renseignements, à la vie privée et à la sécurité des données au cours de la période visée. Quelque 2 800 de ces atteintes étaient en fait des erreurs d'acheminement de courrier. Cela représente environ 0,001 p. 100 des 150 millions de pièces de correspondance que l'ARC traite chaque année.

Naturellement, nous comprenons que nous devons prendre des mesures fermes chaque fois que de l'information concernant un contribuable aboutit au mauvais endroit. Nous avons bel et bien des mesures en place pour traiter les cas d'erreurs d'acheminement de courrier, ce dont ma collègue, Helen Brown, pourra parler.

Je voudrais également vous informer des mesures que nous avons prises à la suite des deux vérifications effectuées par la commissaire à la protection de la vie privée en 2009 et en 2013, auxquelles j'ai fait allusion dans mes déclarations préliminaires.

Essentiellement, nous disposons maintenant d'un mécanisme à plusieurs niveaux pour gérer les atteintes à la sécurité des renseignements et à la vie privée.

Notre première ligne de défense, il va sans dire, ce sont nos employés. Nous avons un code de déontologie très strict qui énonce très, très clairement à nos employés les responsabilités qui leur incombent pour la gestion de la sécurité.

Nous offrons à notre personnel de la formation et de la sensibilisation continues. Nous donnons également à tous les employés de l'ARC un cours sur la sécurité. De plus, nous appliquons maintenant, à l'intérieur de l'ARC, des protocoles complets de communication des renseignements qui nous aident à repérer et à corriger les atteintes qui peuvent survenir; ces protocoles lient tout particulièrement notre direction de la sécurité et des conseils à notre direction de l'AIPRP, à qui incombe la responsabilité de surveiller ces situations.

Nous disposons maintenant de contrôles de première ligne actifs pour nos systèmes technologiques grâce auxquels les seuls systèmes informatiques accessibles aux employés sont ceux dont ils ont besoin pour faire leur travail. Nous avons également des systèmes secondaires très solides que nous travaillons à renforcer davantage au moyen de changements technologiques qui seront mis en place au cours des deux prochaines années. Nous disposerons de systèmes qui nous permettront de surveiller très étroitement les activités des employés sur tous nos systèmes informatiques et de connaître jusqu'aux fichiers auxquels ils ont accès, comment ils y ont accès et quelle information ils y cherchent.

Nous avons un régime très ferme de politiques et de pratiques connexes, y compris une politique disciplinaire très stricte dans laquelle un accès non autorisé est considéré comme une infraction considérablement grave. Nous disposons aussi d'un processus de surveillance très solide, auquel mon bureau participe. Y participent également le comité consultatif sur l'intégrité dont j'ai parlé et, naturellement, le Commissariat à la protection de la vie privée, qui s'intéresse de près à notre dispositif de protection de la vie privée.

[Français]

**Mme Charmaine Borg:** Merci beaucoup.

Madame Brown, vous aurez peut-être l'occasion de répondre à ma prochaine question.

Vous avez dit que 2 800 correspondances ont été envoyées à la mauvaise personne. À ce propos, un de mes concitoyens est venu me voir avec une lettre lui annonçant qu'il était maintenant admissible à la Sécurité de la vieillesse. Sa lettre était accompagnée d'une lettre adressée à une autre personne. Évidemment, ces lettres contenaient des renseignements extrêmement confidentiels. Dans ce cas en question, j'ai moi-même averti l'Agence du revenu du Canada.

Si cela est arrivé dans mon comté, j'imagine que cela est arrivé à plusieurs personnes. Vous avez parlé de 2 800 personnes. Que faites-vous dans de tels cas? Pourquoi nous retrouvons-nous avec une situation où 2 800 correspondances ont été envoyées à de mauvaises personnes?

Personnellement, même si vous dites que c'est un faible pourcentage, il s'agit quand même d'un nombre assez élevé de personnes. Cela peut ouvrir la porte à 2 800 vols d'identité. Selon moi, c'est très sérieux.

• (1120)

[Traduction]

**Mme Helen Brown (directrice générale, Direction de la sécurité et des affaires internes, direction générale des finances et de l'administration, Agence du revenu du Canada):** Je vous remercie de votre question.

C'est un sujet très important. Notre objectif serait de n'avoir aucune erreur d'acheminement de courrier, si cela était possible, et nous avons pris de nombreuses dispositions... je ne sais pas quand l'incident vous concernant s'est produit, mais nous avons mis en place au cours de la dernière année un protocole au moyen duquel chaque fois que quelqu'un nous informe d'une erreur d'acheminement de courrier, des employés de nos services de sécurité prennent contact avec cette personne à l'intérieur d'une journée et nous trouvons un moyen de récupérer la pièce de correspondance concernée.

Nous visons à récupérer les pièces de correspondance mal acheminées à l'intérieur de quatre jours. Nous réussissons à récupérer ces articles dans 95 p. 100 des cas. Nous cherchons à connaître la cause du problème de façon à pouvoir réduire le risque que l'erreur se produise de nouveau, et nous en informons le contribuable si nous estimons qu'il peut y avoir un préjudice.

[Français]

**Mme Charmaine Borg:** Comment prévenir cela?

Admettons que je reçoive une lettre de la Sécurité de la vieillesse et celle d'une autre personne. Si j'étais une personne malveillante, je pourrais utiliser ces informations confidentielles pour faire un vol d'identité.

Comment pouvez-vous rassurer le bénéficiaire de la prestation que l'individu qui a reçu la mauvaise lettre ne va pas utiliser les informations qu'elle contient à des fins criminelles?

[Traduction]

**Mme Helen Brown:** Pour répondre à votre question, je dirais tout d'abord que nous tenterions en premier lieu de récupérer la lettre le plus rapidement possible. Ensuite, si nous estimions que le contribuable pourrait subir un préjudice, nous l'informerions de la situation et l'encouragerions à communiquer avec l'ARC. Nous pourrions soit lui offrir une aide au moyen d'Equifax, un organisme qui offre des services pour le crédit, et nous pourrions accoler un fanion à son dossier pour signaler l'existence d'un risque potentiel de vol d'identité.

**Le président:** Merci, madame Brown.

Je vous prie de m'excuser, madame Borg, le temps qui est accordé est expiré.

Maintenant, la parole est aux conservateurs; allez-y madame Hawn.

**L'hon. Laurie Hawn (Edmonton-Centre, PCC):** Je remercie les témoins de comparaître devant nous.

J'aimerais parler encore un peu des conséquences de tels incidents, qui sont rares — et c'est bien tant mieux. Histoire simplement de nous rafraîchir la mémoire sur les chiffres — dans le cas de l'ARC — avez-vous dit 150 millions de pièces de correspondance envoyées?

**Mme Susan Gardner-Barclay:** Nous gérons 150 millions de pièces de correspondance; 120 millions de ces articles sont envoyés par l'ARC et le reste est constitué de pièces retournées à l'ARC. Cela fait 150 millions en tout.

**L'hon. Laurie Hawn:** Vous avez dit, je crois, que 0,001 p. 100 des pièces de correspondance que vous envoyez aboutissent à la mauvaise adresse.

**Mme Susan Gardner-Barclay:** C'est exact.

**L'hon. Laurie Hawn:** Quel est le chiffre brut? Était-ce les 5 p. 100 des 2 800?

**Mme Helen Brown:** Bonne question.

**Mme Susan Gardner-Barclay:** Le nombre s'élève à environ 1 600.

**L'hon. Laurie Hawn:** D'accord.

Est-il arrivé que des pièces de correspondance acheminées à la mauvaise adresse soient tombées dans les mains de personnes malveillantes? Il n'y a pas beaucoup de mauvaises personnes dans la population et le risque qu'une lettre tombe sur l'une d'elles est vraiment très mince. Toutefois, est-il arrivé qu'une erreur d'acheminement de courrier ait eu des répercussions négatives sur un contribuable?

**Mme Susan Gardner-Barclay:** Nous n'avons aucune preuve qu'une situation semblable s'est produite. En fait, la grande majorité du courrier qui fait l'objet d'erreurs d'acheminement ne contient aucun renseignement personnel.

**L'hon. Laurie Hawn:** Concernant la question légitime de Mme Borg, je dirais que les probabilités qu'une telle situation se présente sont infimes.

Pour ce qui est de l'expérience des droits de la personne que vous avez eue, je ne sais pas trop comment vous caractériseriez les répercussions d'un incident d'acheminement du courrier. À mon sens, trois situations peuvent survenir : une personne pourrait utiliser l'information à des fins d'extorsion, ou s'en servir simplement pour le vol d'identité ou pour frauder une personne âgée vulnérable ou quelque chose comme cela.

Avez-vous des données sur la fréquence de telles situations?

**M. Philippe Dufresne:** Nous n'avons pas effectué de recherches pour connaître la fréquence du vol d'identité ou de l'utilisation d'informations qui pourraient avoir été volées. Notre rapport porte sur le type d'informations que nous utilisons et le genre de mesures dont nous nous servons pour certifier l'identité des Canadiens qui veulent avoir accès aux services, avoir accès au Canada, etc. et sur les répercussions négatives possibles de ces mesures sur les droits de la personne et les dispositions que nous pouvons prendre pour prévenir ces répercussions.

Nous avons constaté que les efforts déployés pour utiliser des mesures qui respectent les droits de la personne ne menacent en rien la sécurité; ils la renforcent dans les faits. Le respect des droits de la personne et la sécurité sont tout à fait compatibles.

• (1125)

**L'hon. Laurie Hawn:** D'accord.

Ma question s'adresse aux deux organismes. À l'évidence, beaucoup d'efforts sont déployés pour assurer la sécurité de l'information, et chaque organisme fait sa part à cet égard. Dans quelle mesure des organismes comme la Commission canadienne des droits de la personne, la Sécurité publique, l'ARC, etc. communiquent-ils entre eux pour faire connaître leurs pratiques exemplaires?

À vous de décider qui va me répondre.

**Mme Susan Gardner-Barclay:** La participation est très active à deux niveaux. Ce sont les responsables de l'accès à l'information qui interviennent en premier. Nous participons aux réunions des comités permanents interministériels du personnel de l'AIPRP où nous parlons de nos pratiques exemplaires. D'ailleurs, nous avons présenté récemment à d'autres organismes fédéraux un exposé sur la création du poste de responsable de la protection de la vie privée et sur le rôle de cette personne dans d'autres organismes. Mme Brown participe également aux activités d'un groupe semblable d'organismes qui se penche sur les mesures de sécurité organisationnelles.

**Mme Helen Brown:** J'aimerais ajouter à ce que ma collègue vient de dire qu'un groupe d'agents de sécurité ministériels très actif à Ottawa se réunit fréquemment pour échanger sur les pratiques exemplaires. En fait, l'ARC est l'un de ceux qui font part de leurs pratiques exemplaires, parce qu'elle est perçue comme un chef de file.

**L'hon. Laurie Hawn:** Oui, vous seriez l'un des plus importants.

Qu'en est-il de la Commission canadienne des droits de la personne?

**M. Philippe Dufresne:** Nous avons à la commission le double mandat de protéger les droits de la personne et d'en faire la promotion. Nous sommes un organisme de réglementation, nous recevons des plaintes et nous participons à l'examen de cas, mais nous avons également le mandat très important de travailler avec les intervenants pour favoriser les droits de la personne, effectuer des recherches dans le domaine et communiquer de l'information. Ce faisant, nous communiquons de l'information aux ministères, comme le ministère de la Justice, et aux organismes.

Pour cette recherche, nous avons consulté un certain nombre d'organismes visés par la sécurité nationale, dont les Affaires étrangères, Passeport Canada et CIC, auxquels nous avons communiqué nos pratiques exemplaires.

Dans ce cas-là, il fallait trouver des options concernant les méthodes utilisées pour identifier les Canadiens et tenter de recueillir de l'information afin d'éviter que les décisions discrétionnaires prises pénalisent un groupe donné.

**L'hon. Laurie Hawn:** D'accord.

Au sujet des mesures disciplinaires visant le personnel — pour plus de précisions — j'imagine que vous avez vraisemblablement à l'ARC un régime très strict de surveillance et de filtrage pour quoi que ce soit entre chez vous.

L'ARC est l'un de ces organismes que beaucoup de gens aiment haïr parce qu'elle prend leur argent. Je comprends cela. Toutefois, vous faites un travail difficile et vous le faites bien.

Avec toute la surveillance que vous exercez et toutes les mesures dont vous parlez, à quelle fréquence êtes-vous obligés d'imposer une mesure disciplinaire à un employé, et quel type de mesure disciplinaire imposez-vous?

**Mme Helen Brown:** Nous avons une grille à l'ARC qui nous aide à appliquer des mesures disciplinaires cohérentes, car nous sommes un grand organisme qui emploie 40 000 personnes. La grille prévoit les divers types d'inconduite possibles et les mesures disciplinaires à appliquer dans chaque cas.

Pour les incidents d'accès non autorisé, les mesures prévues dans la grille vont de la suspension jusqu'au renvoi. Je peux vous dire qu'au cours de la dernière année, 14 employés ont été renvoyés et 18 autres ont été suspendus pour cette raison.

**L'hon. Laurie Hawn:** Sur 40 000 employés, cela représente un faible pourcentage. Avez-vous des moyens de comparer vos données avec celles d'autres grands organismes gouvernementaux?

**Mme Helen Brown:** Non.

**L'hon. Laurie Hawn:** Votre travail est plutôt unique.

**Mme Susan Gardner-Barclay:** Les chiffres montrent que nous prenons le problème très au sérieux, que nous agissons lorsque des incidents surviennent et que toutes nos directions utilisent une approche assez cohérente pour reconnaître et corriger le problème.

**L'hon. Laurie Hawn:** Vous devez respecter tous les codes de travail, etc., dans quelle mesure est-il difficile — la question est subjective et appelle une réponse subjective, j'imagine — de congédier un employé membre de l'Alliance de la Fonction publique?

**Mme Susan Gardner-Barclay:** Je ne peux pas répondre à cette question. Je crois que les faits parlent d'eux-mêmes et montrent que la chose est arrivée.

**Une voix:** J'invoque le Règlement.

**Le président:** Je vous prie de m'excuser, mais nous avons deux points à traiter. Premièrement, votre temps est écoulé, M. Hawn, mais, deuxièmement, Mme Borg a invoqué le Règlement.

[Français]

**Mme Charmaine Borg:** Monsieur le président, je pense que sa question n'est pas pertinente par rapport à cette étude. Le fait de savoir s'il est difficile ou non de congédier une personne n'a pas d'effet sur le vol d'identité.

• (1130)

[Traduction]

**Le président:** Votre rappel au Règlement est pertinent, mais le problème ne se pose plus parce que M. Hawn doit immédiatement cesser de chercher une réponse à sa question.

J'estime toutefois que votre rappel au Règlement est pertinent.

Nous passons maintenant à M. Regan pour le Parti libéral.

Soyez le bienvenu, monsieur Regan. Vous avez sept minutes.

**L'hon. Geoff Regan (Halifax-Ouest, Lib.):** Merci beaucoup.

[Français]

Tout d'abord, j'aimerais adresser ma question à M. Dufresne.

Vous avez parlé du fait qu'il y a aux États-Unis des cartes d'identification personnelle utilisant des systèmes biométriques. J'ai entendu parler de dispositifs qui pourraient effacer des détails d'une carte quand on passe devant un tel appareil. Selon vous, quelle est la meilleure façon d'éviter cela? Jusqu'à quel point vous intéressez-vous à ce sujet?

**M. Philippe Dufresne:** Avec plusieurs de nos intervenants, on a partagé un outil qui est un guide sur l'impact des mesures de sécurité sur les droits de la personne. Ce guide vise justement à soulever ce genre de questions. On se demande si les personnes handicapées et les membres de certains groupes protégés par la loi ont accès à la mesure qui est mise en place. Il faut faire cette analyse au tout début lorsqu'on met en place la mesure. Il faut ensuite tester cette mesure pour voir si elle est efficace sur le plan de la sécurité et si elle a un impact négatif.

Dans la situation que vous décrivez, il y aurait un impact. On pourrait dire que cette mesure semblait bonne à première vue, mais qu'il y a un impact négatif sur la sécurité, sur la santé ou sur les individus.

Ce processus ne devrait pas cesser même après l'adoption de la mesure. Il faut continuer de l'évaluer et de l'améliorer.

[Traduction]

**L'hon. Geoff Regan:** Alors, il n'y aurait pas de distinction en ce sens, j'imagine, qu'il n'y a pas de... Vous ne pouvez pas penser à pied levé à une façon dont ce genre d'activité, une tentative de vol de renseignements sur une personne avec ce genre de scanner, pourrait constituer de la discrimination contre les personnes dont vous devez vous préoccuper.

**M. Philippe Dufresne:** Chaque situation doit être examinée au regard de ses répercussions sur les droits de la personne.

Lorsqu'un groupe devant être protégé, disons les personnes handicapées, risque de faire l'objet d'un vol d'identité en raison d'une mesure donnée, il faut établir les répercussions possibles. Il faut alors se demander comment réduire le plus possible ou, idéalement, éliminer les répercussions négatives. C'est ce que l'évaluation des impacts des mesures de sécurité sur les droits de la personne permet de faire. Nous examinons la situation des groupes; et nous ne nous penchons pas seulement sur les impacts directs, mais sur les impacts indirects également. Nous nous assurons, et deux fois plutôt qu'une, que la situation ne doit pas avoir de répercussions sur la sécurité, car la sécurité est fondamentale, mais nous veillons à que les droits de la personne soient pris en considération dès la conception même de la mesure et, encore, tout au long de sa mise en oeuvre et au-delà.

**L'hon. Geoff Regan:** À ce que je comprends, on peut placer sa carte de crédit ou d'autres cartes et ce genre d'information dans une chemise sûre. Certains porte-feuilles offrent une bonne protection, alors que ce n'est pas le cas pour d'autres. Beaucoup de gens sauraient cela, mais beaucoup ne le sauraient pas; il serait donc important de transmettre cette information.

Vous avez laissé entendre que les méthodes multimodales sont préférables pour confirmer l'identité de quelqu'un. Pouvez-vous nous donner des exemples de telles méthodes et nommer des institutions ou des compagnies qui les utilisent?

**M. Philippe Dufresne:** J'ai parlé de la carte d'identité personnelle utilisée aux États-Unis. Cette carte contient les empreintes digitales. Si les empreintes ne permettent pas d'identifier quelqu'un, il y a ensuite la reconnaissance faciale.

**L'hon. Geoff Regan:** Y a-t-il de tels dispositifs au Canada dont vous pourriez nous parler?

**M. Philippe Dufresne:** Je vais demander à mon collègue, M. Karpinski, si la recherche a mis au jour quelque chose à ce sujet.

**M. Maciej Karpinski (analyste principal de recherche, Direction générale de la promotion des droits de la personne, Commission canadienne des droits de la personne):** Quelques exemples existent au Canada.

Nous indiquons dans le rapport que nous avons examiné un lot de pièces d'identité secondaires produites par le gouvernement du Canada. Il y a, entre autres, la carte NEXUS qui comporte deux mesures biométriques, soit les empreintes digitales et le balayage de l'iris. De cette façon, si les empreintes digitales d'une personne ne sont pas lisibles ou qu'une personne n'a pas des doigts que la machine peut scanner, les responsables peuvent se tourner vers le balayage de l'iris. Ces mesures en soi ne sont peut-être pas nécessairement inclusives parce que ce n'est pas tout le monde qui a des doigts et des iris balayables. C'est pour que...

Ce que montre le rapport, c'est que lorsqu'on élabore ce genre de systèmes, il faut toujours prendre un certain temps pour réfléchir aux mesures de rechange qui peuvent être utilisées au besoin lorsque des cas spéciaux se présentent.

Il y a d'autres exemples simples. Ainsi, on peut apercevoir dans les épiceries des scanners à main qui permettent aux employés d'enregistrer l'heure de leur arrivée. Là encore, il y a des scanners à une main et d'autres à deux mains; or un système capable de scanner vraisemblablement les deux mains peut être préférable, parce qu'il est arrivé que des gens se sont opposés au scannage d'une main au profit d'une autre. Avec des systèmes semblables, nous

estimons qu'on ne peut pas se fier exclusivement à un système en particulier, mais qu'il vaut mieux en avoir d'autres en complément.

• (1135)

**L'hon. Geoff Regan:** J'essaie de penser à la façon dont je pourrais m'opposer à quelque chose comme gaucher, mais je ne trouve pas d'exemple à brûle-pourpoint.

**M. Maciej Karpinski:** Il existe un exemple dans le rapport auquel on se reporte. Certaines pratiques religieuses sont plus favorables au balayage d'une main au lieu des deux, ou d'une main en particulier.

**L'hon. Geoff Regan:** Merci beaucoup.

Madame Gardner-Barclay, vous nous l'avez probablement déjà dit, mais à quelle période se rapportent les 2 900 atteintes dont vous avez parlé?

**Mme Susan Gardner-Barclay:** À l'année 2013.

**L'hon. Geoff Regan:** Alors, c'était pour une année.

**Mme Susan Gardner-Barclay:** Oui.

**L'hon. Geoff Regan:** Quel processus était en place avant cela pour prévenir les atteintes?

**Mme Susan Gardner-Barclay:** En fait, nous avons plusieurs processus. À la suite de cela, et tout particulièrement après le rapport du Commissariat à la protection de la vie privée de 2013, nous avons renforcé nos processus. Toutefois, nous avons bel et bien des contrôles de première ligne qui visaient à gérer soigneusement l'accès des employés aux systèmes de l'ARC.

Nous avons des contrôles secondaires. Nous sommes en train de mettre en place un système qui renforcera ces contrôles; ce travail s'étendra sur une période de deux ans. Nous avons effectivement la capacité de surveiller l'accès des employés à nos systèmes et de savoir de quelle information ils prennent connaissance.

Au cours de la période allant de 2010 à 2013, nous avons revu nos politiques et nos procédures relatives à la protection de la vie privée. Nous avons également mis en oeuvre un nouveau régime de mesures disciplinaires. Nous avons renforcé la formation et les programmes de sensibilisation destinés à nos employés. Cette tâche a été entreprise en 2010 et elle se poursuit, mais le plus gros du travail a été effectué au cours des trois dernières années.

**L'hon. Geoff Regan:** La grande majorité de ces cas, dites-vous, étaient constitués d'erreurs d'acheminement de courrier.

**Mme Susan Gardner-Barclay:** C'est exact.

**Le président:** Geoff, votre temps est écoulé.

**L'hon. Geoff Regan:** Déjà?

**Le président:** Vous avez, dans les faits, largement dépassé le temps qui vous est accordé. Je vous ai laissé beaucoup de marge parce que vous êtes nouveau. Vous devrez poursuivre cette discussion au cours de la prochaine série de questions.

La dernière personne qui peut poser une question de sept minutes est Mme Pat Davidson.

**Mme Patricia Davidson (Sarnia—Lambton, PCC):** Merci aux témoins d'être avec nous cet avant-midi. L'information que vous nous donnez est des plus intéressantes.

Je veux commencer par une courte question pour l'ARC. Vous avez dit dans vos déclarations préliminaires: « Il est important de noter qu'un grand nombre des atteintes à la sécurité des données relevées par l'ARC ne constituent pas des atteintes à la vie privée, puisque aucun renseignement personnel n'a été divulgué. »

Qu'entendez-vous par « renseignement personnel »?

**Mme Helen Brown:** Je pourrais peut-être répondre à cette question.

Un renseignement personnel est un renseignement qui concerne un individu. Nous avons établi une différence entre les atteintes à la sécurité des renseignements personnels et les atteintes à la sécurité des renseignements pouvant concerner une entreprise, par exemple, une pièce de correspondance comportant le nom et l'adresse de l'entreprise, qui sont de l'information publique. Nous aurions considéré ce cas comme une atteinte à la sécurité des renseignements mais pas nécessairement une atteinte à la vie privée.

Je ne sais pas si mon explication est satisfaisante.

**Mme Susan Gardner-Barclay:** Je pourrais peut-être ajouter quelque chose.

Pour définir une atteinte à la vie privée, nous nous reportons aux lignes directrices du Conseil du Trésor, qui désignent comme une atteinte à la vie privée la collecte, l'usage, la communication, la conservation ou le retrait inappropriés ou non autorisés de renseignements personnels. Nous estimons que tout ce qui n'entre pas dans cette définition constitue une atteinte à la sécurité des renseignements et des données, mais non une atteinte à la vie privée.

**Mme Patricia Davidson:** Considérez-vous que le nom, l'adresse, la date de naissance, le NAS d'une personne constituent des renseignements personnels?

**Mme Susan Gardner-Barclay:** Oui.

**Mme Patricia Davidson:** D'accord. Mais s'il s'agit du nom et de l'adresse d'une compagnie qui sont connus, la situation est différente.

**Mme Susan Gardner-Barclay:** Oui. C'est lorsque le nom et l'adresse sont publics et disponibles dans des bases de données publiques. C'est exact.

**Mme Patricia Davidson:** D'accord.

Dans vos déclarations préliminaires, vous avez également parlé de l'article 241 de la Loi de l'impôt sur le revenu et de l'article 295 de la Loi sur la taxe d'accise qui interdisent la divulgation de renseignements sur les contribuables par un employé sauf si la divulgation a été autorisée expressément en vertu de ces lois.

Qu'est-ce que cela veut dire? Qu'est-ce qui est expressément autorisé au juste?

• (1140)

**Mme Susan Gardner-Barclay:** La loi permet la divulgation de certains renseignements, si l'autorisation en a été donnée. L'exemple le plus clair serait la divulgation effectuée à la suite du consentement donné par le contribuable. Dans certains cas, des contribuables acceptent que des renseignements les concernant soient communiqués à une tierce partie.

Un bon exemple serait les cabinets de fiscalistes qui préparent les déclarations de revenus et qui ont besoin du consentement des contribuables pour avoir accès à l'information les concernant. C'est l'exemple le plus évident.

**Mme Patricia Davidson:** Dans un cabinet de député, pour travailler au nom d'un électeur, nous devons avoir une formule de consentement signée.

**Mme Susan Gardner-Barclay:** C'est exact. Ce serait une autre exemple. Nous avons une formule de consentement. Les contribuables remplissent la formule, les députés également, et ils nous l'envoient. C'est le mécanisme par lequel nous sommes autorisés à communiquer des renseignements confidentiels sur un contribuable à un député qui le représente.

**Mme Patricia Davidson:** D'accord.

Un de mes électeurs m'a fait part de préoccupations au cours de la fin de semaine dernière. Naturellement, nous savons tous qu'il est temps de remplir les déclarations d'impôts et nous nous affairons tous à le faire. Cet électeur a utilisé les services d'un spécialiste pendant plusieurs années, il a eu des problèmes avec cette personne et a décidé de s'adresser à quelqu'un d'autre cette année.

L'électeur s'est présenté au deuxième spécialiste en apportant les rapports précédents. On lui a répondu que cela n'était pas nécessaire parce que le nouveau spécialiste pouvait avoir accès en ligne à toutes ses déclarations de revenus précédentes.

Est-ce exact?

**Mme Susan Gardner-Barclay:** Cela ne relève pas tout à fait de mon aire de compétence, mais le deuxième spécialiste a probablement dû obtenir l'autorisation du contribuable pour avoir accès à quelque renseignement en ligne que ce soit sur lui. Je n'ai jamais entendu dire qu'un spécialiste de déclarations de revenus pouvait simplement trouver cette information en ligne sans avoir obtenu l'autorisation appropriée. Nos contrôles à ce sujet sont très stricts. Nous utilisons les mêmes contrôles que ceux dont se servent la majorité des institutions financières canadiennes pour pouvoir gérer l'accès à ce genre de renseignements disponibles en ligne.

**Mme Patricia Davidson:** Lorsque les déclarations sont envoyées à l'ARC, sont-elles conservées à l'ARC, ou chez les spécialistes, ou aux deux endroits?

**Mme Helen Brown:** Là encore, c'est un peu en dehors de notre champ de compétence, mais l'ARC doit à l'évidence conserver l'information qui la concerne et qui concerne nos impôts. J'imagine que le spécialiste devrait également garder cette information dans ses dossiers.

Je ne suis par certaine si cela répond à votre question.

**Mme Patricia Davidson:** Oui. Je suis un petit peu préoccupée par la façon dont le contribuable alors... il y a peut-être quelque chose sur le formulaire original du spécialiste indiquant que le consentement est donné pour la divulgation de l'information. Je ne sais pas, c'est peut-être ce que cette personne devrait vérifier.

**Mme Susan Gardner-Barclay:** C'est avec plaisir que nous vous fournirions plus d'information pour vous donner une bonne idée du cadre qui serait utilisé pour gérer cette situation.

**Mme Patricia Davidson:** J'aimerais avoir cette information. Ce serait bien si vous pouviez la communiquer au greffier. Merci beaucoup.

Vous avez parlé de communication de l'information, de contacts avec les collectivités et les groupes vulnérables, etc., et vous avez parlé des divers organismes qui sont des interlocuteurs pour vous. J'ai simplement une proposition; vous le faites peut-être déjà pour beaucoup de choses, mais vous ne le faites peut-être pas pour certaines autres. Les députés sont d'excellents interlocuteurs. Nous avons tous des sites Web et la plupart d'entre nous sommes présents sur les réseaux sociaux, que ce soit Facebook ou Twitter, et comptons de nombreux abonnés qui suivent ce que nous faisons. C'est une bonne façon de communiquer de l'information. Je sais que nous avons reçu de l'information sur les tactiques d'hameçonnage que nous avons communiquée, et cela a été très bien accueilli dans la population. Les gens veulent être mis au courant de ce genre de choses. Nous sommes donc bien placés pour vous aider.

**Mme Susan Gardner-Barclay:** J'aimerais ajouter quelque chose. Nous l'avons toujours su, mais nous avons agi à ce sujet au cours de la saison des déclarations de revenus de l'an dernier lorsqu'en fait, nous avons fourni pour les députés une trousse d'information complète sur la déclaration de revenus destinée à leurs électeurs. Nous avons pris cette initiative l'an dernier et la réaction a été excellente. Les pages en question ont été consultées des milliers et des milliers de fois. Nous avons reconduit la chose cette année et la réponse est encore meilleure. La trousse a été envoyée aux cabinets de tous les députés.

Toute proposition d'amélioration est la bienvenue. Nous veillerons à ce que l'information sur les tactiques d'hameçonnage soit incluse dans la trousse si elle ne l'a pas été l'an dernier. Je revois la table des matières dans ma tête et je ne suis pas sûre que cette information y figurait. Je sais qu'elle a été fournie séparément, mais nous veillerons à ce qu'elle soit incluse dans la trousse l'an prochain.

• (1145)

**Le président:** Merci, madame Davidson. Votre temps est écoulé.

Nous commençons maintenant la série de questions de cinq minutes. La parole est à M. Mathieu Ravignat.

**M. Mathieu Ravignat (Pontiac, NPD):** Ma question s'adresse à l'Agence de revenu du Canada. Je vous remercie d'être là, mesdames.

Corrigez-moi si je me trompe, mais je crois comprendre que seulement 1 p. 100 des 2 983 incidents ont été réellement signalés à la commissaire à la protection de la vie privée. Cela représente environ 1 700 Canadiens, je crois. Faut-il en déduire que ces gens n'ont aucune idée de ce qu'il est advenu des données les concernant et qu'ils ne savent pas si ces données ont pu être dérobées à des fins de vol d'identité?

**Mme Helen Brown:** J'aimerais apporter une précision et ma collègue, j'en suis sûre, pourra continuer de répondre à votre question. Sur les 2 983 atteintes signalées, seulement 46 p. 100 étaient dans les faits des atteintes à la vie privée. Le reste se composait d'atteintes à la sécurité des renseignements. Alors, pour ce qui est des chiffres, je veux juste m'assurer que c'est ce...

**M. Mathieu Ravignat:** Est-ce que ces cas qui représentent 46 p. 100 de l'ensemble des atteintes ont tous été signalés à la commissaire à la protection de la vie privée?

**Mme Susan Gardner-Barclay:** Non. Un protocole du Conseil du Trésor est en vigueur qui donne des directives aux ministères sur les cas devant être signalés à la commissaire à la protection de la vie privée. Ce code permet de faire une évaluation du risque assez détaillée. Les ministères doivent évaluer le caractère délicat de l'information divulguée. Est-ce, par exemple, une information de nature financière ou médicale? Les ministères doivent effectuer une évaluation du risque de vol d'identité ou de fraude découlant de la perte de cette information. Ils doivent évaluer le potentiel de préjudice pour la personne, par exemple, sa réputation, sa carrière...

**M. Mathieu Ravignat:** Un pour cent semble assez faible. Pouvez-vous m'en dire un peu plus sur les lignes directrices que vous suivez lorsque vous ne signalez pas ces cas à la commissaire à la protection de la vie privée? Pourquoi y a-t-il eu autant de cas que vous avez décidé de ne pas signaler à la commissaire à la protection de la vie privée en appliquant ces critères? Y avait-il une raison principale ou...?

**Mme Susan Gardner-Barclay:** Nous agissons en fonction de l'évaluation que nous faisons du risque. Si l'évaluation montre qu'il y a un risque plausible de préjudice pour la personne, nous signalons

l'incident à la commissaire. Au cours de la période visée par le rapport, nous avons signalé 479 cas.

**M. Mathieu Ravignat:** La décision se prend-elle complètement au niveau interne? L'évaluation du risque est-elle faite complètement au niveau interne, ou faites-vous intervenir un pair de l'extérieur dans le processus d'examen qui peut vous dire : « Oui, vous avez raison, ces cas ne doivent pas être signalés à la commissaire à la protection de la vie privée »?

**Mme Susan Gardner-Barclay:** Le processus est interne, mais il est réalisé à deux endroits dans l'organisme. La Division de la sécurité et des affaires internes de Mme Brown fait l'évaluation initiale, laquelle est ensuite revue par une boîte distincte, dans une direction distincte de notre organisation d'AIPRP, qui doit veiller à ce que nos évaluations soient de la plus haute qualité et qui entretient des rapports étroits avec la commissaire à la protection de la vie privée.

**M. Mathieu Ravignat:** Y a-t-il une validation par le Conseil du Trésor?

**Mme Helen Brown:** Non, je crois comprendre que le Conseil du Trésor vient tout juste de mettre en place un cadre pour que nous lui fassions rapport sur ces cas; mais avant cela, nous traitons de ces questions avec le Commissariat à la protection de la vie privée.

**Mme Susan Gardner-Barclay:** Le Conseil du Trésor a demandé à ce que, l'an prochain au plus tard, toutes les atteintes à la vie privée lui soient communiquées, ainsi qu'au Commissariat à la protection de la vie privée; le système se met donc en place actuellement.

**M. Mathieu Ravignat:** Une fois informée des atteintes et du pourcentage qu'elles représentent, la commissaire à la protection de la vie privée vous a-t-elle demandé de l'information supplémentaire?

• (1150)

**Mme Helen Brown:** Vous avez demandé si le processus est interne, je peux vous dire que nous avons bel et bien revu notre outil d'évaluation du risque avec le Commissariat à la protection de la vie privée pour nous assurer qu'il respecte l'esprit des lignes directrices du Conseil du Trésor.

Je veux également préciser que nous évaluons deux choses : s'il faut informer le contribuable et s'il faut informer la commissaire. La réponse à votre question comporte deux volets.

**M. Mathieu Ravignat:** Dans une question inscrite au Feuilleton, mon collègue Charlie Angus vous a demandé de lui fournir les statistiques sur le nombre d'atteintes à la vie privée survenues entre 2006 et 2012, mais il n'a obtenu aucune réponse. Je me demande pourquoi. Est-ce parce que vous ne recueillez pas ces données ou parce que ces données ne sont pas disponibles?

**Mme Susan Gardner-Barclay:** C'est exact, mais je suis certaine que Mme Brown voudra apporter des précisions à ma réponse.

À cette époque-là, l'ARC surveillait, c'est certain, les atteintes à la vie privée, mais elle le faisait en exerçant un suivi du nombre d'enquêtes au niveau central. Lorsque la question a été posée, nous n'avions pas encore commencé à consigner au niveau central le nombre d'atteintes en cause dans chaque enquête ni le nombre de personnes touchées.

Or, c'est précisément ce que M. Angus a demandé à connaître. Pour répondre à sa question, nous aurions dû parcourir les rapports de plusieurs années et extraire manuellement l'information recherchée.

À la lumière des conseils de M. Angus, nous avons changé notre procédé de façon à pouvoir exercer un suivi au niveau central à la fois des personnes touchées et du nombre d'atteintes en cause dans chaque enquête.

**Le président:** Merci.

J'ai bien peur que cela mette fin au temps qui vous est attribué, monsieur Ravignat.

Maintenant, je cède la parole à Mme Tilly O'Neil Gordon, pour les conservateurs.

**Mme Tilly O'Neill Gordon (Miramichi, PCC):** Je veux remercier les témoins de comparaître devant nous aujourd'hui. Vous nous apportez de l'information sur des sujets qui demandent réflexion. Je veux également vous remercier des mesures que vous mettez en place pour protéger les renseignements personnels sur les Canadiens et réduire ainsi les risques de vol d'identité. Naturellement, cette question est très importante pour nous et elle nécessite toute notre attention.

Parallèlement, j'allais dire, à l'intention de l'ARC, que nous avons tous un rôle à jouer pour prévenir le vol d'identité. Selon vous, quel rôle les consommateurs, les entreprises, les banques, le gouvernement fédéral et la commissaire à la protection de la vie privée doivent-ils jouer pour prévenir et combattre le vol d'identité? Pouvez-vous nous faire part de certaines idées à ce sujet?

**Mme Susan Gardner-Barclay:** Eh bien, vous avez raison, l'ARC considère évidemment que la protection de la vie privée...

**Mme Tilly O'Neill Gordon:** Vous y travaillez beaucoup, nous devrions donc faire quelque chose nous-mêmes.

**Mme Susan Gardner-Barclay:** Évidemment, nous considérons que la protection de la vie privée est une responsabilité partagée.

Nous demandons toujours aux contribuables canadiens de vérifier qu'ils s'adressent bel et bien à nous. En cas de doute, nous leur demandons de profiter de nos numéros 1-800 pour s'assurer qu'ils envoient l'information à la bonne personne et de la bonne façon. Nous collaborons étroitement avec le Bureau de la concurrence; nous participons également aux activités du mois de la littératie financière. Nous croyons fermement qu'il est important et utile pour les Canadiens de bien comprendre leurs activités financières et de savoir quel genre d'information doit faire l'objet de mesures de protection.

À certains égards, c'est en bonne partie une question de bon sens, assurément. Notre site Web comporte beaucoup d'informations qui aident les gens à comprendre le fonctionnement du système fiscal, à quelles étapes ils doivent intervenir, les précautions à prendre pour ne nous communiquer que l'information requise et pour la protéger.

**Mme Tilly O'Neill Gordon:** Avez-vous quelque chose à ajouter?

**Mme Helen Brown:** Je pensais tout juste à toutes les mesures que nous prenons à l'ARC et une chose est ressortie à laquelle ma collègue a fait allusion dans ses déclarations préliminaires : les activités de communication que nous réalisons pour informer les gens sur les risques qui menacent leur vie privée. Nous publions dans notre site Web des conseils pour aider les gens à se protéger contre le vol d'identité.

**Mme Tilly O'Neill Gordon:** Plus nous entendons des témoins nous parler du vol d'identité, plus je dirais, et tous les électeurs de ma circonscription en feraient autant, qu'il est très important — et il faut en prendre conscience — que les contribuables gardent les renseignements sur eux très confidentiels et prennent des mesures

pour prévenir le vol d'identité, car ce problème peut, j'imagine, devenir endémique, avec toute la nouvelle technologie.

Ma question s'adresse à la Commission canadienne des droits de la personne. En janvier 2010, le projet de loi S-4, Loi modifiant le Code criminel (vol d'identité et infractions connexes) a été adopté et a permis d'ajouter de nouvelles infractions au Code criminel applicables aux divers aspects du vol d'identité.

Quelle incidence l'entrée en vigueur de ces nouvelles dispositions a-t-elle eue sur les organismes du gouvernement responsables de l'application de la loi? Ces dispositions ont-elles eu une incidence sur eux?

• (1155)

**M. Philippe Dufresne:** Je ne suis pas certain que nous sommes les mieux placés pour répondre à cette question. Ces nouvelles infractions ne sont pas du ressort de la Commission canadienne des droits de la personne, selon nous. Elles ne peuvent pas être le sujet de plaintes déposées auprès de nous; je ne suis donc pas certain de l'incidence qu'elles ont eue sur d'autres organismes.

**Mme Tilly O'Neill Gordon:** D'accord.

L'un de vous aurait-il des recommandations à nous faire concernant des aspects particuliers que notre comité devrait examiner de près dans son étude de la question?

**M. Philippe Dufresne:** À la Commission canadienne des droits de la personne, nous estimons qu'il faut toujours examiner les mesures proposées sous l'angle des droits de la personne, et cela comprend les mesures pour prévenir et corriger le vol d'identité. Nous croyons qu'il n'y a aucun antagonisme entre le respect des droits de la personne et les objectifs des politiques, quelles qu'elles soient, et que la prise en compte des droits de la personne dans les politiques ne fait réellement que les renforcer. Voilà la grande recommandation que nous formulerions à ce sujet.

**Le président:** Cela met fin au temps qui vous est accordé. Merci beaucoup.

Nous allons procéder à une autre série de questions. Le NPD prendra la parole en premier, suivront le Parti conservateur et le Parti libéral, ce qui conclura cette partie de notre étude. Chers collègues, nous tiendrons ensuite le reste de notre réunion à huis clos pour planifier nos activités futures.

C'est Mme Borg qui prendra la parole pour le NPD.

Vous avez cinq minutes; allez-y, madame, je vous en prie.

[Français]

**Mme Charmaine Borg:** Merci beaucoup, monsieur le président

Je vais poser ma première question à M. Dufresne.

Selon vous, le processus de traitement des plaintes liées à des vols d'identité est-il équitable et efficace? Peut-il mener à de la discrimination? Le système est-il adéquat?

**M. Philippe Dufresne:** Nous n'avons pas précisément abordé cette question. J'hésiterais donc à la commenter d'une façon ou d'une autre.

Toutefois, nous disons que pour n'importe quel processus ou n'importe quelle méthodologie, il est utile de se poser cette question. Il est important de se demander si le processus, qui peut avoir été créé avec de très bonnes intentions, a un impact négatif sur les personnes âgées, sur les femmes ou sur les personnes handicapées. Par la suite, il ne s'agit pas de simplement arrêter automatiquement ces mesures, mais de se demander si elles sont nécessaires et si on peut en réduire l'impact discriminatoire.

C'est ce qu'on a tenté de faire avec notre outil qui mesure cet impact. On ne veut pas seulement le dire de façon théorique et être un obstacle. On veut essayer d'aider les organisations. On sait qu'il n'est pas facile d'atteindre ces objectifs, mais il faut les atteindre.

**Mme Charmaine Borg:** Merci beaucoup.

Ma deuxième question s'adresse aux représentants de l'Agence du revenu du Canada.

De plus en plus de Canadiens font maintenant leur déclaration de revenus en ligne. Évidemment, on est rendus à l'ère numérique. Y a-t-il des risques plus élevés à utiliser les nouveaux logiciels qui sont disponibles pour faire sa déclaration de revenus? Si oui, comment peut-on informer les Canadiens sur ces risques et sur la façon de s'en prémunir?

[Traduction]

**Mme Susan Gardner-Barclay:** Là encore, la question déborde un peu de notre champ de compétence. Je peux vous dire toutefois que nous appliquons un processus de recertification très imposant pour tous les logiciels disponibles dans notre site, les logiciels commerciaux, servant à remplir les déclarations de revenus et de prestations. Ces logiciels ne peuvent pas être certifiés par l'ARC tant qu'ils n'ont pas satisfait à nos normes de sécurité les plus élevées.

Je peux également vous dire que nos propres systèmes et portails utilisés par les entreprises, les particuliers et les représentants pour traiter avec nous d'une gamme de questions et pour avoir accès à plusieurs services, dont la production des déclarations, satisfont aux mêmes exigences de sécurité que celles appliquées par les institutions financières canadiennes pour les services en ligne. Ces systèmes font l'objet d'une surveillance constante, à plus forte raison pendant la saison de la production des déclarations de revenus, parce que nous sommes tout à fait conscients que la sécurité, la sécurité de ces portails, est essentielle pour que les Canadiens se sentent à l'aise de nous communiquer de l'information sur eux. L'ARC s'est donc dotée d'un système de sécurité très rigoureux pour l'ensemble de son organisation.

Il s'agit essentiellement d'un système à paliers. Le premier palier se compose de Services partagés Canada. Cet organisme applique un certain nombre de mécanismes de sécurité qui constituent la couche extérieure de protection. Le palier suivant, c'est le coupe-feu de l'ARC, qui est extrêmement fort. Dans les cas très rares où un logiciel malveillant peut réussir à franchir ce coupe-feu, nous en avons un deuxième qui bloque les logiciels malveillants ou les attaques malicieuses. Nous avons l'un des régimes de sécurité les plus forts, sinon le plus fort, du gouvernement pour protéger nos systèmes technologiques, précisément pour les raisons dont je vous ai parlé.

• (1200)

[Français]

**Mme Charmaine Borg:** C'est parfait. Ce sont de bonnes nouvelles.

Ma dernière question pourra paraître un peu bizarre.

Pouvez-vous énumérer toutes les données personnelles que vous détenez sur un Canadien typique qui fait chaque année ses déclarations de revenus?

[Traduction]

**Mme Susan Gardner-Barclay:** Eh bien, c'est... oui, nous pouvons...

**Des voix:** Oh, oh!

**Mme Susan Gardner-Barclay:** À l'évidence, toute l'information contenue dans la déclaration de revenus et de prestations d'une personne... ce serait donc le NAS, le revenu et les crédits dont elle veut se prévaloir. Pour profiter d'un crédit, il faut fournir des renseignements supplémentaires; ce peut être des renseignements d'ordre médical, s'il s'agit d'un crédit d'impôt pour personne handicapée, par exemple.

Le même procédé général s'applique pour les entreprises. Naturellement, les entreprises doivent déclarer leurs revenus. Elles doivent fournir de l'information sur la TPS et la TVH qu'elles ont perçues au nom du gouvernement. Si elles demandent à se prévaloir de crédits d'impôt, par exemple, le crédit pour la recherche scientifique et le développement expérimental, elles doivent fournir des renseignements sur le travail qu'elles font pour se qualifier.

C'est très difficile de résumer la question, mais, oui, nous recueillons beaucoup de renseignements. Je ne vous en ai donné qu'un aperçu.

[Français]

**Mme Charmaine Borg:** C'est probablement davantage que tous les autres ministères.

**Mme Susan Gardner-Barclay:** C'est possible.

[Traduction]

Il faut également mentionner que nous recueillons de l'information pour certaines provinces et les territoires à des fins de rationalisation; nous recueillons donc des renseignements de nature provinciale en leur nom.

**Le président:** Très bien.

Merci, madame Borg.

M. Zimmer, pour le Parti conservateur.

**M. Bob Zimmer (Prince George—Peace River, PCC):** Merci de comparaître devant nous aujourd'hui.

Comme nous parlons des répercussions économiques, et corrigez-moi si je n'ai pas entendu le nombre, quel est l'impact économique moyen pour un Canadien victime d'un vol d'identité et pour les Canadiens dans leur ensemble? La Commission canadienne des droits de la personne aurait une meilleure idée de cela. Je suis sûr que cet impact va d'une petite somme à une grande, mais quel est l'impact moyen au niveau financier?

**M. Philippe Dufresne:** Malheureusement, nous ne recueillons pas ce genre d'information, l'impact sur la vie privée... Nous examinerions les répercussions de la discrimination sur les droits de la personne de Canadiens, etc. Je ne peux vous fournir cette information.

**M. Bob Zimmer:** Essentiellement, la valeur en dollars ne pourrait pas être quantifiée, selon votre...

**M. Philippe Dufresne:** Elle peut l'être, mais ce n'est pas quelque chose que la Commission canadienne des droits de la personne s'appliquerait à faire.

**M. Bob Zimmer:** L'ARC pourrait-elle répondre à la même question? Cela serait simplement...

**Mme Susan Gardner-Barclay:** Malheureusement, l'information existe peut-être quelque part, mais l'ARC ne fait pas ce calcul.

**M. Bob Zimmer:** D'accord.

C'est la saison des déclarations de revenus et beaucoup de gens utilisent des programmes offerts sur le Web pour remplir leurs déclarations. J'imagine qu'il existe de bons programmes et de mauvais programmes. J'ai fait quelques recherches sur le Web. Y voyez-vous un terrain fertile pour le vol d'identité, le ciblage de programmes gratuits ou ce genre de choses? Avez-vous eu connaissance de ce genre de choses au Canada? Cela s'est produit dans d'autres pays, mais est-ce arrivé au Canada?

**Mme Susan Gardner-Barclay:** Cela est également en dehors de notre champ de compétence, mais nous n'avons jamais eu connaissance de ce genre d'incident.

Dans une réponse à une question précédente, j'ai dit que tous les logiciels commerciaux disponibles sur le site Web de l'ARC ont fait l'objet d'une authentification et d'une certification extrêmement rigoureuses. Nous sommes persuadés que les logiciels qui figurent sur notre site fonctionnent bien avec les systèmes de l'ARC et qu'ils sont d'une utilisation sûre.

• (1205)

**M. Bob Zimmer:** Il est donc primordial que les Canadiens prennent connaissance de votre liste en ligne et utilisent les services qui y figurent. Bien.

La question s'adresse aux deux groupes. Quel est le meilleur moyen, et ne parlons pas de ce qui est évident, que peuvent prendre les Canadiens pour lutter contre le vol d'identité? La question est très large, mais existe-t-il des programmes particuliers que vous recommanderiez? Je sais que cela déborde aussi un peu de votre aire de compétence, mais auriez-vous des recommandations à formuler pour le Canadien moyen qui lirait ce dont nous discutons ici? Selon vous, quel est le meilleur moyen pour les Canadiens de prévenir le vol d'identité?

Commençons par Philippe, s'il vous plaît.

**M. Philippe Dufresne:** Ce que nous aurions à dire réellement concernerait surtout les organismes qui recueillent de l'information, qu'ils soient publics, privés ou encore gouvernementaux; il s'agirait pour eux de voir à ce que les méthodes utilisées n'aient pas de répercussions négatives sur des gens pour un motif illicite, ce pourrait être des répercussions sur des personnes âgées ou handicapées, notamment. Si de telles répercussions sont possibles, il faut les repérer dès le début, lorsque la mesure envisagée est en élaboration; il faut évaluer la mesure, recueillir l'information pour vérifier réellement s'il y a des répercussions et déterminer ce qui peut être fait pour les réduire le plus possible.

**M. Bob Zimmer:** D'accord.

Oui, Helen.

**Mme Helen Brown:** L'Agence du revenu du Canada a un site Web sur la façon de se protéger contre le vol d'identité, que vous trouverez peut-être intéressant. On y fait valoir notamment qu'il ne faut jamais fournir des renseignements personnels par Internet ou par courriel. L'ARC ne demande jamais de lui fournir ce genre d'information par courriel. De toute façon, il y a une liste, on y incite les gens à garder leurs codes d'accès, leurs noms d'utilisateur et leur NIP secrets, à tenir leur adresse à jour... Il y a beaucoup de choses dans le site sur la façon de réduire le plus possible les risques en protégeant son NAS, en signalant sans tarder la perte ou le vol de ses cartes de crédit, etc. Vous y trouverez des renseignements que vous jugerez peut-être utiles.

**M. Bob Zimmer:** Certainement.

J'ai une dernière question. Je crois que ma collègue d'en face a posé la question sur les atteintes qui sont survenues. Vous avez dit

qu'il s'est agi d'erreurs d'adressage et d'acheminement de courrier. J'aimerais simplement souligner une chose en particulier que vous avez mentionnée. Vous avez dit qu'il n'y avait pas de renseignements personnels dans ces lettres... dans certaines d'elles. Quel pourcentage de ce groupe devrait inquiéter les Canadiens, selon vous? Sur 100 atteintes, combien n'auraient pas mis en cause des renseignements personnels?

**Mme Helen Brown:** Si je comprends bien votre question, une partie de la réponse tient à ce que sur ces 3 000 erreurs ou presque d'acheminement de courrier, 46 p. 100 étaient considérées comme des atteintes à la vie privée. Pour ce qui est du nombre, je ne suis pas sûre si...

**M. Bob Zimmer:** Non, ce n'est pas exactement ce que j'ai demandé. Alors, sur 3 000 erreurs ou presque, environ la moitié seraient considérées comme sérieuses, alors littéralement... Et pour ces gens, c'est 1 600 de trop, n'est-ce pas? Voilà ce que nous dirions. Je suis sûr que vous en convenez. Toutefois, c'est un nombre assez petit.

**Mme Susan Gardner-Barclay:** N'oubliez pas que beaucoup de ces pièces de correspondance ont fini, en fait, par être récupérées par l'agence.

**M. Bob Zimmer:** C'est parfait. Merci.

C'est tout ce que j'avais à dire.

**Le président:** Merci, monsieur Zimmer, votre temps est écoulé.

Monsieur Regan.

**L'hon. Geoff Regan:** Monsieur le président, je vais reprendre la question que j'avais commencé à poser avant d'être interrompu à juste titre et, je dois dire, de façon courtoise; cela semble contradictoire, n'est-ce pas? C'était la chose à faire parce que mon temps était de toute évidence écoulé.

Revenons donc à la question des atteintes. Lorsque je vous ai demandé quels processus vous utilisiez avant l'an dernier pour éviter les atteintes, vous avez parlé essentiellement des atteintes qui ne découlaient pas d'erreurs d'acheminement de courrier. Permettez-moi de me reporter aux 2 800 erreurs d'acheminement de courrier. La grande question, je crois, serait de vous demander ce que vous avez changé depuis le 1er janvier de l'an dernier. Cela me permettrait de savoir à la fois comment les choses étaient alors et comment elle sont maintenant.

**Mme Helen Brown:** Je peux répondre à votre question de deux ou trois façons.

Au cours des deux ou trois dernières années, nous avons commencé à gérer au niveau central le signalement des erreurs d'acheminement de courrier pour pouvoir mieux les gérer. Lorsque nous prenons connaissance d'une erreur, nous pouvons restreindre les dommages en cessant d'envoyer du courrier à cette adresse. Nous récupérons la pièce de correspondance dans 95 p. 100 des cas, comme je l'ai dit. Nous essayons de trouver le problème à l'origine de l'erreur pour pouvoir corriger la situation et réduire le risque qu'une nouvelle erreur se produise.

**L'hon. Geoff Regan:** Vous dites que vous récupérez 95 p. 100 des pièces acheminées à la mauvaise adresse, mais j'imagine que la seule façon pour vous de savoir qu'une erreur est survenue, c'est lorsque quelqu'un vous en informe. Est-il juste de dire que vous ne pouvez pas vraiment affirmer avec certitude que vous récupérez 95 p. 100 des pièces de correspondance mal acheminées?

•(1210)

**Mme Helen Brown:** Vous avez raison. Nous ne pouvons pas l'affirmer avec certitude.

**L'hon. Geoff Regan:** J'aimerais comprendre comment cela peut arriver, est-ce une erreur humaine? Y a-t-il quelqu'un qui met la lettre dans une enveloppe? Avez-vous examiné la possibilité d'effectuer cette tâche de façon électronique? Avez-vous constaté qu'une façon de procéder est plus propice aux erreurs que l'autre?

**Mme Helen Brown:** L'un des avantages qu'il y a à gérer les cas au niveau central tient à ce que nous pouvons réellement retracer les causes du problème.

Par exemple, dans environ 10 à 15 p. 100 des cas, la raison tient à ce que nous n'avions pas la bonne adresse du contribuable. Le contribuable avait peut-être déménagé et ne nous en avait pas informé. Un certain pourcentage de cas sont attribuables à des erreurs de Postes Canada, qui livre le document au mauvais endroit. Les erreurs d'entrée de données comptent également pour un certain pourcentage: un employé reçoit une déclaration de revenus établie à la main et lorsqu'il entre l'information dans le système, il peut inverser les chiffres, ou quelque chose comme cela. Nous avons retracé également un certain nombre d'erreurs électroniques ou techniques, et certaines enveloppes contiennent parfois plus d'une déclaration.

Nous retraçons les problèmes et nous tentons de les corriger pour réduire les erreurs d'acheminement de courrier.

**L'hon. Geoff Regan:** Pour ce qui est des erreurs commises par quelqu'un qui place le mauvais document dans la mauvaise enveloppe, permettez-moi de revenir à ma question concernant le recours à une machine plutôt qu'à un humain. La chose est-elle possible? Avez-vous un moyen d'évaluer si cette façon de procéder serait plus sûre et donnerait lieu à moins de problèmes?

**Mme Susan Gardner-Barclay:** Dans les faits, toutes nos opérations depuis l'impression des documents jusqu'à l'envoi sont essentiellement automatisées maintenant.

Lorsqu'un document se retrouve dans la mauvaise enveloppe, c'est habituellement une erreur de la machine. Cela survient généralement lorsque la machine attrape deux pages au lieu d'une ou lorsqu'un changement quelconque est survenu, à l'intérieur de la machine, dans le processus d'acheminement des documents devant aller dans l'enveloppe.

Il est très rare, et je ne suis pas certaine de pouvoir citer un seul cas, que nous placions les documents dans les enveloppes manuellement. Nous avons tout simplement trop de documents à traiter.

**L'hon. Geoff Regan:** Je vous encourage évidemment à continuer de travailler à cela parce que les gens sont très mécontents lorsque

des erreurs de ce genre surviennent et je vous suis reconnaissant d'être venus nous en parler aujourd'hui.

Merci.

**Le président:** Merci beaucoup, monsieur Regan.

Si vous n'avez pas d'autres questions, nous en resterons là, mais j'aimerais me prévaloir de ma prérogative de président pour poser une question, ou demander une précision au moins, sur une chose que je crois avoir entendue dans un témoignage.

La commissaire à la protection de la vie privée dit souvent que les gens ont le droit de savoir si les renseignements sur eux détenus par d'autres personnes ont été compromis. L'ARC a-t-elle pour politique d'informer, par mesure de précaution, un citoyen qui peut avoir été victime d'une atteinte à la vie privée?

**Mme Susan Gardner-Barclay:** Dans ces cas-là, nous suivons la politique du Conseil du Trésor du Canada.

Nous avons parlé plus tôt de l'évaluation du risque effectuée pour déterminer la gravité de l'atteinte et son impact sur une personne; cela comprend le potentiel de vol d'identité. Cette évaluation comporte trois volets : le genre de préjudice possible en regard des renseignements personnels perdus, y compris l'impact sur la réputation, la carrière, la santé ou la sécurité de la personne concernée. Notre évaluation est très détaillée. Elle est conforme aux politiques du Conseil du Trésor du Canada. Lorsqu'il ressort d'une évaluation qu'il vaut mieux informer la commissaire à la protection de la vie privée de la situation, nous le faisons et nous en informons également la personne visée.

**Le président:** Alors, seulement pour bien comprendre, dans le cas qui est arrivé à Mme Borg, lorsqu'elle a ouvert une enveloppe contenant des renseignements sur quelqu'un d'autre, auriez-vous informé cette personne que des renseignements sur elle avaient été envoyés à quelqu'un d'autre?

**Mme Susan Gardner-Barclay:** Je ne peux pas parler de cas particuliers, mais la décision de prendre contact avec cette personne dépendrait de l'évaluation du risque effectuée à la lumière des critères applicables.

**Le président:** D'accord, très bien. Je vous remercie beaucoup alors.

Merci à nos témoins de la Commission canadienne des droits de la personne et de l'Agence du revenu du Canada.

Nous allons suspendre notre réunion un court instant avant de tenir une séance de planification à huis clos; tous ceux qui ne sont pas autorisés à demeurer dans la salle peuvent partir à ce moment-ci.

Je vous remercie beaucoup de vos témoignages.

[ *La séance se poursuit à huis clos.* ]





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

---

### PERMISSION DU PRÉSIDENT

---

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

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

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

---

Aussi disponible sur le site Web du Parlement du Canada à l'adresse suivante : <http://www.parl.gc.ca>

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

---

### SPEAKER'S PERMISSION

---

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

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

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

---

Also available on the Parliament of Canada Web Site at the following address: <http://www.parl.gc.ca>