CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

LE PROBLÈME GRANDISSANT DU VOL D'IDENTITÉ ET SES RÉPERCUSSIONS ÉCONOMIQUES ET SOCIALES

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

Le président

Pierre-Luc Dusseault

MAI 2015

41e LÉGISLATURE, DEUXIÈME SESSION

LE PROBLÈME GRANDISSANT DU VOL D'IDENTITÉ ET SES RÉPERCUSSIONS ÉCONOMIQUES ET SOCIALES

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

Le président

Pierre-Luc Dusseault

MAI 2015

41e LÉGISLATURE, DEUXIÈME SESSION

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

PRÉSIDENT

Pierre-Luc Dusseault

VICE-PRÉSIDENTS

Patricia Davidson
Scott Simms

MEMBRES

Charlie Angus
Charmaine Borg
Ray Boughen
Paul Calandra
Larry Maguire
Tilly O'Neill Gordon
Bob Zimmer

AUTRES DÉPUTÉS AYANT PARTICIPÉ

Scott Andrews
John Carmichael
Jacques Gourde
Laurie Hawn
Pat Martin
Mathieu Ravignat

GREFFIERS DU COMITÉ

Joann Garbig
Chad Mariage

BIBLIOTHÈQUE DU PARLEMENT
Service d'information et de recherche parlementaires

Maxime-Olivier Thibodeau
Miguel Bernal-Castillero
Dara Lithwick

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

SEPTIÈME RAPPORT

Conformément au mandat que lui confère l’article 108(3)*h*) du Règlement, le Comité a étudié le problème grandissant du vol d'identité et ses répercussions économiques et a convenu de faire rapport de ce qui suit :

TABLE DES MATIÈRES

LE PROBLÈME GRANDISSANT DU VOL D'IDENTITÉ ET SES RÉPERCUSSIONS ÉCONOMIQUES ET SOCIALES

INTRODUCTION

Le 7 novembre 2013, 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 la motion suivante visant à examiner la question du vol d'identité :

> Que le Comité étudie le problème grandissant que constitue le vol d'identité et ses répercussions économiques sur les citoyens et les entreprises, ainsi que les mesures prises par les entreprises et les organismes chargés de l'application de la loi afin de contrer ce phénomène au Canada, et qu'il fasse rapport de ses conclusions au Parlement[1].

Il y a vol d'identité lorsque quelqu'un obtient ou recueille des renseignements personnels concernant une autre personne à des fins criminelles et principalement dans le but d'en faire un usage frauduleux. La « fraude d'identité » est l'utilisation délibérée de l'identité d'une autre personne, par exemple pour employer sa carte de crédit, avoir accès à ses comptes bancaires et à ses soldes de transfert de fonds, faire des achats ou obtenir un prêt, des services gouvernementaux ou d'autres avantages en son nom.

Le Comité a entrepris cette étude le 1er avril 2014 et l'a conclue le 23 février 2015. Au cours des 10 réunions consacrées à cette étude, le Comité a entendu 39 témoins issus de ministères et d'agences gouvernementales, des forces de l'ordre, de groupes d'intérêt, d'universités, de bureaux d'avocats, d'agences d'évaluation du crédit, de banques et d'entreprises des technologies de l'information.

1 Chambre des communes, Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, *Procès-verbal*, 2e session, 41e législature, 7 novembre 2013. La même motion avait été adoptée au cours de la 1re session de la 41e législature bien que le Comité n'ait pas examiné la question avant la fin de la session.

DÉFINIR LE VOL D'IDENTITÉ ET SES RÉPERCUSSIONS ÉCONOMIQUES

A. Législation canadienne concernant le vol d'identité

Le projet de loi S-4 : Loi modifiant le Code criminel (vol d'identité et inconduites connexes)

C'est en janvier 2010 que le projet de loi S-4 : Loi modifiant le Code criminel (vol d'identité et inconduites connexes) est entré en vigueur[2]. Plusieurs nouvelles infractions sont désormais prévues au *Code criminel* pour viser précisément les aspects du vol d'identité qui n'étaient pas pris en compte dans les dispositions existantes. Les trois principales infractions créées par le projet de loi S-4 sont les suivantes : l'obtention et la possession de renseignements personnels dans le but de commettre un crime (nouveau paragraphe 402.2(1) du *Code criminel*); le trafic de renseignements personnels en sachant qu'ils serviront à commettre un crime (nouveau paragraphe 402.2(2) du *Code criminel*); la possession illicite ou le trafic de documents d'identité délivrés par le gouvernement (nouveau paragraphe 56.1 du *Code criminel*).

Le vol d'identité et les dispositions des lois fédérales sur la protection des renseignements personnels

La *Loi sur la protection des renseignements personnels et les documents électroniques*[3] (LPRPDE), qui protège les renseignements personnels détenus par le secteur privé au Canada, s'applique aux activités commerciales à l'échelle du pays, exception faite de trois provinces considérées comme ayant des lois essentiellement similaires[4]. La Colombie-Britannique et l'Alberta se sont dotées de lois intitulées *Personal Information Protection Act* (PIPA)[5], tandis que c'est la *Loi sur la protection des renseignements personnels dans le secteur privé*[6] qui est en vigueur au

---

2 Le projet de loi S-4 a reçu la sanction royale le 22 octobre 2009 et est devenu la L.C. (2009), ch. 28.

3 *Loi sur la protection des renseignements personnels et les documents électroniques* (L.C. (2000), ch. 5).

4 Le Nouveau-Brunswick, l'Ontario et Terre-Neuve-et-Labrador ont des lois considérées essentiellement similaires pour ce qui est du domaine de la santé.

5 Colombie-Britannique, *Personal Information Protection Act*, (SBC (2003) ch. 63); Alberta, *Alberta's Personal Information Protection Act*, (SA (2003), ch. P-6.5). Rappelons que, dans l'arrêt *Alberta (Information and Privacy Commissioner) c. Travailleurs et travailleuses unis de l'alimentation et du commerce, section locale 401*, 2013 CSC 62, rendu le 15 novembre 2013, la Cour suprême du Canada a statué que la loi albertaine limitait indûment la collecte, l'utilisation et la communication de renseignements et portait atteinte au droit à la liberté d'expression du syndicat, garanti par l'alinéa 2*b*) de la *Charte canadienne des droits et libertés*. La Cour a estimé que la PIPA de l'Alberta était non valide, mais a suspendu cette déclaration pour une période de 12 mois afin de permettre à la législature albertaine d'y apporter les modifications propres à en garantir le caractère constitutionnel. Le 30 octobre 2014, la Cour a accordé à l'Alberta un délai supplémentaire de six mois.

6 Québec, *Loi sur la protection des renseignements personnels dans le secteur privé*, (ch. P-39.1).

Québec. Par ailleurs, la *Loi sur la protection des renseignements personnels*[7] (comparable aux lois provinciales) réglemente les activités du secteur public fédéral.

Ces lois de protection des données s'appliquent à la collecte, à l'utilisation et à la communication des renseignements personnels recueillis par des organismes publics et privés. La LPRPDE et les lois provinciales équivalentes jouent un rôle important dans la réduction du risque de vol d'identité en contraignant les entreprises du secteur privé à prendre les mesures de sécurité qui s'imposent pour ne recueillir que les renseignements personnels nécessaires à telle ou telle opération et pour détruire en toute sécurité les renseignements dont elles n'ont plus besoin. La *Loi sur la protection des renseignements personnels* impose des limites semblables au gouvernement fédéral en matière de collecte, d'utilisation et de communication de renseignements personnels.

Le Commissariat à la protection de la vie privée du Canada (CPVP) a publié plusieurs documents sur le vol d'identité à l'intention des entreprises et des consommateurs[8]. Par exemple, dans une fiche d'information, le CPVP invite les détaillants canadiens à faciliter la protection des renseignements personnels de leurs clients (comme l'exige la LPRPDE) en n'imprimant qu'une partie du numéro de carte de crédit sur les reçus remis aux clients, « car si un reçu est perdu, volé ou jeté, le numéro qui y figure peut être utilisé à des fins de fraude ou de vol d'identité, ou à d'autres fins criminelles[9] ».

Dans une autre fiche, intitulée « Pratiques exemplaires pour l'utilisation des numéros d'assurance sociale dans le secteur privé », il explique pourquoi les entreprises ne devraient pas utiliser de numéro d'assurance sociale (NAS) comme identificateur général et il rappelle que les organisations devraient limiter la collecte, l'utilisation et la communication des NAS aux seules fins prévues par la *Loi*[10], c'est-à-dire aux fins de la déclaration de revenus. Cela dit, comme le fait remarquer le CPVP, « il n'existe aucune loi qui interdit à une organisation de demander le NAS d'un client, ou à un client de fournir son NAS, à des fins autres que celles liées au revenu ». Le CPVP y voit deux problèmes : premièrement, le NAS est un renseignement personnel qui peut servir à voler l'identité de quelqu'un s'il n'est pas suffisamment bien protégé. Deuxièmement, comme le NAS est un renseignement personnel, la LPRPDE s'applique à sa collecte, à son utilisation et à sa communication.

Enfin, dans une fiche intitulée « Les entreprises et le vol d'identité », le CPVP explique en détail le lien entre la LPRPDE et la prévention du vol d'identité[11]. Il y insiste

---

7 *Loi sur la protection des renseignements personnels* (L.R.C. (1985), ch. P-21).

8 On peut trouver une liste de publications sur le vol d'identité sur le site du Commissariat à la protection de la vie privée, à la page intitulée *Vol d'identité et fraude*.

9 Commissariat à la protection de la vie privée du Canada, *Fiches d'information : Numéros de carte de crédit tronqués*, décembre 2009. Les sociétés émettrices de cartes de crédit comme Visa et MasterCard exigent désormais des commerçants qu'ils tronquent les numéros de carte de crédit sur leurs reçus.

10 Commissariat à la protection de la vie privée du Canada, *Fiche d'information : Pratiques exemplaires pour l'utilisation des numéros d'assurance sociale dans le secteur privé*, juillet 2004. Voir aussi : Commissariat à la protection de la vie privée, *Fiches d'information : Numéro d'assurance sociale*, avril 2008.

11 Commissariat à la protection de la vie privée, *Fiches d'information : Les entreprises et le vol d'identité*, mars 2007.

notamment sur l'importance de la responsabilité des entreprises dans la protection des renseignements de leurs clients et la réduction du risque de vol d'identité. L'un des problèmes qui multiplie ce risque est celui de l'accès illicite aux données :

> Les grands titres traitant d'importantes fuites de données et des risques de fraude d'identité ont suscité l'inquiétude des Canadiennes et Canadiens, et avec raison : ce type de fraude a fait des millions de victimes partout en Amérique du Nord.
>
> […]
>
> Conséquemment, il importe que les entreprises et les autres organisations — petites et grandes — élaborent des stratégies exhaustives pour protéger les renseignements personnels qui leur sont confiés.
>
> Au Canada, la loi exige la protection des renseignements personnels.
>
> […]
>
> Que peuvent faire les entreprises pour se prémunir contre le vol d'identité? En quelques mots, elles doivent gérer les renseignements personnels de la même façon qu'elles gèrent l'argent. Après tout, les renseignements personnels représentent une véritable mine d'or pour les voleurs d'identité et les criminels organisés.
>
> Il est possible de réduire les risques de vol d'identité en intégrant les principes fondamentaux de protection des renseignements personnels prévus dans la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) au sein de la culture des organisations.[12]

Selon le rapport annuel 2012-2013 du CPVP sur la *Loi sur la protection des renseignements personnels*, les Canadiens sont de plus en plus inquiet des « atteintes à la sécurité des renseignements personnels et [des] fuites de renseignements personnels d'une grande ampleur » dont ils entendent souvent parler[13]. Ces atteintes peuvent multiplier le risque de vol d'identité[14]. Dans son rapport, l'ex-commissaire invite les organisations du secteur public et du secteur privé à s'imposer l'obligation de signaler les atteintes à la sécurité des renseignements personnels pour améliorer la cybersécurité.

---

12 *Ibid*.

13 Commissariat à la protection de la vie privée au Canada, *Rapport annuel 2012-2013 concernant la* Loi sur la protection des renseignements personnels, octobre 2013.

14 Comme le fait remarquer l'ex-commissaire à la protection de la vie privée, Jennifer Stoddart, concernant la vérification des violations commises par l'Agence du revenu du Canada, « [u]ne atteinte liée à la consultation ou à la communication de renseignements sensibles sur des contribuables peut avoir de graves répercussions sur la ou les personnes touchées. Dans le pire des scénarios, elle peut entraîner un vol d'identité, une fraude financière et un embarras personnel pour les contribuables visés ».

APERÇU DES RÉPERCUSSIONS ÉCONOMIQUES DU VOL ET DE LA FRAUDE D'IDENTITÉ

A. Problèmes identifiés par les agences d'évaluation du crédit

Les agences d'évaluation du crédit des consommateurs (aussi appelées bureaux de crédit), comme Equifax Canada, Forrest Green et TransUnion Canada, recueillent et mettent en marché des données sur les antécédents des consommateurs en matière de crédit. Selon l'Agence de la consommation en matière financière du Canada (ACFC), organisme fédéral de réglementation chargé d'informer et de protéger les consommateurs de produits et de services financiers, le dossier des antécédents des consommateurs en matière de crédit fait la synthèse des types de crédit qu'ils utilisent, tels que les cartes de crédit, les prêts et les plans de financement[15]. Les antécédents en matière de crédit indiquent aussi si les paiements ont été effectués dans les délais. Ces renseignements sont obtenus auprès des agences d'évaluation du crédit des consommateurs. Celles-ci transmettent les renseignements sur les antécédents de crédit des consommateurs sous deux formes : le dossier de crédit et le pointage de crédit.

Le dossier de crédit est établi en fonction des antécédents des consommateurs en matière de crédit. Il contient des renseignements personnels, dont les données financières, comme les renseignements sur les comptes bancaires, les crédits en cours (cartes de crédit, marges de crédit et prêts), les faillites et les décisions judiciaires liées au crédit, les dettes ayant fait l'objet de mesures de recouvrement, ainsi que la liste de toutes les demandes de renseignements présentées à l'égard du crédit d'un consommateur.

Le pointage de crédit indique le risque que représente un consommateur pour les prêteurs potentiels, par comparaison à d'autres consommateurs. Les agences d'évaluation du crédit utilisent une échelle de 300 à 900 pour déterminer le pointage d'un consommateur. Les agences considèrent que plus le pointage s'approche de 900, moins le risque est élevé pour les prêteurs[16].

Equifax Canada

Au nom d'Equifax Canada, M. John Russo a présenté au Comité trois éléments principaux concernant le vol d'identité :

1. l'augmentation constante depuis 1998 des crimes reliés à l'identité,
2. l'existence de deux types de vols d'identité : vrais et synthétiques,

---

15 Gouvernement du Canada, Agence de la consommation en matière financière du Canada, *Au sujet de l'ACFC*.

16 Gouvernement du Canada, Agence de la consommation en matière financière du Canada, *Dossier de crédit et pointage de crédit*.

3. les problèmes les plus inquiétants découlant du vol d'identité et les mesures que peuvent prendre les consommateurs et les entreprises pour les éviter[17].

En ce qui concerne l'augmentation constante des crimes reliés à l'identité, M. Russo l'a expliquée par le nombre grandissant d'atteintes aux données personnelles, l'utilisation accrue des modes de livraison électronique et des réseaux, et l'influence des médias sociaux dans notre société[18]. Il s'est appuyé sur les données du Centre antifraude du Canada pour souligner que le nombre de Canadiens victimes de vol d'identité a augmenté de 14 % en 2013[19].

M. Russo a souligné le fait qu'un crime lié au vol d'identité commence nécessairement par un vol de renseignements personnels[20]. Selon Equifax, l'augmentation de renseignements personnels volés ou perdus est en partie imputable à des employés imprudents ou indisciplinés ou à des accès non autorisés dans diverses institutions, comme les détaillants, les fournisseurs de soins de santé, les institutions financières et le gouvernement[21]. M. Russo a souligné que l'augmentation des vols d'identité est également imputable aux infractions aux données personnelles. Il a donné l'exemple suivant : « à notre bureau de crédit, ces 18 derniers mois, nous avons protégé plus de 1,5 million de dossiers de crédit de Canadiens grâce à des alertes de crédit ou à une surveillance de crédit découlant directement d'infractions aux données personnelles, et ces chiffres sont constamment en hausse[22]. »

M. Russo a cité l'existence de statistiques récentes, qui démontrent que « la majorité des menaces qui pèsent de nos jours sur les renseignements personnels viennent d'attaques malveillantes ou criminelles contre les bases de données des organisations » et que « les infractions aux données personnelles sont en voie de devenir un trésor pour les fraudeurs[23]. » Il s'est basé sur une récente étude menée par le Ponemon Institute pour affirmer que 42 % des incidents concernant les renseignements personnels mettent en jeu des attaques malveillantes ou criminelles. Ces mêmes résultats démontreraient que les clients mettent fin à leur relation avec les entreprises dont les données ont été volées dans une plus grande proportion, le taux de roulement moyen ayant augmenté de 15 % entre 2013 et 2014[24].

---

17 Chambre des communes, Comité permanent de l'accès à l'Information, de la protection des renseignements personnels et de l'éthique (ETHI), *Témoignages*, 2e session, 41e législature, 27 mai 2014, 1105 (John Russo, vice-président, avocat et chef de la protection des renseignements personnels, Equifax Canada Co.).

18 *Ibid*.

19 *Ibid*.

20 *Ibid*.

21 *Ibid*.

22 *Ibid*.

23 *Ibid*.

24 *Ibid*.

M. Russo a mentionné l'existence de nombreux cas d'employés indisciplinés, ou de « fantassins », qui auraient vendu les renseignements personnels contenus dans les demandes de crédit faites auprès de leur employeur à des groupes criminels organisés[25]. Plusieurs enquêtes de police sur le vol d'identité auraient démontré que les renseignements personnels volés sont souvent trouvés par hasard lors de contrôles routiers ou de perquisitions menées pour d'autres motifs[26].

Selon M. Russo, le nombre de vols d'identité signalés au Canada a augmenté de 500% entre 1998 et 2003. L'augmentation se serait ensuite stabilisée de 2004 à 2005, mais serait revenue aux niveaux élevés de 2003 à partir de 2008, alors que les crimes d'identité fictive — ou synthétique — ont commencé à apparaître[27].

Un crime d'identité fictive ou synthétique consiste à utiliser des renseignements personnels volés pour créer une personne qui n'existe pas réellement ou à créer une identité de toutes pièces à partir de renseignements personnels inventés[28]. M. Russo a expliqué que ce genre d'identité est souvent créé en utilisant le NAS d'une personne décédée ou qui n'a pas encore obtenu de crédit, comme un enfant[29]. Le fraudeur aurait ensuite le loisir d'effectuer des centaines de milliers de dollars en opérations financières avant d'abandonner l'identité qu'il a créée et de disparaître sans laisser de trace[30]. Selon M. Russo :

> [N]ous voyons communément des dizaines, voire des centaines, d'identités fictives utilisées par le même groupe au même moment. Le crime organisé joue un grand rôle ici, puisque les produits de cette criminalité servent à financer une vaste gamme d'autres activités mondiales illégales, voire le terrorisme[31].

Selon les analyses de coûts menées par Equifax Canada, la fraude d'identité synthétique — ou fictive — coûterait aux Canadiens près d'un milliard de dollars en pertes par année[32]. Selon M. Russo, la création d'identités fictives entraîne des revenus de dizaines de millions de dollars pour des groupes du crime organisé chaque année[33]. Equifax aurait constaté que 1 300 dossiers de consommateurs fictifs sont créés en moyenne tous les mois au Canada par des fraudeurs et autres criminels organisés[34].

En ce qui concerne le troisième point mentionné par M. Russo, c'est-à-dire les problèmes les plus inquiétants qui découlent du vol d'identité et les mesures que peuvent

---

25 *Ibid*.

26 *Ibid*.

27 *Ibid*.

28 *Ibid*.

29 *Ibid*.

30 *Ibid*.

31 *Ibid*.

32 *Ibid*.

33 *Ibid*.

34 *Ibid*.

prendre les consommateurs et les entreprises pour les éviter : les problèmes identifiés suivent, alors que les mesures proposées seront abordées plus loin dans ce rapport.

M. Russo s'est appuyé sur une étude d'ABI Research pour souligner que le « hacktivisme » est en hausse : il représenterait maintenant 47 % de toutes les activités des groupes de cybermenace. Le mot « hacktivisme » est une contraction des mots « hacker » et « activisme », autrement dit le fait pour un criminel informatique de violer l'intégrité d'un système informatique dans le but de prôner une action politique violente. M. Russo a expliqué que si les activités de ces « hacktivistes » ne semblent pas liées à première vue, elles permettent en fait la communication de renseignements personnels qui peuvent ensuite servir à créer une identité réelle ou synthétique qui, à son tour, présente un risque financier réel pour les consommateurs[35].

Une autre source d'inquiétude pour les consommateurs et les entreprises, selon M. Russo, réside dans le fait qu'un consommateur sur trois qui est touché par des pertes de données devient une victime réelle de vol d'identité, tel que le démontrerait une étude nord-américaine de Javelin Strategy and Research[36]. Cette proportion était d'un consommateur sur quatre en 2012[37].

En réponse aux questions des membres du Comité, M[me] Carol Gray, présidente d'Equifax Canada, a mentionné qu'une proportion de 25 à 30% des Canadiens demandent d'avoir accès à leur dossier de crédit et que cette proportion change en fonction de l'âge, les personnes âgées ayant tendance à consulter leur dossier de crédit moins fréquemment que les jeunes[38]. Pour donner une idée du volume de dossiers de crédit qui sont détenus par Equifax, M. Russo a précisé que les dossiers de ses membres sont consultés 150 000 fois par jour et que 50 millions de comptes sont mis à jour chaque mois[39].

Forrest Green

Au nom de Forrest Green, M. Murray Rowe, Jr. s'est concentré sur la situation des communautés des Premières Nations face aux agences d'évaluation du crédit. Il a expliqué aux membres du Comité que l'entreprise dont il est le président considère que les communautés des Premières Nations sont parmi les plus vulnérables à la fraude et à l'exploitation financière[40]. C'est le manque de données de crédit concernant les membres des Premières Nations qui les rendrait plus sujets à la fraude[41]. M. Rowe a présenté ainsi leur situation :

---

35 *Ibid*.

36 *Ibid*, 1110.

37 *Ibid*.

38 *Ibid*, 1135 (Carol Gray, présidente, Equifax Canada Co.).

39 *Ibid*, 1140 (Russo).

40 *Ibid*, 1115 (Murray Rowe, Jr., président, Forrest Green Group of Companies).

41 *Ibid*.

> Dans de nombreux cas, ils ne comprennent pas le fonctionnement des bureaux de crédit. Ils vérifient rarement leurs rapports de solvabilité et, par conséquent, les gens à qui j'ai parlé sont surveillés de près; ils reçoivent des appels d'agences de recouvrement...[42]

Qui plus est, selon M. Rowe, les personnes habitant dans les réserves sont difficiles à trouver dans les cas où une entreprise comme la sienne cherche à les avertir qu'elles ont été victimes de fraude[43]. D'ailleurs, ces personnes communiquent rarement avec les agences d'évaluation du crédit[44]. Les données que M. Rowe a présentées au Comité démontrent que moins de 5 % des membres des Premières Nations ont examiné leur dossier de crédit : selon lui, la réalité pourrait même être plus près de 1 %[45].

M. Rowe a également attiré l'attention du Comité sur la question de la vérification de l'identité. En ce qui concerne les gens qui postulent pour des emplois à faibles revenus, les données des agences d'évaluation du crédit seraient utilisées régulièrement pour les analyses d'antécédents de crédit des postulants[46]. Selon M. Rowe, cette situation est ironique, parce que les personnes les plus vulnérables et qui ont le plus besoin d'un emploi sont celles qui sont les plus susceptibles d'être victimes de discrimination en raison d'une mauvaise cote de crédit[47]. Il considère que des liens doivent être établis entre le manque de données ou des données de faible qualité, la fraude, le vol d'identité et la vulnérabilité des personnes concernées[48].

En s'appuyant sur les conclusions d'un rapport du Comité permanent des affaires autochtones et du développement du Grand Nord de la Chambre des communes, M. Rowe a constaté que les communautés autochtones ont tendance à ne pas faire confiance aux organisations qui recueillent des données parce qu'elles ne font pas confiance à l'idée de partager des données ou qu'elles n'ont pas accepté cette idée[49].

TransUnion Canada

M. Todd Skinner, président de TransUnion Canada, a rappelé au Comité que son entreprise est régie par les lois sur la protection des consommateurs et sur la protection de la vie privée et que le consentement de la personne concernée est nécessaire pour obtenir un dossier de crédit[50].

---

42 *Ibid*.

43 *Ibid*.

44 *Ibid*.

45 *Ibid*.

46 *Ibid*.

47 *Ibid*.

48 *Ibid*.

49 *Ibid*.

50 *Ibid*, 1120 (Todd Skinner, président, TransUnion Canada).

Selon M. Skinner, le vol d'identité se divise en trois catégories: « la perte ou l'atteinte aux données, le vol d'identité en tant que tel qui en découle, et la fraude qui s'ensuit[51]. »

M. Skinner a noté que ce sont les consommateurs ou les entreprises qui informent son entreprise des atteintes aux données[52]. Cependant, les entreprises ne déclarent pas toujours ces atteintes, tel que le recommande le Commissariat à la protection de la vie privée du Canada dans sa publication « Principales étapes à suivre par les organisations en cas d'atteintes à la vie privée »[53].

Selon les statistiques de TransUnion, le nombre d'atteintes aux données déclarées au cours des cinq dernières années a diminué de 30 %, alors que le nombre de victimes potentielles aurait augmenté de 600 %[54]. M. Skinner a précisé que 8 % des atteintes déclarées viennent des institutions financières alors que 70 % de ces atteintes viennent du secteur médical, de celui des services ou encore du secteur du détail[55]. En ce qui concerne le gouvernement, les compagnies d'assurances ou les entreprises du secteur financier, M. Skinner a noté qu'il y avait très peu d'atteintes aux données déclarées[56].

Selon M. Skinner, le nombre confirmé de victimes de fraude d'identité a augmenté de 100 %[57]. Il a noté qu'une grande partie des consommateurs déclarent ces fraudes au Centre antifraude du Canada tout en notant une augmentation de 300 % du nombre d'alertes à la fraude publiées[58]. Il s'est toutefois dit d'avis que ces chiffres laissaient place à l'amélioration[59].

En cas d'atteinte aux données, M. Skinner a souligné que ce sont les consommateurs qui en assument les conséquences, « à moins que les entreprises ou les organisations gouvernementales ayant causé l'atteinte soient prêtes à payer pour les dommages qu'elles ont créés[60]. » Selon ce qu'a affirmé M. Skinner au Comité, ce sont les entreprises qui ont compromis les renseignements personnels des consommateurs qui devraient en assumer les frais, même si ce ne sont pas toutes les entreprises qui le font ou qui investissent pour réduire le risque que ces atteintes surviennent[61].

---

51 *Ibid*.

52 *Ibid*.

53 *Ibid*. Voir : Commissariat à la protection de la vie privée du Canada, Lignes directrices, *Principales étapes à suivre par les organisations en cas d'atteintes à la vie privée*.

54 ETHI, *Témoignages*, 2e session, 41e législature, 27 mai 2014, 1120 (Skinner).

55 *Ibid*.

56 *Ibid*.

57 *Ibid*.

58 *Ibid*.

59 *Ibid*.

60 *Ibid*, 1125.

61 *Ibid*.

M. Skinner a également attiré l'attention du Comité sur le fait qu'aucune méthode automatisée ne permet présentement au secteur privé d'obtenir la confirmation qu'une pièce d'identité a été émise par le gouvernement ou qu'une pièce d'identité appartient réellement à la personne qui se présente comme sa propriétaire[62].

B. Problèmes identifiés par le secteur bancaire

Banque Canadienne Impériale de Commerce

Au nom de la Banque Canadienne Impériale de Commerce, M. Philip Fisher a expliqué que le vol d'identité n'est pas un problème nouveau ou grandissant, mais plutôt une « réalité en constante évolution[63]. » Les méthodes utilisées pour commettre ce crime auraient changé : l'époque des vols de reçus, de factures ou de portefeuille, ainsi que des fraudes par téléphone, serait donc révolue[64]. Selon M. Fisher, il est plutôt question aujourd'hui de menaces persistantes avancées, d'atteintes aux dispositifs de sécurité des commerçants, de logiciels malveillants et de hameçonnage[65]. Le risque concernant l'intégrité de l'identité d'une personne ne serait plus le même, en raison des avancées technologiques et de la diffusion de renseignements personnels sur Internet[66].

Pour l'étude du Comité, M. Fisher a souligné l'importance de s'entendre sur une définition commune du vol d'identité. Il a souligné le fait que les institutions financières n'utilisent pas toutes la même définition du vol d'identité, ce qui expliquerait en partie la difficulté d'obtenir des données globales sur ce problème[67]. M. Fisher a cité la définition du *Code criminel*, selon laquelle quiconque obtient ou a en sa possession des renseignements identificateurs sur une autre personne en vue de commettre un acte criminel commet un vol d'identité[68]. Les renseignements identificateurs en question comprennent, notamment « le nom d'une personne, son adresse, sa date de naissance, sa signature manuscrite ou électronique, son code d'usager, son numéro de carte de crédit ou de débit, son numéro de compte d'une institution financière, son numéro d'assurance sociale ou de permis de conduire ou l'un de ses mots de passe[69]. »

Selon M. Fisher, les institutions financières utilisent généralement une définition plus restreinte du vol d'identité et ont tendance à surveiller et à déclarer les fraudes en fonction des types de fraude qui, à leur tour, sont généralement définis en fonction de la

---

62 *Ibid*.

63 ETHI, *Témoignages*, 2e session, 41e législature, 29 mai 2014, 1105 (Philip Fisher, directeur sénior, Gestion des risques des canaux électroniques, Services intégrés de contrôle des affaires, Banque Canadienne Impériale de Commerce).

64 *Ibid*.

65 *Ibid*.

66 *Ibid*.

67 *Ibid*.

68 *Ibid*.

69 *Ibid*.

source des renseignements volés ou de la manière dont les renseignements sont utilisés[70].

En guise d'exemple de fraude, il a mentionné la copie de données contenues dans une carte à bande magnétique à un point de vente ou à un guichet automatique, qui mène habituellement à la création de cartes contrefaites ou à des achats qui ne nécessitent pas de carte[71]. Selon M. Fisher, les banques n'assimilent généralement pas ce type de fraude à un vol d'identité parce que le nombre de renseignements volés est limité[72].

Par opposition, le vol de renseignements contenus dans un ordinateur personnel infecté par un logiciel malveillant représenterait un type de fraude préoccupant parce que le nombre de renseignements en cause est plus élevé que dans l'exemple précédent et le niveau de difficulté pour déceler et régler le problème est plus élevé[73].

M. Fisher a présenté au Comité un type de fraude en pleine évolution : la fraude par courriel ou le hameçonnage visant l'obtention de renseignements personnels, comme un authentifiant ou un numéro de carte de crédit, qui permettent d'accéder à un compte bancaire en ligne[74]. M. Fisher a également constaté que les fraudeurs tentent de plus en plus d'élargir la gamme de renseignements volés[75].

M. Fisher a présenté d'autres exemples de fraude, comme le vol de courriels ou les atteintes à la protection des données de tierces parties : les commerçants et les fournisseurs de services de traitement des transactions, par exemple[76]. Il a souligné que selon l'entreprise visée par l'attaque, ces atteintes aux données peuvent toucher un grand nombre de consommateurs[77].

Autres banques

M. Paul Milkman, au nom du Groupe Financier Banque TD, a tenu à faire une distinction entre le crime de vol d'identité et celui de l'utilisation active d'une identité volée pour perpétrer une fraude financière[78]. Considérant qu'il existe un lien de cause à effet entre un vol d'identité et une fraude financière, il a affirmé que les banques doivent

---

70 *Ibid*.

71 *Ibid*.

72 *Ibid*.

73 *Ibid*.

74 *Ibid*.

75 *Ibid*.

76 *Ibid*.

77 *Ibid*.

78 *Ibid*, 1115 (Paul Milkman, vice-président sénior, Chef de la Gestion du risque technologique et de la Sécurité des systèmes d'information, Groupe Financier Banque TD).

disposer de stratégies de prévention intégrées à l'égard de ces deux crimes et que les intérêts des banques rejoignent ceux de leurs clients dans la prévention de ces crimes[79].

M. Ed Rosenberg, de BMO Groupe financier, a expliqué que la vitesse à laquelle changent les processus et les dispositifs de contrôle internes de la banque qu'il représente fait en sorte que la qualité et la sécurité des documents peuvent varier d'une administration à l'autre et qu'il existe peu de moyens fiables d'authentifier les documents de façon universelle[80].

Le représentant de la RBC, M. Jay Stark, a tenu à souligner qu'en plus de provoquer des pertes financières substantielles et d'autres conséquences négatives pour les consommateurs, le vol d'identité peut permettre aux criminels de financer leurs activités, incluant des activités terroristes[81].

M. Stark a remarqué que les avis des différents intervenants dans l'étude du Comité divergent sur le nombre de cas de vols d'identité commis, sur la définition du crime de vol d'identité, ainsi que sur les solutions à apporter à ce problème[82].

M. Stark a également remarqué que les stratégies que les banques utilisent ont donné lieu à un déplacement des activités liées à la fraude : la présence des cartes à puce et des numéros d'identification personnels (NIP) aurait entrainé une augmentation des fraudes transfrontalières et des fraudes liées aux transactions sans carte, par exemple[83].

---

79 *Ibid*.

80 *Ibid*, 1120 (Ed Rosenberg, vice-président et chef de la sécurité, Groupe légal, corporatif et de conformité, BMO Groupe financier).

81 *Ibid*, 1125 (Jay Stark, vice-président, Services de vérification interne, Services bancaires aux particuliers et aux entreprises, RBC).

82 *Ibid*.

83 *Ibid*.

MESURES PRISES, OU SUGGÉRÉES, PAR LES ENTREPRISES POUR PROTÉGER LES CANADIENS CONTRE LE VOL D'IDENTITÉ

A. Mesures prises, ou suggérées, par les entreprises afin de contrer le phénomène du vol d'identité au Canada

Agences d'évaluation du crédit

Equifax Canada

Selon M. Russo, d'Equifax Canada, bien que les entreprises canadiennes aient pris plusieurs mesures de prévention contre le vol d'identité, il y a des limites aux mesures qu'elles peuvent prendre[84]. Il a insisté sur la quantité importante de transferts électroniques de renseignements personnels dans le traitement des transactions financières, alors que des milliers de dossiers de crédit personnels sont transmis par voie électronique tous les jours[85]. Qui plus est, des milliers de demandes de crédit, allant des prêts bancaires aux crédits-bails automobiles, seraient traitées chaque jour[86].

Selon M. Russo, « l'industrie des services financiers et du crédit continuent de faire leur part en aidant les victimes de crimes d'identité et en investissant des millions de dollars chaque année pour détecter les fraudes d'identité le plus rapidement possible[87]. »

M. Russo a argué que face au problème de la hausse d'identités fictives qui sont créées, nos lois, notre sécurité et nos tactiques de prévention doivent changer en même temps que les criminels évoluent[88]. Il a plaidé pour la concertation des autorités réglementaires, des forces de l'ordre et des solutions proposées par des organisations comme la sienne afin de régler le problème[89].

Par ailleurs, M. Russo a profité de son passage devant le Comité pour offrir certains conseils aux consommateurs. Premièrement, ces derniers devraient « vérifier leur dossier de crédit au moins une fois par trimestre afin de détecter toute anomalie ou fraude possible dans leur dossier[90]. »

---

84 ETHI, *Témoignages*, 2e session, 41e législature, 27 mai 2014, 1105 (Russo).

85 *Ibid*.

86 *Ibid*.

87 *Ibid*.

88 *Ibid*.

89 *Ibid*.

90 *Ibid*.

Deuxièmement, les victimes de perte de renseignements personnels devraient demander à l'organisation responsable de la perte de leur fournir, à ses frais, des services de surveillance de crédit pour au moins 12 mois suivant la perte en question[91]. Selon M. Russo, c'est durant cette période de 12 mois suivant la perte de renseignements personnels que la plupart des crimes liés au vol d'identité sont commis[92].

Troisièmement, M. Russo considère que les consommateurs doivent être vigilants et ne pas communiquer de renseignements personnels qui ne sont pas nécessaires pour l'opération visée, comme un numéro d'assurance sociale ou une date de naissance pour effectuer une simple opération au détail ou une location[93].

En somme, la lutte contre les crimes liés à l'identité commence par l'éducation et la conscientisation des consommateurs et des ménages canadiens, selon M. Russo[94]. Cette éducation et cette conscientisation se feraient à la lumière de certains incidents d'infractions aux données personnelles, où des entreprises ont été piratées ou attaquées avec malveillance en vue d'obtenir des renseignements personnels de nature délicate et confidentielle[95].

En réponse aux questions des membres du Comité sur des moyens qui pourraient encourager les consommateurs à demander l'accès à leur dossier de crédit, M. Russo a cité l'exemple des visites de représentants d'Equifax Canada dans les écoles, dans le cadre des programmes de réussite des jeunes, pour enseigner aux jeunes Canadiens ce qu'est un rapport de solvabilité, comment le lire et ce qui influe sur leur cote de solvabilité, en préparation au moment où ils pourront accéder au crédit[96]. M[me] Tara Zecevic, également d'Equifax Canada, a ajouté à cet égard que l'éducation et la littératie financière sont des éléments importants pour prévenir l'endettement des consommateurs[97].

Forrest Green

Selon M. Rowe, de Forrest Green, l'éducation contribuera à régler le problème de la vulnérabilité des membres des Premières Nations face à la fraude d'identité causée par le manque de données de crédit les concernant[98]. Selon M. Rowe :

> Il faut en parler et on ne peut pas seulement se fier aux chefs d'aujourd'hui. Ils ne connaissent pas ce sujet. Ils ne peuvent pas expliquer à leurs enfants comment préparer de bons rapports de solvabilité parce que personne ne leur a dit comment le faire[99].

---

91 *Ibid*.

92 *Ibid*.

93 *Ibid*, 1110.

94 *Ibid*, 1105.

95 *Ibid*.

96 *Ibid*, 1220.

97 *Ibid*, 1220 (Tara Zecevic, vice-présidente, Decision Solutions, Equifax Canada Co.).

98 *Ibid*, 1115 (Rowe).

M. Rowe a fait un lien entre ce besoin d'éducation financière et la discrimination dont sont victimes les membres des Premières Nations dans l'obtention de crédit de la part d'institutions financières. Une enquête informelle effectuée par Forrest Green auprès de cinq bandes montrerait que les taux d'intérêt sont plus élevés de 300 % pour les collectivités autochtones, même en tenant compte des garanties de prêt du gouvernement, qui garantissent l'entièreté de la somme empruntée[100]. Selon M. Rowe, le problème systémique du secteur bancaire avec les Autochtones et la façon dont les agences d'évaluation du crédit recueillent et distribuent des renseignements sont des problèmes qui doivent être examinés avec les collectivités autochtones[101].

TransUnion Canada

Les données de TransUnion indiquent que les entreprises, mises à part celles du secteur financier, ne sont pas suffisamment sensibilisées au problème du vol d'identité[102]. La solution serait de faire plus d'éducation dans ce domaine sur les obligations découlant d'une atteinte aux données et sur les protocoles de sécurité pour empêcher ces atteintes[103].

Dans le même ordre d'idées, M. Skinner a affirmé que TransUnion appuyait les dispositions du projet de loi S-4 concernant la divulgation des atteintes aux données[104]. Selon M. Skinner, qui a dit ne pas vouloir pour autant que les clients des entreprises concernées soient inondés d'avis d'atteinte aux données, le fait d'aviser ces clients en cas de risque de préjudice matériel découlant d'une atteinte présente des avantages[105].

Selon M. Skinner, les atteintes aux données augmentent le volume d'appels aux centres de TransUnion et d'Equifax ainsi que les demandes de divulgation d'alertes aux consommateurs[106]. Il a affirmé que ces entreprises ont fait des investissements technologiques afin de rendre leur réponse aux consommateurs la plus efficace possible et pour contribuer à l'augmentation de 300 % du nombre d'alertes à la fraude publiées par les bureaux de protection des consommateurs à laquelle il faisait allusion plus tôt[107]. M. Skinner a affirmé que les mesures prises par les agences d'évaluation du crédit

---

99 *Ibid*.

100 *Ibid*, 1140.

101 *Ibid*.

102 *Ibid*, 1125 (Skinner).

103 *Ibid*.

104 *Ibid*. Le 21 avril 2015, le Comité permanent de l'industrie, de la science et de la technologie de la Chambre des communes a adopté le projet de loi S-4, Loi modifiant la Loi sur la protection des renseignements personnels et les documents électroniques et une autre loi en conséquence, et en a fait rapport à la Chambre le lendemain sans l'amender.

105 ETHI, *Témoignages*, 2e session, 41e législature, 27 mai 2014, 1125 (Skinner).

106 *Ibid*.

107 *Ibid*..

réduisent le nombre de fraudes et il s'est réjoui du fait que ce nombre n'augmente pas au même rythme que celui des victimes de fraudes potentielles[108].

M. Skinner a insisté sur le fait que la première chose à faire en cas d'atteinte aux données est d'aviser le Commissariat à la protection de la vie privée[109]. À cet égard, il a informé le Comité que TransUnion appuyait les modifications à la LPRPDE contenues dans le projet de loi S-4. Selon M. Skinner, après qu'une organisation ait confirmé la perte de données financières, elle devrait en informer Equifax et TransUnion qui devraient, à leur tour, publier des alertes à la fraude pour réduire la possibilité de vol d'identité[110].

Les mesures prises par TransUnion consistent à collaborer avec les autorités policières pour déclarer les activités suspectes, selon M. Skinner. TransUnion reçoit des renseignements concernant des activités suspectes, les entre dans une base de données sur la fraude et les transmet aux institutions financières[111]. La prévention de ces crimes passerait par une meilleure technologie, qui empêcherait que les cartes d'identité soient facilement copiées et authentifiées[112]. De plus, une véritable résolution du problème passerait par la mise en commun des renseignements détenus par les agences gouvernementales et le secteur financier[113]. Selon M. Skinner, les fraudeurs profitent de cette absence de partage de renseignements[114].

Face au problème d'absence de méthode automatisée qui permettrait au secteur privé d'obtenir la confirmation qu'une pièce d'identité a été émise par le gouvernement, ou qu'une pièce d'identité appartient réellement à la personne qui se présente comme sa propriétaire, M. Skinner a argué que TransUnion et Equifax Canada pourraient « servir de courroies de transmission pour les institutions financières », étant donné qu'elles font déjà une vérification d'identité pour l'analyse des profils de clients dans le cadre de la lutte contre le blanchiment d'argent[115].

En réponse aux questions des membres du Comité sur des moyens qui pourraient encourager les consommateurs à demander l'accès à leur dossier de crédit, M[me] Banfield a souligné qu'en plus des campagnes dans les écoles, beaucoup d'information se trouve sur le site Web de TransUnion, ce qui serait le résultat d'une collaboration avec les services de police et plusieurs autres agences[116].

---

108 *Ibid*.

109 *Ibid*.

110 *Ibid*.

111 *Ibid*.

112 *Ibid*.

113 *Ibid*.

114 *Ibid*.

115 *Ibid*. À cet égard, M. Skinner a fait référence au document « Stratégie nationale de lutte contre les crimes liés à l'identité », publié par la GRC.

116 ETHI, *Témoignages*, 2[e] session, 41[e] législature, 27 mai 2014, 1220 (M[e] Chantal Banfield, vice-présidente et avocate générale, TransUnion Canada).

Secteur bancaire

Banque Canadienne Impériale de Commerce

Selon M. Fisher, de la Banque Canadienne Impériale de Commerce, certains des problèmes reliés au vol d'identité qui ont été identifiés par le secteur bancaire ont mené, avec le temps, à la mise en place de mesures de contrôle solides et bien établies conçues pour déceler ces problèmes et les régler[117]. Cependant, certains problèmes liés au vol d'identité plus récents ont donné lieu à des mesures de contrôle correspondantes qui ne sont pas aussi solidement établies[118].

M. Fisher a mentionné le fait que les institutions financières se sont dotées de dispositifs perfectionnés de détection et de contrôle de la fraude tout en arguant qu'une lutte efficace contre le vol d'identité passe par une collaboration entre les institutions financières, les consommateurs et le gouvernement[119]. En guise de mesure prise par les banques qui serait un exemple à suivre, M. Fisher a cité le cas du dispositif inviolable dont sont dotés les guichets automatiques, qui aurait fait en sorte que les cas de trafiquage de guichets automatiques ont diminué de façon draconienne[120].

Tout en soulignant l'importance du rôle des consommateurs dans cette lutte, il a reconnu que les consommateurs ne sont pas des spécialistes de la fraude et qu'ils ont besoin que les institutions financières et les organismes gouvernementaux les informent des risques encourus et leur fournissent des outils de protection contre le vol d'identité[121]. L'envoi d'alertes en cas de transaction douteuse ou la surveillance gratuite d'une agence d'évaluation du crédit fournis par certaines institutions financières constitueraient de bons exemples d'outils à la disposition des consommateurs[122].

M. Fisher a également souligné l'importance du rôle du gouvernement dans la protection des consommateurs contre le vol d'identité et a prôné un renforcement des mesures de contrôle dans ce domaine[123].

Groupe Financier Banque TD

M. Milkman a estimé que la prévention en matière de crimes reliés à l'identité est une responsabilité partagée entre les banques et leurs clients[124]. À cet égard, le Groupe Financier Banque TD a mis en place un processus en quatre étapes qui cherche à

---

117 ETHI, *Témoignages*, 2e session, 41e législature, 29 mai 2014, 1105 (Fisher).

118 *Ibid*.

119 *Ibid*.

120 *Ibid*, 1110.

121 *Ibid*, 1105.

122 *Ibid*.

123 *Ibid*.

124 *Ibid*, 1115 (Milkman).

responsabiliser ses clients en matière de protection des renseignements personnels en leur demandant de :

1. faire preuve de prudence au moment de communiquer leurs renseignements personnels : demander comment seront utilisés les renseignements demandés, la raison pour laquelle ils sont demandés, les personnes auxquelles ils seront transmis et les mesures qui seront prises afin d'en préserver la confidentialité; ne jamais divulguer un numéro d'identification personnel, un numéro d'assurance sociale ou un mot de passe; ne pas publier dans les médias sociaux de mots de passe utilisés pour des transactions bancaires[125];

2. prendre des mesures de sécurité appropriées : conserver en lieu sûr les relevés de compte; tirer parti des technologies qui permettent de naviguer sur Internet de façon plus sécuritaire et en protégeant mieux les renseignements personnels, comme les signatures numériques, les logiciels antivirus, les pare-feu personnels et le cryptage des données[126];

3. vérifier l'exactitude des relevés de compte : s'assurer que toutes les transactions et tous les frais qui y figurent sont exacts et obtenir une fois par année un rapport de solvabilité d'une agence d'évaluation du crédit pour s'assurer que tout est en ordre[127];

4. protéger les cartes bancaires, les chèques et les cartes d'identité : n'apporter en voyage que les cartes de crédit nécessaires; laisser à la maison la carte d'assurance sociale et entreposer en lieu sûr une liste de toutes les cartes et des numéros qui y sont reliés[128].

Selon M. Milkman, les banques « investissent des sommes substantielles afin de répondre continuellement à des normes élevées en matière de sécurité et de protéger leurs systèmes et les renseignements personnels de leurs clients contre toute consultation ou utilisation non autorisée[129]. » Il a mentionné en guise d’exemple que les systèmes du Groupe Financier Banque TD ont été conçus pour « préserver en tout temps le caractère privé et confidentiel des numéros d'identification personnels, des mots de passe et des autres codes d'accès[130]. »

---

125 *Ibid*.

126 *Ibid*.

127 *Ibid*.

128 *Ibid*.

129 *Ibid*.

130 *Ibid*.

Selon M. Milkman, les banques ont pris des mesures pour rendre les transactions en ligne plus sécuritaires[131]. En ce qui concerne la banque qu'il représente, M. Milkman a mis de l'avant le fait qu'elle avait, notamment pris des mesures concernant

> la collecte de renseignements exhaustifs sur les menaces, la mise en place de dispositifs de contrôle de gestion de l'accès, la journalisation et l'analyse des transactions, la mise en place de pare-feu sécurisés, la surveillance continue visant la détection proactive des activités inhabituelles dans les comptes des clients, la protection contre le hameçonnage et les pourriels et l'adoption des logiciels de cryptage les plus perfectionnés pour faire en sorte que les données ne puissent être décodées et déchiffrées que par notre système ou le client concerné[132].

BMO Groupe financier

Au nom de BMO Groupe financier, M. Ed Rosenberg a mentionné au Comité des exemples de mesures que la banque a prises pour contrer le vol d'identité, comme l'organisation de séances d'information sur la lutte contre la fraude à l'intention de ses employés, la mise à la disposition de ses clients en succursale de dépliants sur le hameçonnage, l'ajout aux relevés bancaires de conseils pour éviter la fraude, et la diffusion de messages de prévention sur Twitter et sur Facebook[133].

M. Rosenberg a insisté sur la collaboration qui existe entre la direction de la banque et ses employés pour élaborer des programmes destinés à prévenir et à détecter les risques d'activité criminelle dans différents secteurs, comme la gestion du traitement des espèces, des dossiers de crédit et des transactions; la gestion des renseignements personnels et financiers et la conformité avec les exigences des organismes de réglementation[134].

M. Rosenberg a précisé que BMO Groupe financier collabore à certaines initiatives qui sont organisées par l'ensemble du secteur bancaire, menées sous l'égide de l'Association des banquiers canadiens (ABC), qui ont pour objectif d'identifier les criminels et d'aider les organismes d'application de la loi à les poursuivre en justice[135].

---

131 *Ibid*.

132 *Ibid*, 1120.

133 *Ibid*, 1120 (Rosenberg).

134 *Ibid*.

135 *Ibid*.

Selon M. Rosenberg,

> [l]'adoption des normes en matière de cartes à puce et de numéros d'identification personnels a coûté à elle seule des millions de dollars à l'industrie, qui a fait ces investissements en vue de réduire les risques de fraude liés aux cartes au Canada[136].

M. Rosenberg a expliqué que l'adoption par le crime organisé de nouvelles technologies a mené les membres du secteur bancaire à mettre en place des forums de discussion et des outils de collaboration pour échanger des renseignements en matière de fraude et de mécanismes de contrôle préventif[137]. Cette collaboration, qui se fait, notamment par le truchement de l'ABC, amène les banques à entrer en communication avec différents intervenants, comme des fournisseurs d'accès Internet en ce qui concerne la cybercriminalité, des compagnies d'assurance en ce qui concerne les fraudes courantes, ou les organismes d'application de la loi en ce qui concerne le partage de renseignements sur les tendances criminelles[138]. M. Rosenberg a ajouté que ce genre de collaboration se fait également à l'échelle internationale[139].

RBC

Selon M. Stark, de la RBC, une réaction appropriée au problème du vol d'identité doit passer par l'optimisation des liens entre « les quatre piliers de la gestion de la fraude » suivants : les répercussions sur les clients ou les désagréments qui leur sont causés; les pertes liées aux fraudes; les coûts liés à la fraude que doivent assumer les banques et la société; et la gestion des risques[140].

M. Stark a affirmé que la lutte contre la fraude doit se faire en établissant un équilibre entre ce qu'il a appelé « les divers éléments stratégiques clés de la gestion de la fraude », c'est-à-dire le renseignement; la prévention, ce qui renvoie à la sensibilisation et à l'éducation des consommateurs; la détection; et l'analyse des causes profondes du crime[141]. Selon lui, les progrès réalisés au chapitre des analyses relatives à la détection représentent la mesure de lutte contre la fraude qui s'est avérée la plus efficace au cours de la dernière décennie[142].

M. Stark s'est réjoui des bons résultats qu'ont donné la démarche et les stratégies décrites, notamment en ce qui concerne les fraudes liées aux prêts sur carte de débit ou

---

136 *Ibid*.

137 *Ibid*.

138 *Ibid*.

139 *Ibid*.

140 *Ibid*, 1125 (Stark).

141 *Ibid*.

142 *Ibid*.

carte de crédit et les fraudes liées aux chèques[143]. Selon lui, le nombre de cas de fraude qui ont touché la RBC l'an dernier a été le plus bas des 10 dernières années[144].

Banque Scotia

Au nom de la Banque Scotia, M[me] Jennifer Frook a concentré ses observations relatives aux mesures prises pour contrer le vol d'identité autour des éléments suivants : la formation et l'éducation; la prévention; la détection et l'atténuation; et la collaboration[145]. Elle a affirmé que pour protéger ses clients contre le vol d'identité et les autres formes de fraude, la Banque Scotia accorde beaucoup d'importance à la formation de son personnel et transmet de l'information sur la sécurité des données à ses clients[146].

En guise d'exemples de mesures prises par la banque qu'elle représente pour protéger l'intégrité des renseignements de ses clients, M[me] Frook a d'abord mentionné le fait que la technologie de la carte à puce, qui est intégrée aux cartes de crédit et aux cartes de débit de toutes les banques canadiennes, est également intégrée aux guichets automatiques de la Banque Scotia[147]. Les cartes de débit émises de cette dernière sont également dotées de la technologie Flash Interac, qui utilise des puces sécurisées empêchant le clonage et la contrefaçon[148]. Quant à ses cartes de crédit pour la vente au détail, elles sont munies d'une technologie semblable : la fonctionnalité Visa payWave[149].

M[me] Frook a également mentionné l'existence d'un service d'alertes qui envoie aux clients de la Banque Scotia des courriels ou des messages texte dans le but de les aider à surveiller l'activité de leurs comptes bancaires[150].

M[me] Frook a expliqué que les réseaux que sa banque utilise et les produits qu'elle offre ont certains dispositifs de contrôle qui détectent les activités suspectes dans le but d'empêcher les fraudeurs d'accéder à son système[151].

M[me] Frook a également expliqué la procédure que suivent les banques en cas de vol des renseignements personnels de ses clients : elles avisent d'abord leurs clients que la sécurité de leur carte ou de leur compte a été compromise, elles bloquent ensuite l'authentifiant qui a été volé et elles le remplacent, en émettant, par exemple une nouvelle

---

143 *Ibid*.

144 *Ibid*.

145 *Ibid*, 1130 (Jennifer Frook, directrice, Services partagés, Bureau de la gestion des fraudes, Banque Scotia).

146 *Ibid*.

147 *Ibid*.

148 *Ibid*.

149 *Ibid*.

150 *Ibid*.

151 *Ibid*.

carte de crédit ou en réinitialisant le mot de passe du client victime du vol en question[152].

Selon M[me] Frook, la Banque Scotia surveille les mouvements liés aux comptes de ses clients pour détecter les transactions suspectes ou frauduleuses[153]. Elle met également à jour les profils de ses clients pour inscrire les vols d'identité dont ils ont été victimes, ce qui permet aux employés de la banque d'appliquer les mesures appropriées au moment d'authentifier ses clients et leur compte[154]. Selon M[me] Frook, sa banque indemnise entièrement ses clients pour leurs pertes lorsqu'ils sont victimes d'un vol d'identité[155].

M[me] Frook a également affirmé que « les banques collaborent avec le commissaire à la protection de la vie privée et lui transmettent toute information concernant une atteinte importante ou systémique à la sécurité des renseignements personnels[156]. »

En ce qui concerne la collaboration rendue nécessaire par le fait que le vol d'identité serait presque toujours commis à l'extérieur de l'environnement bancaire, M[me] Frook a mentionné que les activités internes de surveillance de la fraude permettent à la banque de recueillir des renseignements qu'elle transmet à d'autres organisations comme Visa, American Express, Interac, des organismes d'application de la loi et l'ABC[157].

Selon M[me] Frook,

> [c]es organisations compilent également de l'information transmise par d'autres institutions financières, et elles fournissent à l'industrie des paramètres et des points de repère à partir desquels nous pouvons évaluer la mesure dans laquelle nous parvenons à limiter les cas de fraude, dont un certain nombre sont attribuables à un vol quelconque de renseignements personnels d'un client[158].

En guise d'exemple de cette forme de collaboration, M[me] Frook a cité l'exemple d'un groupe créé par l'ABC et composé d'experts dont le mandat est de prévenir la fraude et de mettre en commun des renseignements et des pratiques exemplaires[159].

---

152 *Ibid*.

153 *Ibid*.

154 *Ibid*.

155 *Ibid*.

156 *Ibid*.

157 *Ibid*, 1135.

158 *Ibid*.

159 *Ibid*.

Entreprises des technologies de l'information

Rogers Communications

Au nom de Rogers Communications, M. Kenneth Engelhart a présenté au Comité un rapport, publié le matin même, qui donne le nombre et le type de requêtes d'information sur les clients de Rogers que l'entreprise a reçues en 2013 de la part d'agences gouvernementales et d'organismes chargés d'appliquer la loi[160]. Rogers a d'ailleurs invité le gouvernement fédéral à « soumettre son propre rapport afin de faire davantage la lumière sur ces demandes[161]. »

Le tableau qui suit présente les six catégories de requêtes établies par Rogers ainsi que le nombre de requêtes qu'elle a reçues dans chacune de ces catégories.

Nombre de requêtes par catégorie en 2013

Vérification du nom et de l'adresse d'un client	87 856
Mandat/ordonnance du tribunal	74 415
Lettre d'ordonnance gouvernementale (nous sommes contraints de fournir des renseignements en vertu d'une loi fédérale ou provinciale)	2 556
Requêtes urgentes des services policiers dans les cas où la vie de quelqu'un est en danger	9 339
Requêtes d'aide urgente dans les cas d'exploitation sexuelle des enfants	711
Ordonnance d'un tribunal validant une requête soumise par un organisme étranger en vertu d'un traité d'entraide juridique	40
Total	174 917

Remarques :

1. Ces statistiques comprennent les scénarios suivants : (a) L'information demandée a été fournie; (b) De l'information partielle a été fournie; (c) Aucune information n'a été fournie étant donné qu'elle n'existe pas ou que la personne n'est pas un client de Rogers; (d) Nous avons refusé la requête ou nous l'avons contesté avec succès devant les tribunaux.

2. Ces statistiques ne comprennent pas les requêtes informelles comme les appels téléphoniques des organismes d'application de la loi cherchant à obtenir des renseignements

---

160 ETHI, *Témoignages*, 2e session, 41e législature, 5 juin 2014, 1110 (Kenneth Engelhart, vice-président principal, Réglementation et chef de la protection des renseignements personnels, Rogers Communications inc.). Le rapport s'intitule *Rapport sur la transparence de 2013*.

161 *Ibid*.

> exigeant un mandat. Ces requêtes sont refusées, puisqu'elles ne sont pas issues de l'autorité juridique compétente et aucune réponse officielle n'est fournie.
>
> Source : Rogers Communications, *Rapport sur la transparence de 2013*, p. 2.

Le rapport indique pour chaque catégorie l'autorité juridique en vertu de laquelle Rogers décide de communiquer des renseignements, comme la LPRPDE, le *Code criminel* ou la *Loi de l'impôt sur le revenu*.

Fait à noter, le rapport n'indique pas le nombre de requêtes qui ont effectivement entrainé une communication de renseignements de la part de Rogers. À cet égard, M. Engelhart a apporté la précision suivante :

> Veuillez noter que nous ne répondons pas à toutes les demandes que nous recevons. Lorsque nous estimons que la portée d'une ordonnance est trop vaste, nous la refusons, et, si nécessaire, nous nous adressons aux tribunaux pour contester la demande[162].

Selon M. Engelhart, la catégorie qui suscite le plus d'intérêt est celle des demandes ayant trait à la vérification des noms et des adresses des clients[163]. M. Engelhart a affirmé à ce sujet que dans plusieurs cas, la police ne sait pas quel fournisseur de services cibler par sa demande de mandat, ce qui peut l'amener à demander à Rogers de vérifier si une personne demeurant à telle adresse ou possédant tel numéro de téléphone est un de ses clients[164]. Dans un tel cas, Rogers répond par oui ou par non, selon M. Engelhart[165].

Rogers considère que cette forme de collaboration avec la police est utile, parce que les renseignements qui sont communiqués à la police lui évitent de demander un mandat qui cible le mauvais fournisseur de services ou la mauvaise personne.

En ce qui concerne les métadonnées, M. Engelhart a confié que certaines agences américaines ont manifesté un grand intérêt pour en acquérir sans mandat de perquisition. M. Engelhart a tenu à assurer le Comité que son entreprise ne communique de métadonnées à aucun organisme canadien d'application de la loi sans mandat de perquisition, qu'elle ne l'a jamais fait et qu'elle ne le fera jamais[166].

Google

En ce qui concerne le rapport sur la transparence présenté par Rogers lors du témoignage de ses représentants devant le Comité, M. Colin McKay, de Google, a tenu à préciser que Google publie un rapport semblable tous les six mois sur son site Web[167]. Fait à noter, le rapport de Google sur les demandes de renseignements sur les utilisateurs

---

162 *Ibid*.

163 *Ibid*.

164 *Ibid*.

165 *Ibid*.

166 *Ibid*.

167 *Ibid*, 1115 (Colin McKay, chef, Politiques publiques et relations gouvernementales, Google inc.).

canadiens montre que Google a « partiellement accédé » à 33 % des demandes faites de janvier à juin 2014[168].

En s'appuyant sur l'exemple de mots de passe faciles à deviner, M. McKay a affirmé que l'expérience démontre que le maillon le plus faible de la chaîne en matière de sécurité de l'information est souvent l'utilisateur[169].

Selon M. McKay, Google élabore des systèmes et des outils pour alerter ses utilisateurs de tentatives d'atteinte à leur compte et à leur information, donne aux utilisateurs de l'information sur les sites qui pourraient tenter d'injecter des logiciels malveillants et prendre le contrôle de leur ordinateur et investit beaucoup d'efforts pour avoir les réseaux les plus sécuritaires au monde[170].

M. McKay a également insisté sur le bilan du système de courriel de Google, Gmail, en matière de protection des utilisateurs contre les pourriels[171]. Selon M. McKay,

> lorsqu'un polluposteur tente d'utiliser un nouveau type de pourriel, nos systèmes le détectent souvent et le bloquent des comptes Google en l'espace de quelques minutes, et si par hasard il apparaît dans votre boîte de réception, vous pouvez cliquer sur un bouton pour envoyer un signal à nos systèmes pour nous indiquer qu'à l'avenir, les messages semblables devraient être considérés comme des pourriels[172].

En ce qui concerne les résultats de recherche sur le site Web de Google, M. McKay a expliqué que les outils technologiques de son entreprise examinent des milliards d'adresses URL sur le Web, à la recherche de sites qui pourraient tenter d'injecter des codes malicieux dans les ordinateurs des utilisateurs, convaincre ces derniers de télécharger un logiciel contenant un virus, ou encore essaieraient de faire passer un site frauduleux pour un site financier légitime[173].

M. McKay a souligné le fait que chaque jour, Google détecte plus de 7 500 sites non sécuritaires et qu'elle envoie des avertissements à la suite de plus de 6 millions de résultats de recherche sur le site de Google et d'un million de téléchargements[174].

Selon M. McKay, plus d'un milliard d'utilisateurs sont protégés contre l'hameçonnage et les logiciels malveillants chaque jour par les avertissements envoyés

---

168 Google, Transparence des informations, Demandes de renseignements sur les utilisateurs, *Canada*. Le site de Google fournit une liste d'entreprises qui ont publié un rapport sur la transparence des informations qui inclut Rogers et TELUS.

169 ETHI, *Témoignages*, 2e session, 41e législature, 5 juin 2014, 1115 (McKay).

170 *Ibid*.

171 *Ibid*.

172 *Ibid*.

173 *Ibid*.

174 *Ibid*.

par Google relativement aux sites Web dangereux[175]. De plus, Google partagerait ces données avec d'autres navigateurs, comme Safari et Firefox[176].

M. McKay a mentionné qu'aux bureaux de Google en Californie, à New York, à Munich, à Zurich et à Montréal, une équipe de plus de 250 experts en génie de la sécurité travaillent dans le but de fournir à l'entreprise des services leur permettant de demeurer compétitifs en matière de sécurité de l'information[177].

M. McKay a rappelé au Comité qu'en 2011, Google avait lancé un processus de vérification en deux étapes, selon lequel l'utilisateur doit confirmer son identité au moyen d'un mot de passe en plus d'un autre code transmis à un téléphone ou à un dispositif USB distinct sur son ordinateur, par exemple[178]. Selon M. McKay ce processus de vérification en deux étapes ajoute un élément de sécurité supplémentaire pour l'ouverturedu'une session[179].

M. McKay a ajouté qu'en ce qui concerne les réseaux, Google a, depuis un an, élargi à l'ensemble de la séance de navigation le protocole de cryptage SSL (Secure Sockets Layer), pour qu'il s'ouvre par défaut à l'ouverture d'une session dans Gmail, Google Search, Google Docs et d'autres services[180]. Selon M. McKay, cette mesure de protection empêche les intrus de s'immiscer dans l'activité d'un utilisateur qui se situe dans un réseau ouvert[181].

M. McKay a également mentionné le fait que Google a crypté les données qui circulent entre ses différents centres de données, et que ses experts de la sécurité élargissent et renforcissent constamment cette protection pour englober plus de services et de liens[182].

M. McKay a ajouté que Google a dépensé près de 3 millions de dollars depuis quatre ans pour cerner les points faibles de ses programmes et de ses services sur le plan de la sécurité, ce qui entraine ensuite des ajustements pour résoudre les problèmes identifiés par les chercheurs en matière de sécurité[183].

Le Comité considère que le fait pour une entreprise des technologies de l'information de publier un rapport qui fait état des demandes provenant des organismes gouvernementaux portant sur la communication de renseignements personnels est une

---

175 *Ibid*.

176 *Ibid*.

177 *Ibid*.

178 *Ibid*, 1120.

179 *Ibid*.

180 *Ibid*.

181 *Ibid*.

182 *Ibid*.

183 *Ibid*.

pratique utile. Le Comité note que ce type de rapport est plus utile lorsqu'il contient de l'information concernant les instances où l'entreprise a effectivement répondu à ces demandes.

CRITIQUES DES MESURES PRISES PAR LES ENTREPRISES ET SUGGESTIONS D'AMÉLIORATIONS

A. Questions des membres du Comité aux agences d'évaluation du crédit

En réponse aux questions des membres du Comité portant sur le fait que les agences d'évaluation du crédit des consommateurs exigent des frais pour communiquer un dossier de crédit électroniquement, les représentants de ces agences ont expliqué leur pratique par les dépenses qui découlent du fait que la législation canadienne exige qu'elles gardent des bureaux ouverts aux consommateurs.

La propriété et les droits civils étant un pouvoir exclusif des provinces en vertu de la Constitution canadienne, ce qui inclut les relations contractuelles et la protection des consommateurs, plusieurs provinces ont adopté des lois qui visent les activités des agences d'évaluation du crédit des consommateurs. Certaines de ces lois provinciales exigent des agences de crédit qu'elles aient une place d'affaires ouverte au public dans leur province[184]. En ce qui a trait à la législation fédérale, la LPRPDE, dans la mesure où elle s'applique, impose certaines obligations à ces organisations concernant la protection des renseignements personnels.

M[me] Banfield, au nom de TransUnion, a insisté sur le fait que s'ajoute aux frais encourus par TransUnion l'investissement dans des technologies téléphoniques, comme les systèmes de réponse vocale interactive, qui permettent aux consommateurs de s'authentifier pour ensuite recevoir leur dossier de crédit par la poste[185]. M. Russo, au nom d'Equifax, a souligné qu'un consommateur peut avoir accès à son dossier de crédit chaque jour, 365 jours par année[186]. L'accès par un consommateur à son dossier de crédit est gratuit s'il demande de le recevoir par la poste; il lui en coûte cependant 15,50$ pour l'obtenir en ligne chez Equifax, par exemple[187].

Ces deux témoins ont expliqué davantage la pratique d'Equifax et de TransUnion d'imposer des frais aux consommateurs pour leur donner accès à leur dossier de crédit en faisant une comparaison avec la législation en vigueur aux États-Unis[188]. Dans ce pays, la *Fair and Accurate Credit Transactions Act of 2003* donne le droit aux consommateurs de consulter leur dossier de crédit gratuitement une fois par année, par un accès en ligne[189].

---

184 Par exemple, le paragraphe 4.2(1) de la *Consumer Reporting Act* de l'Île-du-Prince-Édouard prévoit que « Toute agence d'évaluation du crédit des consommateurs enregistrée en vertu de cette loi doit mener ses opérations à partir d'une place d'affaires établie à l'Île-du-Prince-Édouard qui doit être ouverte au public durant les heures d'affaires normales. » [TRADUCTION]

185 ETHI, *Témoignages*, 2e session, 41e législature, 27 mai 2014, 1130 (Banfield).

186 *Ibid* (Russo).

187 Equifax Canada, *Dossier de crédit Equifax*.

188 ETHI, *Témoignages*, 2e session, 41e législature, 27 mai 2014, 1130 (Banfield et Russo).

189 United States Government, *Fair and Accurate Credit Transactions Act of 2003*, article 211.

La pratique d'Equifax et de TransUnion s'expliquerait par le fait que la législation canadienne ne prévoit aucune obligation semblable et qu'elle impose à ces entreprises d'autres obligations qui entrainent des dépenses.

En réponse aux questions des membres du Comité sur les changements législatifs qui pourraient permettre aux agences d'évaluation du crédit de réduire leurs dépenses et d'offrir de l'information de façon électronique aux consommateurs, M[me] Banfield a répondu qu'elles le demandent chaque fois qu'il y a une réforme des lois sur les renseignements concernant les consommateurs dans les diverses provinces[190]. M. Russo a ajouté à cette réponse que ce ne sont pas seulement les lois provinciales qui imposent des obligations aux agences d'évaluation du crédit, mais également la LPRPDE, et que cette dernière devrait également être modifiée en conséquence[191].

Le Comité considère que ses questions aux agences d'évaluation du crédit des consommateurs concernant l'imposition de frais pour communiquer un dossier de crédit électroniquement n'ont pas trouvé de réponses satisfaisantes. Plus particulièrement, le Comité constate qu'il n'y a pas de lien de cause à effet entre la législation applicable à ces agences et leur décision d'imposer des frais aux consommateurs pour communiquer un dossier de crédit électroniquement. À la lumière de l'ensemble des témoignages reçus dans le cadre de son étude, le Comité est d'avis qu'un meilleur accès par les consommateurs à leur dossier de crédit contribuerait à réduire les crimes liés à l'identité.

Recommandation 1 : Le Comité exhorte les agences d'évaluation du crédit des consommateurs à fournir gratuitement aux consommateurs canadiens un accès électronique à leur dossier de crédit, au moins une fois par année.

B. Critiques des mesures prises par les entreprises et suggestions d'améliorations par des universitaires et des spécialistes

José Manuel Fernandez, professeur à l'École polytechnique de Montréal

M. José Manuel Fernandez, professeur à l'École polytechnique de Montréal, a utilisé l'exemple du bogue Heartbleed, qui avait touché les serveurs Web de l'Agence du revenu du Canada (ARC) et avait mené à la divulgation non autorisée d'au moins 900 numéros d'assurance sociale de contribuables canadiens, pour illustrer le risque réel en matière de vol d'identité que pose l'infrastructure de technologie de l'information (TI) en place au Canada[192]. Selon M. Fernandez, « l'histoire de Heartbleed, c'est celle de l'état

190 ETHI, *Témoignages*, 2e session, 41e législature, 27 mai 2014, 1150 (Banfield).

191 *Ibid* (Russo).

192 ETHI, *Témoignages*, 2e session, 41e législature, 29 avril 2014, 1100 (José Manuel Fernandez, professeur adjoint, Département de génie informatique et de génie logiciel, École polytechnique de Montréal, à titre personnel).

pitoyable de notre infrastructure de l'information et de la façon dont nous l'avons laissé se détériorer jusqu'à ce point[193]. »

M. Fernandez a expliqué que les numéros d'assurance sociale dévoilés risquaient d'être utilisés par des fraudeurs qui se feraient passer pour les victimes de ce vol d'identité et pourraient effectuer des transactions bancaires frauduleuses, détruire des antécédents en matière de crédit ou encore accéder sans autorisation à des comptes de courriel et de réseaux sociaux[194].

Cependant, M. Fernandez a affirmé que le vol d'identité n'est qu'un problème parmi tant d'autres, et même que c'est probablement un des problèmes les moins importants. Selon lui, le problème du vol d'identité n'est que la pointe visible de l'iceberg[195].

M. Fernandez considère plutôt que les problèmes les plus importants en matière de sécurité de données résident dans « la menace imminente que présentent le cybercrime, le cyberespionnage et le cybersabotage[196]. »

Selon M. Fernandez, « certains experts crédibles évaluent les coûts totaux reliés au cybercrime à plusieurs centaines de milliards de dollars par année[197]. » Il s'est appuyé sur une étude de la société spécialisée dans les logiciels informatiques Symantec pour évaluer les pertes liées au cybercrime à 3 milliards de dollars au Canada en 2013[198].

Pour illustrer le fait que le cybercrime se porte très bien, M. Fernandez a ajouté que

> [l]es cybercriminels utilisent des ordinateurs infectés dans les entreprises, les bureaux gouvernementaux et les domiciles d'usagers non avertis afin de générer un profit par divers moyens: fraude bancaire par Internet, le plus commun, mais aussi fraude publicitaire par Internet, extorsion et des formes traditionnelles de fraude et d'escroquerie[199].

Selon M. Fernandez, le cybercrime est une industrie en croissance avec des ramifications internationales et « qui met en jeu un réseau complexe de groupes criminels organisés qui travaillent ensemble[200]. » M. Fernandez a fait référence à des sondages publiés par l'Union européenne qui montrent qu'entre 30 et 35 % des utilisateurs sondés ont rapporté que leur ordinateur aurait été infecté au cours de la dernière année[201].

---

193 *Ibid*.

194 *Ibid*.

195 *Ibid*.

196 *Ibid*.

197 *Ibid*.

198 *Ibid*.

199 *Ibid*.

200 *Ibid*.

201 *Ibid*.

M. Fernandez a réalisé son propre essai clinique en 2012 à la Polytechnique auprès de 50 sujets utilisant chacun leur ordinateur personnel durant une période de quatre mois : 5 % des sujets ont été infectés par des logiciels malveillants dangereux et 20 % par des logiciels nuisibles, et ce, malgré l'installation d'un antivirus à jour dans chaque ordinateur[202]. L'analyse de M. Fernandez a démontré que « 38 % des usagers auraient été infectés par une forme de logiciel nuisible si aucun antivirus n'avait été installé[203]. » M. Fernandez en est venu à la conclusion que la contamination toucherait l'ordinateur de deux Canadiens sur cinq[204].

Selon M. Fernandez, les cybercriminels investissent leurs profits faramineux dans la recherche et le développement, ce qui leur permet de mettre au point des outils et des techniques de piratage qui bafouent les experts en sécurité informatique de l'industrie[205] :

> En fait, leurs investissements totaux en recherche et développement sont probablement plus importants que ceux de toute l'industrie de la sécurité informatique. Nous sommes donc en train de perdre la bataille. Il y a une course à l'armement. C'est un fait communément accepté, mais rarement admis en public: nous sommes effectivement en train de perdre la guerre contre les cybercriminels d'un point de vue technique[206].

M. Fernandez a d'ailleurs constaté que, de plus en plus, les banques commencent à ne pas payer lorsque leurs clients sont victimes de cybercrime[207].

Selon M. Fernandez, l'avantage technologique obtenu par les cybercriminels sert à d'autres fins, comme la pornographie juvénile, qui a mené à la mise sur pied d'équipes spécialisées au sein de la police[208]. Mais cet avantage technologique aurait également mené à la menace du cyberespionnage et du cybersabotage :

> Nous commençons à peine à découvrir à quel point des services de renseignement étrangers et des intérêts économiques étrangers se promènent sur les ordinateurs et serveurs du gouvernement canadien, des entreprises canadiennes et des citoyens canadiens depuis plus d'une décennie[209].

Les causes profondes du vol d'identité, du cyberespionnage et du cybersabotage sont toutes reliées à la façon dont l'infrastructure des TI est gérée, selon M. Fernandez. Il a argué que les technologies informatiques et Internet sont utilisés à des fins pour lesquelles ils n'ont jamais été conçus :

---

202 *Ibid*, 1105.

203 *Ibid*.

204 *Ibid*.

205 *Ibid*.

206 *Ibid*.

207 *Ibid*.

208 *Ibid*.

209 *Ibid*.

> Un cas d'espèce est le World Wide Web qui a été inventé par des chercheurs en Suisse afin d'avoir un moyen interactif d'échanger des données de recherche, mais 30 ans plus tard, il sert à l'économie mondiale. Là n'était pas le but[210].

M. Fernandez constate que les mécanismes de sécurité et de reddition de comptes appropriés n'ont pas été intégrés dans la conception de ces technologies[211]. Cependant, des solutions technologiques à ce problème ont été développées et elles sont enseignées dans les écoles de génie, selon M. Fernandez[212]. Ce seraient les incitatifs pour mettre en œuvre ces solutions technologiques qui seraient absents[213].

En somme, M. Fernandez a argué qu'une collaboration entre différents secteurs de la société, comme les associations professionnelles, les éducateurs, l'industrie, la fonction publique et les agences de maintien de l'ordre, serait nécessaire pour s'attaquer aux causes profondes des problèmes qu'il a identifiés, en plus de mesures législatives appropriées[214].

Susan Sproule, professeure à la Brock University

M[me] Susan Sproule, qui est professeure adjointe en matière de Finances, opération et systèmes d'information à la Brock University, a établi d'entrée de jeu qu'un des éléments clés à considérer dans la lutte au vol d'identité découle du fait que le vol d'identité et la fraude d'identité sont deux problèmes distincts[215]. M[me] Sproule a expliqué cette distinction ainsi :

> Le vol d'identité est un problème de responsabilité personnelle ou organisationnelle, c'est-à-dire qu'il faut veiller à la sécurité des renseignements personnels que l'on détient. Par contre, la fraude d'identité est un problème d'authentification, c'est-à-dire qu'il faut être en mesure de déterminer que la personne qui présente une pièce d'identité est vraiment celle qu'elle prétend être[216].

Selon M[me] Sproule, cette distinction est importante parce que ces deux crimes peuvent exister sans lien entre eux, le voleur d'identité et le fraudeur de pièce d'identité étant habituellement deux personnes différentes[217]. Qui plus est, elle a remarqué que les cas de vol d'identité, qui incluent les cas d'atteinte à la sécurité des données, sont

---

210 *Ibid*.

211 *Ibid*.

212 *Ibid*, 1110.

213 *Ibid*.

214 *Ibid*, 1115.

215 *Ibid*, 1120 (Susan Sproule, professeure adjointe, Finances, opération et systèmes d'information, Brock University, à titre personnel).

216 *Ibid*.

217 *Ibid*.

rarement liés aux cas de fraude d'identité parce que l'information doit passer par un intermédiaire[218].

Tout en rappelant la responsabilité de la personne qui est propriétaire de ses renseignements personnels qui consiste à garder en lieu sûr ses documents qui contiennent des renseignements liés à son identité et de ne pas divulguer inutilement ses renseignements personnels, elle a noté qu'il est impossible d'empêcher la fraude d'identité[219]. Selon elle, « [u]ne fois que mon information est compromise, la seule chose que je peux faire, c'est d'en prendre connaissance et de le signaler dès que possible[220]. »

M[me] Sproule a également rappelé la responsabilité qui incombe aux organisations, qui ont un rôle à jouer pour prévenir tant le vol d'identité que la fraude d'identité[221]. Selon elle, les organisations

> peuvent prévenir le vol d'identité en assurant la sécurité de tout renseignement personnel qu'elles possèdent. Elles peuvent empêcher la fraude d'identité en s'assurant qu'elles possèdent des processus d'authentification adéquats lorsqu'elles délivrent des pièces d'identité ou lorsqu'elles en font la vérification[222].

À ces obligations s'ajoutent celle de détecter le vol d'identité, lorsque des renseignements personnels ont été compromis, en plus de la fraude d'identité[223]. Une autre preuve que le vol et la fraude d'identité sont deux problèmes différents viendrait du fait que, dans les organisations, deux secteurs différents s'en occupent : les services de sécurité en matière de sécurité physique et les services de TI en matière de sécurité des systèmes[224].

M[me] Sproule a souligné que les nombreux défis provenant de la lutte au vol et à la fraude d'identité sont reliés au problème de la définition des termes utilisés : une grande partie de la population ne saurait pas de quoi il s'agit[225]. À ce manque de compréhension du problème chez les victimes potentielles s'ajoute celui du manque général d'information qui documenterait le problème[226]. Selon M[me] Sproule :

> Les fraudes par carte de débit et de crédit font l'objet d'enquêtes internes de la part des compagnies émettrices de cartes et des banques. Seule une petite partie de ces dossiers sont renvoyés à la police. Un sondage de Statistique Canada sur la fraude dans les

---

218 *Ibid*.

219 *Ibid*.

220 *Ibid*.

221 *Ibid*.

222 *Ibid*.

223 *Ibid*.

224 *Ibid*, 1125.

225 *Ibid*.

226 *Ibid*.

> entreprises de détail démontre qu'entre 40 et 50 % des dossiers n'ont jamais été signalés à la police. Moins de 40 % des victimes individuelles font rapport à la police[227].

Elle explique cette situation par la crainte de publicité négative des entreprises et la crainte des victimes que les gens sachent qu'ils n'ont pas protégé adéquatement leurs renseignements personnels[228]. Selon elle, dans les deux cas, ils estiment (non entièrement sans raison) que la police ne peut rien faire.

Le fait que les organisations assument la plupart des pertes financières liées au vol et à la fraude d'identité se traduit par deux problèmes, selon M[me] Sproule : leur réticence à divulguer ces coûts et le fait que ces coûts « ne constituent pas des incitatifs assez puissants pour empêcher le vol et la fraude d'identité[229]. » Elle a avancé que les pertes que subissent les organisations en raison de la fraude d'identité sont ensuite transmises aux consommateurs sous forme de prix, d'honoraires ou de tarifs plus élevés[230].

Par ailleurs, M[me] Sproule a argué que le manque d'exigences dans la législation canadienne concernant l'obligation de divulguer les atteintes à la sécurité des données fait en sorte que les organisations ne subiront pas nécessairement une atteinte à leur réputation en cas d'atteinte à la sécurité des données[231]. Elle voit d'ailleurs d'un bon œil le fait que le projet de loi S-4 propose des mesures dans cette direction[232].

En ce qui concerne les coûts généraux qu'entrainent le vol et la fraude d'identité pour la société, M[me] Sproule s'est appuyée sur différentes études démontrant qu'entre 20 et 40 % des consommateurs disent avoir rajusté leurs comportements en ligne par crainte de vol d'identité pour conclure que les entreprises canadiennes ne profitent pas de tous les avantages du commerce électronique[233].

M[me] Sproule a formulé deux recommandations à l'intention du Comité. La première concerne les agences d'évaluation du crédit, qui devraient être plus ouvertes aux interventions des consommateurs[234]. En effet, selon elle, pour que les consommateurs puissent contribuer à déceler les fraudes, ils doivent avoir un plus grand accès et un meilleur contrôle sur leurs dossiers de crédit[235]. Elle a résumé ainsi le problème de l'accès aux dossiers de crédit :

> Les agences d'évaluation du crédit doivent vous transmettre gratuitement, chaque année, une copie de votre dossier de crédit, mais elles rendent cette tâche très difficile.

---

227 *Ibid*.

228 *Ibid*.

229 *Ibid*.

230 *Ibid*.

231 *Ibid*.

232 *Ibid*.

233 *Ibid*.

234 *Ibid*.

235 *Ibid*.

> Pour obtenir un exemplaire gratuit, vous devez remplir un formulaire, copier une multitude de documents, envoyer le tout par la poste et attendre quelques semaines pour qu'on vous poste votre rapport. Les agences offrent aussi un service en ligne. Les services en ligne sont plus sécuritaires, et ils sont censés être moins coûteux pour les agences, mais elles facturent 24 $[236].

En ce qui concerne les produits de protection contre le vol d'identité, qui coûtent de 15 à 17 $ par mois, offerts par Equifax et TransUnion, M[me] Sproule fait le dur constat suivant : « [e]n offrant ces produits, ils profitent du problème, ce qui ne les motive que très peu à vouloir en réduire ou en éliminer les menaces[237]. »

La deuxième recommandation de M[me] Sproule concerne le besoin de collectes de données régulières et périodiques pour cerner les tendances en matière de vol et de fraude d'identité et pour mettre au point « des initiatives de sensibilisation efficaces et des politiques efficaces[238]. » Rejoignant d'autres témoins sur ce point, elle estime que l'absence de mesure pour le vol et la fraude d'identité entraine le besoin d'un indice du vol et de la fraude d'identité qui fonctionnerait comme un indice des prix à la consommation ou un indice sur les activités d'achat[239]. Selon M[me] Sproule :

> Cet indice serait calculé à partir de renseignements recueillis au moyen de sondages réguliers auprès des consommateurs, de sondages d'entreprises ainsi que de rapports des forces de l'ordre, des agences d'évaluation du crédit, des commissaires à la protection de la vie privée, des services aux victimes et de n'importe quel autre groupe[240].

Le Comité reconnait le bien-fondé des recommandations concernant les agences d'évaluation du crédit et la création d'un indice du vol et de la fraude d'identité.

Benoît Dupont, directeur du Centre international de criminologie comparée

Faisant écho au témoignage de M[me] Sproule, M. Dupont a rappelé le manque d'information concernant l'ampleur actuelle du problème, c'est-à-dire le nombre réel de victimes et l'évolution de cette tendance, l'absence de ventilation claire des types de vol d'identité, ainsi que l'absence de connaissance des voleurs d'identité[241].

Selon M. Dupont le manque d'information s'étend également à la connaissance que nous avons des organisations qui sont les plus efficaces dans la lutte au vol d'identité, de celles qui sont les plus exposées au risque et de celles qui ont du succès dans la prévention du vol d'identité[242].

---

236 *Ibid*.

237 *Ibid*, 1130.

238 *Ibid*.

239 *Ibid*.

240 *Ibid*.

241 *Ibid* (Benoît Dupont, directeur du Centre international de criminologie comparée).

242 *Ibid*, 1135.

En ce qui concerne plus particulièrement les banques, M. Dupont a noté qu'elles investissent des sommes importantes dans les technologies antifraude et qu'elles sont capables de détecter et de bloquer les tentatives de vol d'identité[243]. Malgré cela, le manque d'information concernant le vol d'identité fait en sorte que

> nous ne savons pas laquelle de ces cinq ou six grandes banques est la meilleure ou laquelle est la pire ni quels sont les types d'entreprises de détail ou de service qui sont à l'origine de la plus grande fuite de renseignements personnels vers les contrevenants[244].

M. Dupont a expliqué l'utilité qu'aurait l'information manquante : elle mènerait à la conception et à la mise en œuvre de stratégies de prévention plus efficaces qui « permettraient de cibler et de renforcer les maillons les plus faibles de l'écosystème des paiements[245]. » De plus, cette information permettrait d'en savoir davantage sur la nécessité de créer de nouveaux outils réglementaires qui forceraient les entreprises à protéger les renseignements personnels de leurs clients et de les aviser d'une atteinte, autant concernant les renseignements personnels que la sécurité[246]. Selon M. Dupont, l'information manquante aiderait également à assurer le caractère raisonnable de ces outils réglementaires afin qu'ils n'imposent pas un fardeau trop lourd aux entreprises[247]. Cette information aiderait également le Centre international de criminologie comparée et les organismes d'application de la loi à concentrer leurs efforts autour des réseaux criminels les plus dangereux et les plus prolifiques[248].

Sur une note plus positive, M. Dupont a souligné certaines mesures qui ont permis de réduire le nombre de vols et de fraudes d'identité au cours des dernières années au Canada, comme l'intégration de la technologie de la puce et du NIP sur les cartes de crédit et de débit et les progrès des technologies antifraude que le secteur bancaire a mises en place. Ces mesures démontrent, selon M. Dupont, que des changements au sein des organisations peuvent produire des résultats systémiques dans tout le pays[249]. Cependant, le problème en ce qui concerne la puce et le NIP réside dans le fait que les États-Unis ont été plus lents à adopter cette technologie, ce qui a permis aux contrevenants de recueillir des données inscrites sur les bandes magnétiques des cartes de crédit et de débit[250].

M. Dupont s'est appuyé sur les statistiques recueillies par Interac pour noter que les montants totaux de pertes attribuées à la fraude par Interac ont diminué de 36 % entre

---

243 *Ibid*.

244 *Ibid*.

245 *Ibid*.

246 *Ibid*.

247 *Ibid*.

248 *Ibid*.

249 *Ibid*.

250 *Ibid*.

2004 et 2012, alors que le nombre de transactions par carte de débit augmentait de 53 %[251]. La fraude serait donc en baisse et le nombre de transactions serait à la hausse.

M. Dupont a observé une tendance semblable concernant les cartes de crédit : les pertes totales ont augmenté de 94 % entre 1999 et 2012, alors que le montant total de transactions par carte de crédit augmentait de 212 %[252]. Il a également observé que la perte monétaire moyenne par transaction Interac s'élevait à environ 2 ¢ et que la perte monétaire ou financière moyenne des transactions par carte de crédit s'élevait à environ un sixième de 1 ¢[253]. Ces pertes n'ont pas varié de façon marquée au cours des 10 dernières années, ce qui tendrait à démontrer que le problème du vol d'identité n'est pas aussi grave que ce qu'en disent certaines entreprises, selon M Dupont[254].

Philippa Lawson, avocate associée à la Clinique d'intérêt public et de politique d'Internet du Canada de l'Université d'Ottawa

Comme ses collègues, M[me] Philippa Lawson, avocate associée à la Clinique d'intérêt public et de politique d'Internet du Canada de l'Université d'Ottawa, a reconnu qu'elle n'était pas en mesure de fournir au Comité des chiffres sur les crimes liés à l'identité ou aux renseignements personnels en raison du manque de données à cet égard[255].

M[me] Lawson a plutôt formulé cinq suggestions de réforme des politiques et des lois canadiennes concernées. Sa première suggestion est d'adopter une loi sur les avis à donner en cas d'atteinte à la sécurité des données[256]. Selon elle, le projet de loi S-4, qui contient des dispositions à cet effet, propose un mode de déclaration au commissaire à la vie privée dont les critères sont trop restrictifs[257]. La conséquence de ces dispositions serait de permettre aux entreprises d'« éviter de s'acquitter de leur responsabilité lorsque leurs mesures de sécurité sont insuffisantes[258]. »

La deuxième suggestion de M[me] Lawson porte sur la réforme de la LPRPDE, qui n'est pas prise au sérieux par les entreprises parce qu'elle manque de mordant, selon elle[259]. M[me] Lawson a noté qu'alors que la LPRPDE devrait protéger les

---

251 *Ibid*.

252 *Ibid*.

253 *Ibid*.

254 *Ibid*.

255 *Ibid*, 1140 (Philippa Lawson, avocate-procureure, associée, Clinique d'intérêt public et de politique d'internet du Canada, Université d'Ottawa, à titre personnel).

256 *Ibid*.

257 *Ibid*.

258 *Ibid*.

259 *Ibid*, 1145.

consommateurs contre les pratiques qui mènent au vol et à la fraude d'identité, les pratiques qui enfreignent la *Loi* sont encore répandues commercialement[260].

Elle a noté que le projet de loi S-4 permettrait au commissaire à la vie privée de dénoncer les entreprises délinquantes et de prendre des mesures contre celles qui ne respectent pas les accords de conformité ce qui représente des améliorations considérables par rapport à la situation actuelle[261]. M[me] Lawson a cependant argué que ces mesures n'étaient pas suffisantes pour rendre efficaces nos lois sur la protection des données numériques[262].

Troisièmement, M[me] Lawson a suggéré que la meilleure protection contre l'ouverture frauduleuse de compte était le gel du crédit, qui est une mesure empêchant les agences d'évaluation du crédit de divulguer le dossier de crédit d'un consommateur[263]. Selon elle, il s'agit d'une mesure particulièrement utile pour les personnes âgées ou celles qui n'ont pas besoin d'emprunter[264]. M[me] Lawson a expliqué que le gel de crédit n'est pas dans l'intérêt des agences d'évaluation du crédit, puisque le principal service qu'elles offrent est « l'évaluation » du crédit[265]. Elle a donné l'exemple des États-Unis, où presque tous les États américains exigent que le gel de crédit soit offert aux consommateurs, sans frais ou à très faible coût, afin de prévenir le vol d'identité[266].

Tout en soulignant que le domaine de la protection des consommateurs est de responsabilité provinciale, le gouvernement fédéral « […] devrait collaborer avec les provinces pour veiller à ce que les consommateurs canadiens disposent des outils nécessaires pour prévenir, déceler et atténuer les effets des vols d'identité, notamment par la capacité de demander le blocage de leurs dossiers de crédit », selon M[me] Lawson[267].

La quatrième suggestion de M[me] Lawson porte sur le besoin de coordonner les initiatives d'aide aux victimes. Elle a noté que malgré le fait que le Centre de soutien aux victimes de vol d'identité du Canada fournisse des données au Centre antifraude canadien, ce dernier ne reconnaît même pas l'existence du centre de soutien aux victimes[268]. Cet exemple illustre le besoin d'une

---

260 *Ibid*.

261 *Ibid*.

262 *Ibid*.

263 *Ibid*.

264 *Ibid*.

265 *Ibid*.

266 *Ibid*.

267 *Ibid*.

268 *Ibid*.

> meilleure coordination et collaboration entre ces organismes financés par les fonds publics, afin que chacun se concentre sur son mandat, plutôt que d'agir comme un rival de l'autre, pour obtenir l'attention du public et des fonds[269].

Enfin, selon M[me] Lawson, le Canada devrait adopter une stratégie nationale de lutte contre les crimes liés au vol d'identité pour mieux les comprendre et ainsi mieux lutter contre eux[270]. Cette stratégie devrait être confiée à de hauts fonctionnaires et intégrer la participation de tous les intervenants clés[271]. Abondant dans le même sens que M[me] Sproule et M. Dupont, M[me] Lawson a argué que le premier pilier d'une stratégie nationale devrait être la création de mécanismes de collecte de données fiables et complètes sur l'incidence, le type et le coût des crimes contre l'identité au Canada[272].

M[me] Lawson a suggéré que le Canada s'inspire des États-Unis, où un groupe de travail spécial avait été mis sur pied en 2006 pour élaborer une stratégie nationale de lutte contre le vol d'identité[273]. Les hauts responsables de tous les organismes gouvernementaux pertinents siégeaient sur ce groupe de travail, qui a examiné le problème sous tous ses angles et a publié un plan stratégique global de lutte contre le vol d'identité aux États-Unis[274]. Selon M[me] Lawson, ce plan, qui comprenait une coordination nationale des réformes en matière de politiques et de lois, a, en grande partie, été mis en œuvre[275]. Elle en conclut que les consommateurs et les victimes de vol d'identité aux États-Unis disposent maintenant de plus d'outils que les Canadiens pour prévenir ce crime et pour y réagir[276].

Éloïse Gratton, associée et vice-présidente, Conformité, McMillan LLP

M[me] Éloïse Gratton a elle aussi souligné que la LPRPDE ne contenait aucun incitatif pour que les organisations et les entreprises s'y conforment et qu'elles adoptent des mesures de sécurité adéquates[277]. Selon elle, le plus grand risque que courent les entreprises si elles ne se conforment pas à la *Lo*i est de voir leur réputation ternie[278]. Une entreprise court également le risque d'être condamnée par la Cour fédérale à payer des dommages-intérêts : il existe quelques décisions à cet égard au cours des 10 dernières années qui ont accordé de petits montants[279].

---

269 *Ibid*.

270 *Ibid*, 1150.

271 *Ibid*.

272 *Ibid*.

273 *Ibid*.

274 *Ibid*.

275 *Ibid*.

276 *Ibid*.

277 ETHI, *Témoignages*, 2[e] session, 41[e] législature, 1[er] mai 2014, 1145 (Éloïse Gratton, associée et vice-présidente, Conformité, McMillan LLP, à titre personnel).

278 *Ibid*.

279 *Ibid*.

M^me^ Gratton a également souligné l'absence au fédéral de l'incitatif qui peut découler des recours collectifs en matière d'atteinte à la vie privée, qui pourrait inciter les entreprises à se conformer à la *Loi*[280]. M^me^ Gratton a suggéré qu'une disposition comme l'article 26 de la *Loi concernant le cadre juridique des technologies de l'information* du Québec serait utile dans la LPRPDE[281]. Cette disposition impose une obligation additionnelle aux entreprises qui s'apprêtent à donner ou à transférer des renseignements à un tiers dans un contexte d'impartition.

M^me^ Gratton s'est appuyée sur certaines études, qui indiquent que la plupart des bris de sécurité sont causés par des erreurs humaines, pour constater que les entreprises ne prennent pas au sérieux la formation des employés en ce qui concerne les bris de sécurité[282]. En ce qui concerne l'obligation de faire état d'un bris de sécurité, M^me^ Gratton a souligné que cette obligation existe en Europe et aux États-Unis, où la plupart des États ont des lois à cet égard[283]. La seule province canadienne à prévoir une telle obligation est l'Alberta, où les amendes imposées aux entreprises peuvent aller jusqu'à 100 000$[284]. M^me^ Gratton a observé que

> l'inclusion de l'obligation de faire état d'un bris de sécurité dans la loi a entraîné une augmentation du nombre de signalements des infractions en matière de sécurité et aussi une augmentation de la formation offerte dans le domaine de la protection des renseignements personnels. Les entreprises sont davantage portées et motivées à dépenser, car elles savent qu'elles seront tenues de faire état d'un bris de sécurité, le cas échéant[285].

En ce qui concerne le projet de loi S-4, M^me^ Gratton considère que ce n'est pas parfait, mais que c'est mieux que rien parce que cela pourrait inciter les entreprises à signaler les incidents[286]. L'idéal, selon elle,

> serait de préciser les amendes qui seraient imposées pour tout manquement à l'obligation de signaler les bris de sécurité aux particuliers et aux commissaires à la protection de la vie privée. Il devrait être obligatoire de signaler un bris de sécurité dès que possible[287].

Selon M^me^ Gratton, le commissaire à la protection de la vie privée devrait pouvoir ordonner à une organisation de signaler un bris de sécurité à ses clients, ces ordonnances devraient être rendues publiques et l'entité devrait être nommée[288]. Ces circonstances créeraient un incitatif suffisant pour que les organisations investissent dans des mesures

---

280 *Ibid*.

281 *Ibid*, 1150.

282 *Ibid*.

283 *Ibid*, 1155.

284 *Ibid*.

285 *Ibid*.

286 *Ibid*.

287 *Ibid*.

288 *Ibid*.

de prévention, qui atténueraient à leur tour le préjudice financier découlant d'un vol d'identité[289].

M[me] Gratton a également suggéré que l'obligation de faire état d'un bris de sécurité pourrait être prévue dans une loi unique, qui pourrait s'inspirer de l'ébauche de loi sur les avis d'atteinte à la protection des données rédigée par la Conférence pour l'harmonisation des lois au Canada il y a quelques années[290].

Avner Levin, professeur agrégé à la Ryerson University

M. Avner Levin a concentré son témoignage autour du rôle des banques dans la lutte contre le vol d'identité[291]. Il a mentionné l'existence d'une étude qu'il a menée sur l'industrie des fournisseurs de services de regroupement[292]. Il s'agit d'une industrie qui rassemble l'information financière d'une variété de sources — carte de crédit, compte de chèques, compte d'épargne provenant tous de banques différentes — et la met à la disposition des clients qui peuvent la consulter sur leur ordinateur, leur tablette ou leur téléphone[293].

La recherche de M. Levin visait à cerner l'attitude des consommateurs à l'égard de ces services et des mesures de sécurité mises en place concernant l'information obtenue des clients, et à l'égard de la protection des renseignements personnels[294]. M. Levin et ses collègues cherchaient à discuter confidentiellement avec ces entreprises, sans les identifier, mais personne de l'industrie n'a accepté de leur parler parce que cela ne présentait aucun avantage[295]. Selon la lecture que fait M. Levin de la LPRPDE, ces entreprises devraient être en mesure de leur fournir cette information[296].

M. Levin a confié aux membres du Comité que, depuis plusieurs années, ses collègues et lui tentent sans succès d'obtenir de la part des banques de l'information sur le vol d'identité et les bris de sécurité liés au vol d'identité[297]. M. Levin a affirmé n'avoir reçu aucune réponse, des banques individuellement ou de l'ensemble des banques par l'intermédiaire de leur association, l'Association des banquiers canadiens (ABC)[298].

Selon M. Levin, les réponses aux questions qu'il souhaitait poser aux banques correspondraient précisément à ce qui pourrait aider le Comité dans ses travaux : comme

---

289 *Ibid*.

290 *Ibid*.

291 *Ibid*, 1200 (Avner Levin, professeur agrégé, Ryerson University, à titre personnel).

292 *Ibid*.

293 *Ibid*.

294 *Ibid*.

295 *Ibid*.

296 *Ibid*.

297 *Ibid*, 1205.

298 *Ibid*.

les sources de fraude, le pourcentage attribuable aux pratiques des consommateurs, le pourcentage des vols d'identité qui découlent du fait que les gens utilisent des mots de passe faciles ou qu'ils ne dissimulent pas leur NIP correctement, le pourcentage qui résulte de la négligence des gens qui gardent leur NIP en évidence[299].

En ce qui concerne les criminels, il cherchait à connaitre, notamment le pourcentage des vols d'identité qui est attribuable à des criminels qui placent des dispositifs sur les guichets automatiques pour voler les NIP des gens, de l'information sur les personnes qui utilisent des copieurs de carte sur des terminaux de point de vente pour voler des informations, le pourcentage de crimes lié à des petits criminels comparativement au crime organisé, le pourcentage qui résulte d'activités d'employés malhonnêtes, le pourcentage lié à des pays étrangers d'où proviennent beaucoup d'activités criminelles[300]. M. Levin considère que sans ces informations, le gouvernement et le Parlement ne seront pas en mesure de mettre en place des politiques adéquates à l'égard du vol d'identité[301].

M. Levin a constaté que les données publiées les plus récentes qui sont disponibles, datant de 2012 sur le site de l'ABC et du milieu de 2013 par le Centre antifraude du Canada, sont des données globales qui n'offrent pas de ventilation par catégorie, donc ne donnent aucune indication qui permettrait d'établir une stratégie adéquate pour l'avenir[302].

Selon M. Levin, les banques ont un rôle clé à jouer dans la lutte contre le vol d'identité; elles doivent faire preuve de transparence et elles doivent rendre des comptes[303]. Il a argué que le fait de régler le problème du vol d'identité fait partie de la « responsabilité d'entreprise » des banques en tant que groupe[304].

M. Levin a finalement exhorté le Comité à demander aux banques de communiquer au public et aux universitaires les renseignements demandés, ou à tout le moins aux membres du Comité pour qu'ils aient devant eux les renseignements nécessaires pour accomplir le travail important qu'ils ont entrepris[305].

Le 31 mars 2015, M. Levin a fait parvenir au Comité un mémoire portant sur le manque d'information publique sur le vol d'identité. Il note dans ce mémoire que la comparution des représentants des banques devant le Comité a démontré que ces dernières n'ont pas adopté la même définition du vol d'identité, ce qui expliquerait qu'elles n'enregistrent ni ne compilent de données globales sur le vol d'identité.

---

299 *Ibid*.

300 *Ibid*.

301 *Ibid*.

302 *Ibid*.

303 *Ibid*.

304 *Ibid*.

305 *Ibid*.

Dans son mémoire, M. Levin fait également une comparaison avec la situation aux États-Unis, où plusieurs États obligent les banques à divulguer les vols d'identité et les atteintes à la sécurité des données. Il cite par ailleurs certains médias, qui ont rapporté au début de 2015 des vols d'identité commis dans des banques canadiennes. Selon M. Levin, les incidents rapportés « montrent l'importance de l'information publique pour l'élaboration de politiques, de même que la faiblesse des allégations faites par les banques devant le Comité, selon lesquelles le vol d'identité se produit en grande partie à l'extérieur de l'environnement bancaire[306]. »

Selon M. Levin, les incidents rapportés ne sont pas isolés : une attaque de grande ampleur commise à l'encontre de plus d'une centaine de banques situées dans plus de 30 pays, incluant le Canada, a également été rapportée par les médias. Les pertes cumulées de cette attaque s'élèveraient à 1 milliard de dollars. M. Levin estime que si le public était plus informé sur ce genre d'incident, et sur les vecteurs d'attaque utilisés, « il serait plus facile de combattre le vol d'identité et de déterminer les menaces les plus sérieuses auxquelles les banques et leurs clients devraient porter attention[307]. »

Enfin, le mémoire de M. Levin présente trois recommandations portant sur le secteur bancaire, que le Comité fait siennes et qui se retrouvent ci-dessous.

À la lumière de l'ensemble des témoignages, et particulièrement de celui de M. Levin, le Comité fait les recommandations suivantes à l'égard du secteur bancaire :

> **Recommandation 2 : Le Comité exhorte les banques canadiennes à adopter, comme définition commune du vol d'identité, la définition qui se trouve dans le *Code criminel* en vigueur au Canada et à compiler des données sur le vol d'identité en conséquence.**
>
> **Recommandation 3 : Le Comité exhorte les banques canadiennes à rendre publique l'information qu'elles détiennent sur le vol d'identité. L'information publiée devrait, notamment porter à la fois sur les tentatives réussies et ratées de voler des renseignements personnels et devrait indiquer la source de l'attaque.**
>
> **Recommandation 4 : Le Comité invite les banques canadiennes à investir dans des dispositifs technologiques afin de protéger les données de leurs clients. Ces dispositifs devraient, notamment comprendre des systèmes de vérification enregistrant le nombre et les types d'accès aux dossiers des clients.**

306 Avner Levin, « Le manque d'information publique sur le vol d'identité », 31 mars 2015.

307 *Ibid*.

CRITIQUES DES MESURES PRISES PAR LES ENTREPRISES ET SUGGESTIONS D'AMÉLIORATIONS PAR DES ORGANISATIONS DE PROTECTION DU CONSOMMATEUR, DES ORGANISATIONS DE DROIT DES VICTIMES ET DES ORGANISATIONS NON GOUVERNEMENTALES

A. Centre de soutien aux victimes de vol d'identité du Canada

Le Centre de soutien aux victimes de vol d'identité du Canada est une organisation sans but lucratif qui fournit un numéro sans frais, un soutien étape par étape en direct et des ressources en ligne pour aider les victimes de vol d'identité à faire face aux conséquences potentielles de ce crime[308]. Le Centre de soutien aux victimes de vol d'identité du Canada offre aussi des renseignements sur la prévention des crimes reliés à l'identité et fournit des conseils sur les mesures à prendre pour réduire le risque de vol d'identité.

M. Kevin Scott, président et fondateur du Centre de soutien aux victimes de vol d'identité du Canada, a voulu présenter au Comité le point de vue des victimes[309]. M. Scott a décrit aux membres du Comité la confusion que vit une personne qui est victime de vol d'identité : « [e]lle ne sait pas à qui s'adresser, elle ne sait pas quoi faire et elle ne sait pas comment sortir du labyrinthe[310]. »

Pour reprendre le contrôle de la situation après un vol d'identité, une personne doit communiquer avec 15 à 20 organismes, qui exigent chacun une procédure et des renseignements différents pour régler le problème[311]. Ces exigences, ajoutées aux conséquences émotionnelles du vol d'identité, font en sorte qu'une personne vit une période de confusion d'environ 400 heures, selon M. Scott[312].

Ces données proviennent de l'Identity Theft Resource Center de San Diego, avec lequel le Centre de soutien aux victimes de vol d'identité du Canada collabore depuis sa mise sur pied[313]. Selon M. Scott, cette organisation a réussi à simplifier le processus pour que la période de confusion de la victime de vol d'identité passe de 400 heures à 15 à 20 heures en plus de « créer une boîte à outils très systématique contenant des

---

308 Centre de soutien aux victimes de vol d'identité du Canada, « Communiqués de presse », *Média*.

309 ETHI, *Témoignages*, 2e session, 41e législature, 3 juin 2014, 1215 (Kevin Scott, président, Centre de soutien aux victimes de vol d'identité du Canada).

310 *Ibid*, 1220.

311 *Ibid*.

312 *Ibid*.

313 *Ibid*, 1215.

formulaires, des textes et d'autres documents, dans le but, essentiellement, de sortir la personne de ce bourbier[314]. »

M. James Dorey, directeur principal du Centre de soutien aux victimes de vol d'identité du Canada, a expliqué que son organisation travaille sur trois grands volets : le soutien aux victimes, l'éducation et la prévention, la recherche et la collecte de données[315].

Le volet de soutien aux victimes a, notamment donné lieu à la publication de feuillets d'information pour aider les victimes de vol d'identité et à une boîte à outils appelée « Victim Toolkit », qui réunit une série de formulaires en un livret et dont l'objectif est d'accompagner une personne du début à la fin du processus afin de lui permettre de rétablir son identité[316]. M. Dorey a précisé que ces ressources sont disponibles sur le site Web de l'organisme. Le Centre a également établi un numéro sans frais et un centre d'appels, où les gens peuvent parler à une autre personne à l'autre bout du fil[317].

M. Dorey a expliqué au Comité que le Centre avait établi certains partenariats avec d'autres organisations canadiennes, dont Equifax pour les cas où l'évaluation de crédit d'une victime est en cause[318].

En ce qui concerne le volet d'éducation et de prévention, M. Dorey a souligné que son organisme avait, notamment créé quatre manuels différents, qui se trouvent sur leur site Web: pour les jeunes, pour les personnes âgées, pour le grand public et un dernier adapté aux situations en ligne[319]. Il a ajouté que le Centre est en train de mettre sur pied un nouveau programme d'éducation et de sensibilisation axé sur deux groupes démographiques qui sont de plus en plus touchés par le vol d'identité : les jeunes et les personnes âgées[320].

Enfin, M. Scott a observé que le vol d'identité affecte actuellement plus de 100 000 personnes au Canada[321]. M. Scott a également formulé les trois recommandations suivantes à l'intention du Comité :

---

314 *Ibid*, 1220.

315 *Ibid*, 1225 (James Dorey, directeur principal, Centre de soutien aux victimes de vol d'identité du Canada).

316 *Ibid*.

317 *Ibid*.

318 *Ibid*.

319 *Ibid*.

320 *Ibid*.

321 *Ibid*, 1230 (Scott).

> [U]ne augmentation du soutien offert aux victimes par le gouvernement et le secteur privé, un accroissement de l'éducation et de la sensibilisation, ainsi que l'élaboration d'un indice national de ce qui se passe au chapitre du vol d'identité[322].

Le Comité prend acte des recommandations du Centre de soutien aux victimes de vol d'identité du Canada et tient compte du point de vue des victimes de vol d'identité dans son évaluation de l'ensemble des témoignages qu'il a entendus et dans la formulation des recommandations qui en découlent.

B. Clinique d'intérêt public et de politique d'Internet du Canada Samuelson-Glushko

La Clinique d'intérêt public et de politique d'Internet du Canada Samuelson-Glushko (CIPPIC) est basée au Centre de recherche en droit, technologie et société dans la Section de common law de la Faculté de droit de l'Université d'Ottawa[323]. Le mandat de la CIPPIC est de promouvoir diverses questions touchant à la fois au droit et à la technologie, et ce, dans l'intérêt public.

En 2007, la CIPPIC a produit plusieurs publications concernant le vol d'identité[324], dont un document intitulé *Identity Theft: Introduction and Background*[325]. Ce document fournit de l'information sur l'histoire, les caractéristiques, les causes et l'étendue du vol d'identité. Il aborde également les défis que représentent la définition du « vol d'identité » et la façon de mesurer son importance et ses conséquences. Enfin, ce document identifie les parties prenantes qui sont incontournables dans l'étude de ce problème et analyse l'impact de la technologie, incluant l'utilisation généralisée d'Internet, sur le vol d'identité.

M. Tamir Israel, au nom de la Clinique d'intérêt public et de politique d'Internet du Canada Samuelson-Glushko[326], a présenté le vol d'identité comme « le crime de l'ère de l'information[327]. » M. Israel a expliqué comment l'information recueillie et classée par le Consumer Sentinel Network de la Federal Trade Commission des États-Unis a démontré que les plaintes liées au vol d'identité constituaient la principale catégorie parmi plus de 2 millions de plaintes de consommateurs en 2013[328]. M. Israel a également expliqué qu'étant donné que le vol d'identité est un véhicule pour d'autres crimes liés à l'identité,

---

322 *Ibid*.

323 Clinique d'intérêt public et de politique d'Internet du Canada Samuelson-Glushko (CIPPIC), *À propos de la clinique*.

324 CIPPIC, « Project Publications », *Privacy, Identity Theft* [DISPONIBLE EN ANGLAIS SEULEMENT].

325 CIPPIC, *Identity Theft: Introduction and Background*, CIPPIC Working Paper No. 1 (ID Theft Series), mars 2007, Ottawa, 21 pages [DISPONIBLE EN ANGLAIS SEULEMENT].

326 ETHI, *Témoignages*, 2e session, 41e législature, 3 juin 2014, 1230 (Tamir Israel, avocat, Clinique d'intérêt public et de politique d'Internet du Canada Samuelson-Glushko).

327 *Ibid*.

328 *Ibid*.

comme la création de fausses identités qui elles-mêmes servent de tremplin vers d'autres, ses coûts économiques et sociaux sont difficiles à mesurer[329].

Selon M. Israel, les méthodes des voleurs d'identité s'adaptent aux nouvelles technologies en tirant avantage de tous les renseignements disponibles sur les médias sociaux et les appareils mobiles[330]. Des marchés d'identités illégaux seraient accessibles sur Internet, où l'achat et la vente en masse d'un accès à des comptes de courriel, des numéros de carte de crédit ou des profils d'identité complets seraient possibles[331]. Il a cité les chiffres d'une étude de l'Organisation pour la coopération et le développement économique en 2009, qui estime qu'on peut acheter des listes d'adresses de courriel valides à des prix allant de 1,70 $ US à 15 $ US par mégaoctet, et un accès à des comptes de courriel compromis à des prix allant de 1 $ US à 20 $ US, selon les fluctuations du marché noir[332].

Par ailleurs, M. Israel a souligné le fait que le temps, l'effort et le traumatisme que suppose le rétablissement d'un vol d'identité ne sont pas faciles à mesurer d'un point de vue économique[333].

Il a identifié trois éléments qui sont, selon lui, nécessaires à toute intervention qui s'attaque au problème du vol d'identité : la prévention, la recherche et l'éducation, et le soutien aux victimes. Un autre élément essentiel serait celui des enquêtes et de l'application de la loi[334].

À ce chapitre, M. Israel considère que plusieurs mesures prises au cours des dernières années ont eu pour effet d'améliorer la capacité de différents organismes canadiens d'enquêter sur les crimes liés à l'identité et de lutter contre des infractions qui facilitent ces crimes[335]. Font partie de ces organismes le Commissariat à la protection de la vie privée du Canada, le Bureau de la concurrence et les organismes d'application de la loi[336].

Malgré ces mesures, notamment l'ajout de dispositions au *Code criminel* et l'adoption de la *Loi canadienne anti-pourriels*, il est important selon M. Israel de « reconnaître que le vol d'identité est là pour rester et qu'une solution associée à l'application de la loi ne sera pas suffisante, à elle seule, pour régler le problème[337]. »

---

329 *Ibid*.

330 *Ibid*.

331 *Ibid*.

332 *Ibid*.

333 *Ibid*.

334 *Ibid*.

335 *Ibid*.

336 *Ibid*.

337 *Ibid*.

M. Israel considère que la protection des renseignements personnels doit être renforcée pour ne pas que ces renseignements se retrouvent entre les mains des voleurs d'identité et que cela passe nécessairement par un renforcement des cadres de protection des données, ce qui comprend un renforcement de la LPRPDE et de la *Loi sur la protection des renseignements personnels* à cet égard[338].

En ce qui concerne la LPRPDE, M. Israel a argué qu'elle doit être au centre de la lutte au vol d'identité[339]. Du point de vue de M. Israel, les réseaux sociaux et les appareils mobiles constituent un répertoire de renseignements qui sont souvent communiqués de façons inattendues au public en général ou aux applications invisibles de tiers[340]. À propos des atteintes à la sécurité des données, il a ajouté que

> [l]a LPRPDE oblige également les organisations à mettre en place des mesures techniques et d'autres mesures de sécurité afin de prévenir l'accès non autorisé aux données des consommateurs. Non seulement les atteintes à la sécurité gagnent en fréquence chaque année, mais le nombre d'identités exposées par chaque atteinte augmente de façon spectaculaire[341].

M. Israel s'est appuyé sur le rapport *Internet Security Threat Report* publiée en 2014 par Symantec pour souligner qu' « une augmentation annuelle de 260% avait été enregistrée relativement au nombre d'identités exposées par chaque atteinte, ce qui signifie qu'il s'agit essentiellement de cyberatteintes ciblant de vastes répertoires de données d'un seul coup[342]. » La conclusion à tirer de ces données consisterait à souligner l'importance de l'adoption de fortes mesures de sécurité techniques pour prévenir le vol d'identité[343].

Le portrait que brosse M. Israel de la situation fait ressortir le besoin que la LPRPDE régisse un cadre juridique qui soit rigoureusement appliqué, alors que le cadre actuel ne reflèterait pas ce besoin[344]. Il a cité à l'appui de ses arguments le rapport du Comité intitulé *Protection de la vie privée et médias sociaux à l'ère des mégadonnées* et l'ancienne commissaire à la protection de la vie privée du Canada, Jennifer Stoddart, pour affirmer que

> l'émergence de géants Internet menace l'équilibre recherché par l'esprit et la lettre de la LPRPDE, et le risque d'atteintes importantes et d'utilisation inattendue, non souhaitée, voire même intrusive, des renseignements des gens exige la prise de mesures de protection correspondant aux conséquences financières qui ne sont actuellement pas prévues dans la LPRPDE.

---

338 *Ibid*.

339 *Ibid*.

340 *Ibid*.

341 *Ibid*.

342 *Ibid*.

343 *Ibid*.

344 *Ibid*.

En ce qui concerne le projet de loi S-4, M. Israel considère qu'il rendra la LPRPDE un peu plus facile à faire appliquer en prévoyant des ordonnances de consentement facultatives[345]. Il a cependant fait remarquer que pour inciter efficacement les entreprises à s'acquitter de façon proactive de leurs obligations en vertu de la LPRPDE, il faudra conférer les pleins pouvoirs et prévoir des pénalités pécuniaires administratives pour les cas de non-conformité[346]. Quant aux dispositions du projet de loi S-4 concernant la notification des atteintes, M. Israel a noté qu'elles étaient attendues « depuis déjà bien longtemps[347] ». Selon lui,

> [m]ême si l'obligation de notification relative aux infractions prévues dans le projet de loi S-4 est un bon pas en avant, elle n'est pas suffisamment calibrée pour prévenir les atteintes à la sécurité. Elle est trop ciblée sur le risque de préjudice direct pour un utilisateur final découlant d'une atteinte particulière. En réalité, dans de nombreux cas, il sera difficile de savoir si une vulnérabilité particulière a été exploitée ou non, ce qui signifie que la majorité des cas de laxisme au chapitre des mesures de sécurité techniques ne seront pas signalés. Ainsi, ce mécanisme ne sera pas efficace pour encourager et motiver les entreprises à renforcer leurs mesures de sécurité techniques[348].

Par ailleurs, M. Israel a cité des cas d'atteintes récents dans des ministères qui ont également été très médiatisés, comme la perte à RHDCC d'un disque dur contenant des renseignements personnels reliés à plus de 500 000 demandes de prêt étudiant, pour illustrer qu'il manque à la *Loi sur la protection des renseignements personnels* non seulement une obligation de notification des atteintes, mais également une « obligation de base d'adopter des mesures de sécurité techniques[349]. »

M. Israel a argué que pour s'attaquer efficacement au problème du vol d'identité, il faut non seulement de la prévention, mais aussi de l'éducation et de la sensibilisation[350]. Il a noté que certains organismes gouvernementaux ont publié à l'intention des consommateurs des documents d'information bien faits qui portent sur le vol d'identité. À cet égard, il a cité avec approbation le document intitulé *Le petit livre noir de la fraude* du Bureau de la concurrence, qui est accessible en ligne[351]. Il a également souligné les efforts louables déployés par des organismes non gouvernementaux, comme le Centre de soutien aux victimes de vol d'identité du Canada et sa « Victim Toolkit »[352]. Cependant, ces efforts ne sont pas suffisants selon M. Israel, particulièrement en ce qui concerne « la sensibilisation à l'égard du processus de rétablissement des victimes[353]. »

---

345 *Ibid*, 1235.

346 *Ibid*.

347 *Ibid*.

348 *Ibid*.

349 *Ibid*.

350 *Ibid*.

351 *Ibid*.

352 *Ibid*.

353 *Ibid*.

M. Israel a également identifié le besoin d'une recherche coordonnée et soutenue sur la portée et les paramètres du vol d'identité[354]. Selon lui, trop peu de recherches systématiques ont été menées sur ce sujet au Canada depuis 2006[355]. Certaines initiatives étrangères abordent la question de la portée et des paramètres du vol d'identité au Canada, mais il doit se faire plus de recherches au Canada en cette matière. Un répertoire des atteintes, tel que mentionné par les représentants du Centre de soutien aux victimes de vol d'identité du Canada lors de leur témoignage, serait utile à cet égard[356].

En ce qui concerne le processus de rétablissement à la suite d'un vol d'identité, M. Israel a souligné qu'il était extrêmement complexe, les victimes devant faire face à « des créanciers qui sont réticents à croire que leur dette n'est pas la leur[357]. » Il a également souligné qu'une mauvaise cote de crédit peut suivre les victimes de vol d'identité pendant des années[358].

M. Israel a souligné l'utilité du type de documents normalisés qui sont fournis par des organismes comme le Centre de soutien aux victimes de vol d'identité du Canada, pour naviguer à travers toutes les contraintes qu'impose le rétablissement à la suite d'un vol d'identité[359]. Selon lui, il est également essentiel de s'assurer que ces documents normalisés soient acceptés par les organismes d'application de la loi et par les fournisseurs de services[360]. Il a aussi mentionné l'offre de gels de crédit sans frais et l'accès en ligne à des rapports de crédit comme d'autres outils utiles et nécessaires au rétablissement à la suite d'un vol d'identité[361]. Selon M. Israel, « l'accessibilité constante d'un centre de soutien aux victimes est essentielle au processus de rétablissement dans son ensemble[362]. »

En somme, il a recommandé d'adopter une stratégie nationale de soutien aux victimes de vol d'identité qui établirait clairement les paramètres d'une collaboration entre les organismes qui viennent en aide aux victimes, comme le Centre antifraude du Canada, le Centre de soutien aux victimes de vol d'identité du Canada et les organismes de réglementation qui s'attaquent au vol d'identité[363]. Cette stratégie nationale de soutien aux

354 *Ibid*.

355 *Ibid*.

356 *Ibid*.

357 *Ibid*.

358 *Ibid*.

359 *Ibid*.

360 *Ibid*.

361 *Ibid*.

362 *Ibid*.

363 *Ibid*.

victimes de vol d'identité établirait également une feuille de route claire pour l'adoption des mécanismes de rétablissement de l'identité qui ont été mentionnés[364].

Le Comité considère qu'une stratégie nationale de soutien aux victimes de vol d'identité permettrait de coordonner les efforts en matière de lutte au vol d'identité afin de contrer ce crime plus efficacement.

> **Recommandation 5 : Le Comité recommande que le gouvernement du Canada cherche à obtenir l'appui des provinces et territoires en considérant l'établissement d'une stratégie nationale afin de coordonner les efforts en matière de lutte au vol d'identité et de contrer ce crime plus efficacement.**

C. Crime Prevention Association of Toronto

M^me^ Janet Sherbanowski, directrice générale de la Crime Prevention Association of Toronto, a expliqué que son organisme collabore, notamment avec le Bureau de la concurrence et la Commission de services policiers de Toronto sur la fraude et des questions connexes[365].

Elle a expliqué que son organisme tient des ateliers sur la fraude en matière de crédit et la fraude d'identité destinés aux nouveaux immigrants et aux aînés dans le cadre du programme Nouveaux Horizons pour les aînés[366]. La Crime Prevention Association of Toronto collabore également avec la banque RBC et la Banque Scotia, qui ont parrainé son programme « ABCs of Fraud » jusqu'en 2011[367].

M^me^ Sherbanowski a noté que son association a collaboré avec le commissaire à la protection de la vie privée de l'Ontario pour déterminer l'information à fournir aux consommateurs sur la protection de leur identité et la façon de leur signaler le risque posé par les mégadonnées et la façon dont elles sont extraites par les entreprises et possiblement par le gouvernement[368].

Selon M^me^ Sherbanowski, les consommateurs devraient être prévenus « lorsque des institutions financières ne déclarent pas les atteintes à la protection des renseignements ou les vols de données sur les cartes de crédit ou de débit[369]. » Le fait que ces actes ne soient pas déclarés nuirait à l'augmentation des services de surveillance

---

364 *Ibid*.

365 ETHI, *Témoignages*, 2^e^ session, 41^e^ législature, 23 février 2015, 1530 (Janet Sherbanowski, directrice générale, Crime Prevention Association of Toronto).

366 *Ibid*.

367 *Ibid*.

368 *Ibid*, 1535.

369 *Ibid*.

de son association et possiblement à l'embauche d'un plus grand nombre de policiers ou de fonctionnaires qui s'attaquent à ces problèmes[370].

D. Claudiu Popa, président-directeur général d'Informatica Corporation, à titre personnel

M. Claudiu Popa a expliqué que son entreprise offre des conseils sur la sécurité et la confidentialité à travers le Canada[371]. Selon les recherches effectuées par l'entreprise de M. Popa, le problème du vol d'identité non seulement prend de l'ampleur, mais se transforme, et de nouvelles façons de commettre ce crime se manifestent partout dans le monde chaque année[372].

Il a cité les études publiées par les entreprises Intel et McAfee dans un rapport sur la cybercriminalité dans le monde en 2014, qui indiquent que la cybercriminalité entraîne des pertes pouvant atteindre 575 milliards de dollars, dont la plupart résulte de la compromission de milliards de dossiers individuels[373]. Il s'agit donc d'un phénomène mondial, selon M. Popa.

M. Popa a également cité la FEC, le FBI et des sources canadiennes selon lesquelles il faudrait au moins six mois et 200 heures pour rétablir une identité après qu'il y ait eu une atteinte aux renseignements personnels[374].

M. Popa a expliqué que l'hameçonnage ciblé, qui consiste à utiliser tout type de renseignements qu'on peut obtenir des victimes, est l'une des pratiques les plus utilisées pour s'en prendre à des organisations, accéder à des ordinateurs personnels ou installer des logiciels sans autorisation, par exemple[375]. Il a également souligné la difficulté inhérente à l'adoption de mesures législatives qui empêcheraient les entreprises qui s'adonnent à ce genre d'activités « d'obtenir des renseignements personnels, d'en faire un usage abusif, de les revendre et de participer au cycle de cybercriminalité[376]. »

Sans pouvoir fournir de chiffres précis à cet égard, comme c'est le cas pour la cybercriminalité selon lui, M. Popa a constaté que le vol de renseignements personnels est très répandu dans le monde et qu'il entretient certains liens avec des activités comme la traite de personnes et le financement du terrorisme[377].

---

370 *Ibid*.

371 *Ibid,* 1540 (Claudiu Popa, président-directeur général, Informatica Corporation, à titre personnel).

372 *Ibid*.

373 *Ibid*.

374 *Ibid*.

375 *Ibid*, 1545.

376 *Ibid*.

377 *Ibid*.

M. Popa a également constaté une utilisation inefficace des services de courtage de crédit, en réaction primaire aux atteintes. D'après lui, le fait qu'une organisation victime d'une atteinte majeure offre gratuitement à toutes les victimes la surveillance crédit et de leur identité est insuffisant[378]. En ce qui concerne une organisation qui se trouve dans cette situation,

> [s]ouvent, ses propres pratiques ne se conforment pas aux pratiques exemplaires normales de protection de l'identité ou de protection contre l'hameçonnage. La création de certains des outils qu'elle offre n'emploie pas de pratiques sûres. Dans la pratique, les contrôles sont très faibles, et il faudrait revoir la normalisation de ces sauvegardes[379].

Selon M. Popa, il faut sévir plus rigoureusement contre la complicité dans la cyberfraude, tout en faisant preuve de clémence pour les individus qui croient pouvoir s'enrichir en faisant un emploi honnête et qui ne sont pas membres du crime organisé[380].

En ce qui concerne le vol et la fraude d'identité synthétique, M. Popa considère qu'ils pourront être cernés par l'analyse des mégadonnées[381]. Par ailleurs, la collaboration des banques et des sociétés d'assurance est nécessaire selon lui pour être en mesure de reconnaître les tendances du risque et construire des modèles qui permettent de trouver les responsables[382].

---

378 *Ibid*, 1550.

379 *Ibid*.

380 *Ibid*.

381 *Ibid*.

382 *Ibid*.

MESURES PRISES PAR LES INSTITUTIONS GOUVERNEMENTALES POUR PROTÉGER LES CANADIENS CONTRE LE VOL D'IDENTITÉ

Dans le cadre de l'étude, plusieurs ministères et organismes gouvernementaux ont comparu devant le Comité afin de discuter des programmes actuellement en place pour protéger les Canadiens contre le vol d'identité et pour prévenir la fraude d'identité. Leurs témoignages ont convaincu le Comité de l'efficacité d'une collaboration constructive entre les différents acteurs des secteurs public et privé. Une telle collaboration — qui vise essentiellement à sensibiliser les citoyens aux risques liés à la communication de leurs renseignements personnels et aux mesures à prendre s'ils sont victimes d'un vol d'identité — est indispensable pour atténuer les incidences économiques du vol d'identité. La section qui suit résume ces témoignages et présente les observations du Comité en ce qui concerne l'efficacité des efforts entrepris et les aspects — comme la collecte des données et la communication des renseignements — qui, de l'avis du Comité, méritent d'être améliorés.

A. Centre antifraude du Canada

Le Centre antifraude du Canada (CAFC) est le fruit d'un partenariat entre la Gendarmerie royale du Canada (GRC), le Bureau de la concurrence et la Police provinciale de l'Ontario. Le CAFC sert de dépôt central de données relatives à la fraude qui fonctionne selon un processus de « soutien entre pairs » permettant aux victimes de signaler une fraude et d'obtenir des conseils sur la façon d'empêcher qu'une telle situation se reproduise[383]. Le dépôt permet aux organismes d'application de la loi de cerner les tendances et les comportements en matière de vol d'identité et les aide lors d'enquêtes éventuelles.

Le surintendant Jean Cormier, directeur des Centres de coordination de la police fédérale de la GRC, a indiqué au Comité que, en 2013, « [p]lus de 24 000 victimes de crimes contre l'identité ont communiqué avec le CAFC et fait état de pertes de 11 millions de dollars », et ce, même si « seuls 5 % des cas de fraude sont signalés » [384] au CAFC. À son avis, « [c]es données illustrent l'importance pour la police de travailler de près avec ses partenaires au pays et à l'étranger afin de prévenir et de détecter le crime, et de poursuivre ceux qui se livrent à de telles activités [frauduleuses][385] ». Si le CAFC a été en mesure de tisser ce type de collaboration entre les secteurs public et privé, le surintendant Cormier a indiqué toutefois que « les défis auxquels nous sommes confrontés lorsque nous travaillons avec les secteurs privé et public et les organismes

383 ETHI, *Témoignages*, réunion n° 17, 2e session, 41e législature, 3 avril 2014, 1130 (surint. Jean Cormier, directeur, Centres de coordination de la police fédérale, Gendarmerie royale du Canada). Voir aussi Centre antifraude du Canada, *Au sujet du CAFC*.

384 *Ibid*, 1105 et 1200.

385 *Ibid*, 1105.

d'application de la loi ont trait à la capacité de communiquer les renseignements personnels, qui est restreinte dans certains cas par les lois en matière de protection des renseignements personnels, bien sûr, et par l'obligation au secret professionnel des entreprises[386] ».

Sous l'égide du CAFC, le Bureau de la concurrence participe aux enquêtes concernant les fraudes par marketing de masse à grande échelle, à savoir des fraudes commises par l'entremise des moyens de communication de masse qui font la promotion d'un produit ou d'intérêts commerciaux et nuisant ainsi à la concurrence. Selon M. Morgan Currie, sous-commissaire adjoint intérimaire de la concurrence au Bureau de la concurrence, « [l]e vol d'identité et le blanchiment d'argent demeurent des volets essentiels des diverses manœuvres de fraude par marketing de masse » qui coûtent chaque année 10 milliards de dollars à l'économie canadienne[387].

À l'instar du surintendant Cormier, M. Currie a souligné l'importance de la collaboration entre les acteurs du secteur public, indiquant que le Bureau de la concurrence joue un rôle central au CAFC — « [qui est] au cœur du réseau national des partenariats en matière de fraude par marketing de masse » — ainsi que dans de nombreux partenariats internationaux, de concert avec les organismes d'application de la loi et de réglementation[388]. Comme il l'a indiqué,

> [p]our combattre efficacement la fraude par marketing de masse, les autorités chargées d'enquête, d'application de la loi et de réglementation de nombreux pays travaillent de manière concertée pour recueillir et échanger l'information sur les manœuvres de fraude par marketing de masse et la façon d'y contrevenir; mènent de plus en plus des programmes de sensibilisation et d'éducation pour aider les particuliers et les entreprises à reconnaître les manœuvres de fraude par marketing de masse et éviter ainsi les pertes; élaborent des mesures pour identifier plus rapidement les manœuvres de fraude par marketing de masse et aider les victimes; et déploient des efforts coordonnés avec les organismes d'application de la loi, et renforcent ces efforts, pour lutter contre les manœuvres de fraude par marketing de masse[389].

Le Comité salue le travail des différents organismes membres du CAFC. Ce type de collaboration entre les organismes d'application de la loi et de réglementation est nécessaire pour bien éduquer la population, prévenir, mettre au jour et entraver les activités frauduleuses et faciliter le processus d'enquête et de poursuite contre les personnes impliquées dans ce type d'activités criminelles. En particulier, le Comité souligne les efforts des campagnes de prévention de la fraude du CAFC — dont le Mois de la prévention de la fraude, qui se tient chaque année en mars — qui visent à éduquer

386 *Ibid*, 1130.

387 *Ibid*, 1110, 1115 (Morgan Currie, sous-commissaire adjoint intérimaire de la concurrence, Bureau de la concurrence, Direction générale des pratiques loyales des affaires Division C , ministère de l'Industrie).

388 *Ibid*, 1115.

389 *Ibid*.

les consommateurs sur « la façon de reconnaître, de signaler et d'enrayer diverses formes de fraude par marketing de masse[390] ».

Toutefois, le Comité constate l'importance de signaler la fraude d'identité. Comme l'ont fait remarquer les représentants de la GRC et du Bureau de la concurrence, la sous-déclaration est un « gros problème » qui complique la compilation des renseignements et l'évaluation de l'ampleur, de la prévalence et des coûts associés à la fraude d'identité. M. Benoît Dupont a mis en garde contre le fait de ne pas connaître l'ampleur du problème relativement au nombre réel de victimes et à l'évolution de la tendance criminelle. Au sujet des 24 000 victimes de fraude qui ont signalé leur cas au CAFC en 2013, M. Dupont a indiqué ce qui suit :

> Il s'agit probablement d'une infime fraction d'un bassin général de victimes, car la plupart d'entre elles […] ne portent pas plainte formellement auprès des services de police. Certaines d'entre elles n'estiment pas le crime suffisamment important ou suffisamment intéressant, tandis que d'autres sont découragés par leur service de police local, lequel n'est pas équipé pour faire face à ce type de crime, notamment si les montants concernés sont inférieurs à un certain seuil[391].

De l'avis de M. Dupont, le fait de connaître le nombre de victimes, les types de vol d'identité qu'elles ont subis, les types de voleurs d'identité qui exécutent de telles escroqueries et l'emplacement depuis lequel ils les exécutent sont tous des éléments qui peuvent aider à concevoir des stratégies réglementaires et d'application de la loi visant à protéger les renseignements personnels des consommateurs et à diriger les ressources plus efficacement. Le Comité souscrit à cette évaluation et observe que le CAFC est en mesure de poursuivre ses efforts pour inciter toutes les victimes de fraude d'identité à signaler leur cas au CAFC.

B. Stratégie nationale de lutte contre les crimes liés à l'identité

Le surintendant Cormier a parlé au Comité de la Stratégie nationale de lutte contre les crimes liés à l'identité, un projet de la GRC mené en 2012 au terme d'un processus consultatif auprès d'acteurs des secteurs privé et public[392]. Comme il l'a expliqué :

> La stratégie repose sur trois piliers : l'éducation et la prévention; les renseignements et l'application de la loi; et les poursuites. La stratégie vise à cibler les priorités et les risques émergents, et à analyser les tendances; à utiliser les données et les analyses émanant du volet sur les renseignements criminels; à accroître la portée du projet d'enquête fondé sur les renseignements et les efforts d'interruption coordonnés; et à élaborer une approche normalisée relative à la fraude d'identité — et donc aux enquêtes —, ce qui comprend la création et l'adoption d'un protocole d'enquête intergouvernemental; comme je l'ai dit, le crime traverse souvent les frontières[393].

---

390 *Ibid*.

391 ETHI, *Témoignages*, réunion n° 19, 2e session, 41e législature, 29 avril 2014, 1130 (Dupont.

392 GRC, *Stratégie nationale de lutte contre les crimes liés à l'identité*.

393 ETHI, *Témoignages*, réunion n° 17, 2e session, 41e législature, 3 avril 2014, 1120 (Cormier).

La stratégie, dont la mise en œuvre s'est amorcée en 2013, vise à « [sensibiliser] la communauté judiciaire et les responsables du gouvernement du Canada et des autres pays à l'égard du vol d'identité[394] ». Selon M[me] Philippa Lawson, de la Clinique d'intérêt public et de politique d'Internet du Canada, la stratégie « est un bon point de départ, mais il faut bien davantage de travail pour aller au-delà des généralités et tenir compte de la protection des consommateurs[395] ». À son avis, « [l]e Canada doit avoir une stratégie nationale pour mieux comprendre la criminalité associée à l'identité, pour mieux lutter contre elle. Cette stratégie doit être confiée à de hauts fonctionnaires et nécessiter la participation de tous les intervenants clés […] y compris les organismes de protection des consommateurs et les commissaires à la protection des renseignements personnels des divers ordres de gouvernement[396] ». M[me] Lawson suggère « la création de mécanismes de collecte de données fiables et assez complètes sur l'incidence, le type et le coût des actes criminels liés à l'identité au Canada[397] ». Le Comité est du même avis : une collecte fiable des données est indispensable à la création de politiques, de stratégies et de programmes efficaces pour lutter contre le vol et la fraude d'identité. Le Comité prend cet élément en considération dans ses recommandations.

C. Loi canadienne anti-pourriel

Adoptée en décembre 2010, la Loi canadienne anti-pourriel (LCAP), dont la plupart des dispositions sont entrées vigueur depuis le 1[er] juillet 2014 — pendant que le Comité menait la présente étude — établit certaines interdictions visant « à protéger les Canadiens, tout en veillant à ce que les entreprises demeurent concurrentielles sur le marché mondial[398] ». Parmi ces interdictions, notons l'envoi de messages électroniques commerciaux, la modification des données de transmission et l'installation de programmes ou de logiciels informatiques sur l'ordinateur d'une autre personne sans son consentement[399]. La LCAP est appliquée grâce à la collaboration de trois organismes gouvernementaux, à savoir le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC), qui supervise les violations des interdictions énoncées; le Bureau de la concurrence, qui enquête sur les indications fausses ou trompeuses et les pratiques commerciales trompeuses; et le Commissariat à la protection de la vie privée, qui enquête sur la collecte de renseignements personnels par le truchement d'accès illégaux à des réseaux informatiques et sur le prélèvement d'adresses électroniques. Aux termes de la loi, le CRTC et le Bureau de la concurrence peuvent tous deux imposer des sanctions

---

394 *Ibid*.

395 ETHI, *Témoignages*, réunion n[o] 19, 2[e] session, 41[e] législature, 29 avril 2014, 1150 (Lawson).

396 *Ibid*.

397 *Ibid*.

398 ETHI, *Témoignages*, réunion n[o] 16, 2[e] session, 41[e] législature, 1[er] avril 2014, 1215 (Michael Jenkin, directeur général, Bureau de la consommation, ministère de l'Industrie). Voir aussi La *Loi canadienne anti-pourriel*, *Au sujet de la loi*.

399 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 [LCAP], L.C. 2010, ch. 23, art. 6 et 8.

administratives pécuniaires, et le Bureau de la concurrence peut en plus prendre des sanctions pénales en vertu de la *Loi sur la concurrence*.

Selon M. Michael Jenkin, directeur général du Bureau de la consommation du ministère de l'Industrie, la LCAP répond à plusieurs préoccupations importantes, dont

> les « messages hameçons », qui sont conçus pour attirer les destinataires vers des sites Web truqués et les inciter à révéler des renseignements personnels comme des noms d'utilisateur, des mots de passe et des renseignements sur des comptes; les logiciels malveillants, qui sont installés dans l'ordinateur, le téléphone intelligent ou tout autre appareil numérique d'une personne à son insu et sans son consentement — ces logiciels espions et ces virus peuvent secrètement recueillir des renseignements personnels qui seront ensuite utilisés à des fins de vol d'identité; et enfin, le détournement du trafic, qui consiste à réacheminer secrètement les recherches en ligne d'une personne vers une destination frauduleuse où les attaquants pourront recueillir des renseignements personnels en vue de procéder à des vols d'identité[400].

M. Currie, du Bureau de la concurrence, a fait remarquer que, grâce à cette loi, son organisme serait « en mesure de s'attaquer plus efficacement aux indications fausses ou trompeuses ainsi qu'aux pratiques commerciales trompeuses dans le marché électronique, notamment les renseignements faux ou trompeurs sur l'expéditeur ou dans l'objet d'un message, les messages électroniques faux ou trompeurs, ainsi que les renseignements faux ou trompeurs sur l'emplacement comme les URL et les métadonnées ».

Les dispositions relatives aux sanctions prévues dans la LCAP permettent au CRTC et au Bureau de la concurrence d'imposer des sanctions administratives pécuniaires pouvant aller jusqu'à 1 million de dollars pour les particuliers et jusqu'à 10 millions de dollars pour les entreprises[401]. M[me] Gratton a indiqué que ces dispositions, qui peuvent étendre la responsabilité aux administrateurs, aux dirigeants et aux employeurs, sont « très élevées »; par conséquent, la loi « est prise au sérieux » par les entreprises, en ce sens qu'elles déploient beaucoup de ressources pour s'assurer qu'elles respectent la LCAP[402]. Selon M[me] Gratton, l'expérience tirée de la loi anti-pourriel est instructive à l'égard des pouvoirs d'application de la loi et de la création d'incitatifs pour encourager les entreprises à investir dans la prévention du vol d'identité[403].

Le Comité constate que les règles de la LCAP concernant l'installation de programmes informatiques sont entrées en vigueur le 15 janvier 2015 et que les articles relatifs au droit privé d'action devraient entrer en vigueur en juillet 2017. À mesure que les entreprises et les particuliers s'adapteront et se conformeront à la LCAP, le Comité voudra continuer à observer les effets de la loi sur les intérêts des Canadiens relativement à la vie privée et à l'identité avant de tirer des leçons pertinentes de la mise en œuvre de la LCAP.

---

400 ETHI, *Témoignages*, réunion n° 16, 2e session, 41e législature, 1er avril 2014, 1215 (Jenkin).

401 LCAP, s. 20(4).

402 ETHI, *Témoignages*, réunion n° 20, 2e session, 41e législature, 1er mai 2014, 1150 (Éloïse Gratton, associée et vice-présidente, Conformité, McMillan LLP, à titre personnel).

403 *Ibid*, 1150,1215 et 1220 (Gratton).

D. Modernisation de l'administration des numéros d'assurance sociale

Les NAS sont utilisés par les ministères et les organismes fédéraux en tant qu'identifiants pour la prestation de programmes et de services, comme l'assurance-emploi, les prêts d'études canadiens, le Régime de pensions du Canada et la Sécurité de la vieillesse, de même qu'à des fins fiscales. Les citoyens canadiens, les résidents permanents et les résidents temporaires reçoivent un NAS unique qui leur permet de travailler au Canada et de se prévaloir des avantages sociaux et des services qu'offrent les programmes publics. Le Registre d'assurance sociale contient tous les NAS ainsi que les renseignements fournis par les particuliers lorsqu'ils font la demande d'un NAS.

Service Canada, un organisme relevant du ministère de l'Emploi et du Développement social, supervise l'attribution des NAS et administre le Registre d'assurance sociale. Si les ministères et les programmes gouvernementaux sont tenus de recueillir et d'utiliser le NAS, les organismes du secteur privé sont quant à eux autorisés à demander le NAS d'un client à des fins précises liées à une exigence du gouvernement (relevant de l'emploi ou de l'impôt sur le revenu, par exemple). Toutefois, aucune loi n'interdit à un organisme privé de demander le NAS d'un particulier à d'autres fins ou n'oblige un particulier à fournir son NAS[404].

Lors des témoignages, des témoins ont expliqué au Comité l'évolution des pratiques d'attribution des NAS et de l'administration du Registre d'assurance sociale « pour renforcer l'intégrité du programme des numéros d'assurance sociale et pour réduire l'incidence et l'impact de la fraude en matière d'identité[405] ». M. Louis Beauséjour, sous-ministre adjoint au ministère de l'Emploi et du Développement social, a parlé au Comité de deux rapports publiés par le Bureau du vérificateur général (BVG) sur le programme du NAS en 1998 et en 2002. Dans ces rapports, le BVG « notait principalement que les procédures de preuve d'identité devaient être améliorées, que les sources d'information existantes devaient être mieux utilisées, que les renseignements que contenait la base de données du NAS n'étaient pas toujours complets ni exacts, et qu'il y avait davantage de NAS en circulation que de Canadiens de plus de 20 ans[406] ».

À la lumière de ces constatations, « d'importantes initiatives ont été lancées pour améliorer l'administration des NAS et du RAS [Registre d'assurance sociale], ce qui a contribué aux efforts faits par le gouvernement pour lutter contre le vol et la fraude liés à l'identité[407] ». Parmi ces initiatives, notons l'indicateur inactif, qui identifie les NAS qui ne sont plus actifs depuis cinq années consécutives ou plus et pour lesquels la réactivation nécessite la présentation d'une preuve d'identité originale; l'introduction d'une date

---

404 ETHI, *Témoignages*, réunion n° 16, 2e session, 41e législature, 1er avril 2014, 1145 (Louis Beauséjour, sous-ministre adjoint, Direction générale des services d'intégrité, Service Canada, ministère de l'Emploi et du Développement social). Voir aussi Service Canada, *Numéro d'assurance sociale — Code de bonnes pratiques*.

405 *Ibid*, 1100.

406 *Ibid*, 1105.

407 *Ibid*.

d’échéance pour les NAS attribués à des travailleurs étrangers temporaires; et la création d’un site Web de référence interne sur les preuves d’identité qui permet aux agents responsables de l’attribution des NAS d’avoir accès à des renseignements détaillés quant aux éléments à examiner dans les documents d’identité afin de s’assurer de leur authenticité.

En outre, le ministère de l'Emploi et du Développement social a instauré un programme d'accréditation pour former les agents à l’attribution et à l’administration des NAS, et il a publié un *Code de bonnes pratiques du NAS* à l’intention des employeurs, des particuliers et des intervenants afin de les guider sur ce qu’ils doivent faire ou ne pas faire pour protéger les renseignements personnels. De plus, le Ministère a signé des ententes avec chacune des provinces en vue de créer des liens électroniques entre les bureaux de l’état civil et le Registre d’assurance sociale. Depuis 2014, exception faite des personnes résidant en région éloignée, faisant face à des restrictions en raison de circonstances atténuantes ou se trouvant à l’étranger, les demandes de NAS ne peuvent plus être envoyées par la poste; elles doivent désormais être faites en personne à un point de service de Service Canada. Une fois attribué, le NAS est communiqué en format papier, les cartes en plastique ayant été abolies. Selon M. Beauséjour, « [c]ette initiative aidera à empêcher le vol et la fraude liés à l'identité en cas de perte ou de vol des cartes d'assurance sociale[408] ».

M. Beauséjour a déclaré au Comité que, au cours de l’exercice financier 2013, Service Canada « [a] mené plus de 4 500 enquêtes, au terme [desquelles] nous avons conclu qu'il y avait utilisation frauduleuse du numéro d'assurance sociale[409] ». Selon ses estimations, dans les trois quarts des cas « il s’agissait aussi d’enquête[s] parallèle[s] sur les prestations, et environ 1 400 portaient sur des problèmes possibles liés à des demandes de NAS[410] ». Lorsque l’utilisation frauduleuse est liée au NAS et risque de mener à d’autres types de fraudes, le dossier est transmis à la GRC à des fins d’enquête. M. Beauséjour a ajouté que, dans les cas d’atteintes importantes, « il y a une entente sur les trois caractéristiques d'une atteinte qu'il faut déclarer à la commissaire ». De telles atteintes visent des renseignements directement liés à des renseignements personnels de nature sensible, l’existence d’un risque de vol ou de fraude d’identité et la possibilité que l’incident nuise à la carrière, à la réputation, à la situation financière, à la sécurité, à la santé ou au bien-être de la personne.

Bien que M. Beauséjour ait indiqué « [ne] pas [être] au courant de mauvaises utilisations du NAS à la suite d'un accès illicite donnant lieu à la perte de renseignements personnels », le dossier concernant la perte d’appareils de stockage portatifs non chiffrés contenant le NAS et d’autres renseignements sur quelque 583 000 personnes par le ministère de l'Emploi et du Développement social a mené à la mise en place de

408 *Ibid*, 1110.

409 *Ibid*, 1120.

410 *Ibid*.

« différentes mesures de renforcement de la protection » et à la recherche de « nouvelles manières de réduire les risques associés à la perte de renseignements personnels[411] ».

E. Lancement du passeport électronique

Le Comité a appris des détails sur le Programme de passeport, et il a été informé qu'il s'agit d'un effort concerté de plusieurs ministères. Le ministre de la Citoyenneté et de l'Immigration assume l'entière responsabilité du Programme de passeport, ce qui comprend « la délivrance, le refus de délivrer, la révocation, la retenue, la récupération et l'utilisation des passeports canadiens[412] ». De plus, le Programme de passeport fait équipe avec les organismes d'application de la loi et du renseignement pour évaluer les demandeurs ou les titulaires de passeport. Au Canada, la prestation des services de passeport relève du ministère de l'Emploi et du Développement social, tandis que le ministère des Affaires étrangères, du Commerce et du Développement s'occupe des demandes présentées par les Canadiens à l'étranger.

Selon les représentants du ministère de la Citoyenneté et de l'Immigration, quelque 5 millions de demandes sont présentées chaque année et 23 millions de documents de voyage canadiens valides sont actuellement en circulation. Les passeports délivrés depuis le 1er juillet 2013 respectent les « normes internationales les plus récentes établies par l'Organisation de l'aviation civile internationale, que l'on considère comme la référence en matière de document de voyage[413] ». Ces passeports électroniques sont dotés d'une puce électronique intégrée qui leur confère un niveau de sécurité supplémentaire pour les prémunir contre le vol d'identité. Selon M. Lu Fernandes, directeur général de la Direction générale de l'intégrité du Programme de passeport :

> La puce renferme les renseignements qui figurent à la page 2 du passeport, y compris la photo du titulaire, procurant ainsi au personnel de contrôle frontalier un outil supplémentaire pour valider l'identité du titulaire du passeport. En consultant l'information sur la puce et en la comparant aux renseignements indiqués à la page 2 du livret, un agent des services frontaliers peut s'assurer que l'information ou la photo n'a pas été modifiée.

La conception des pages de visa du passeport électronique offre un niveau supplémentaire de sécurité, ce qui rend le livret plus difficile à contrefaire. Les pages sont constituées de paires de vignettes uniques qui illustrent des thèmes, des lieux et des personnages marquants de l'histoire du Canada. Grâce aux différentes images sur chaque page et à divers éléments de sécurité visibles et invisibles, il est très difficile et extrêmement coûteux pour les faussaires de reproduire un livret ou de substituer une page[414].

---

411 *Ibid*, 1120, 1150.

412 *Ibid*, 1200 (Lu Fernandes, directeur général, Direction générale de l'intégrité du Programme de passeport, ministère de la Citoyenneté et de l'Immigration).

413 *Ibid*.

414 *Ibid*, 1205. Voir aussi Passeport Canada, *À propos de votre passeport*.

Le Comité a appris que la perte ou le vol d'environ 66 000 passeports sont signalés chaque année, le scénario le plus fréquent étant celui de « gens qui ont simplement oublié où ils ont mis leur passeport ou qui oublient dans quel carton ils ont bien pu le mettre lors d'un déménagement, et qui le déclarent perdu[415] ». Dès que la perte ou le vol d'un passeport est signalé, ce dernier est annulé et l'information est transmise dans les 24 heures à l'Agence des services frontaliers du Canada et au Centre d'information de la police canadienne. Ce dernier transmet ensuite l'information à Interpol, qui met à jour sa base de données. Une fois qu'un passeport a été annulé, il ne peut plus être utilisé pour voyager même s'il est retrouvé par la suite.

Le Comité a appris que, en 2013, Passeport Canada a « refusé ou révoqué environ 1 370 demandes de passeport. Un millier de ces refus ou révocations [ont eu] lieu pour cause de criminalité […]. Dans près de 225 cas, il s'agissait de fraude à l'admissibilité ou d'usage abusif d'un passeport [et] [d]ans 36 autres cas, il s'agissait de problèmes de citoyenneté : un individu qui n'était pas, en fait, citoyen canadien[416] ». Dans quelque 70 cas, le refus ou la révocation reposait sur la fraude d'identité, c'est-à-dire que le demandeur « [a] volé les documents de quelqu'un : carte de citoyenneté, certificat de naissance ou carte d'assurance-maladie […] que la personne utilise pour faire une demande de passeport[417] ». Dans de tels cas, Passeport Canada fait enquête sur le demandeur, avise ce dernier qu'il fait l'objet d'une enquête et met un terme au processus de demande. Lorsque des mesures administratives sont prises, le service de passeport peut être suspendu pendant cinq ans à partir de la date de l'incident. Des exemptions peuvent être accordées pour des motifs d'ordre urgent, impérieux ou de compassion. « [Seuls] les cas les plus graves de fraude ou de vol d'identité » sont signalés à la GRC et c'est cette dernière, et non Passeport Canada, qui fait enquête sur le vol d'identité. Selon les responsables du Programme de passeport qui ont comparu devant le Comité, « nous ne savons pas comment les documents ont été volés au juste […]. Pour nous, c'est une zone vraiment grise[418] ».

F. Cadre d'intégrité de l'Agence du revenu du Canada

Des représentants de l'Agence du revenu du Canada (ARC) ont comparu devant le Comité. Ils ont expliqué que l'organisme s'emploie à mettre en place des mesures de protection pour protéger les renseignements personnels des Canadiens et réduire les risques de vol d'identité. L'ARC compte parmi les plus grandes institutions du gouvernement du Canada et possède l'un des plus importants fonds de données de renseignements personnels du pays. Habituellement, dans le cas d'un contribuable canadien, l'ARC possède « toute l'information contenue dans [sa] déclaration de revenus et de prestations », ce qui comprend son NAS, son revenu, les crédits dont il veut se prévaloir et tout renseignement supplémentaire visant des crédits en particulier, par

415 *Ibid*, 1230.

416 *Ibid*, 1235 et 1240.

417 *Ibid*, 1235 (Peter Bulatovic, directeur, Direction des enquêtes, Direction générale de l'intégrité du Programme de passeport, ministère de la Citoyenneté et de l'Immigration).

418 *Ibid* et 1240 (Fernandes).

exemple des renseignements d'ordre médical dans le cas d'un crédit d'impôt pour personne handicapée. Dans le cas d'une entreprise, l'ARC possède des renseignements sur son revenu, la TPS et la TVH qu'elle a perçues au nom du gouvernement ainsi que tout autre renseignement supplémentaire concernant les crédits[419].

En 2012, l'ARC a lancé son cadre d'intégrité afin de regrouper l'ensemble de ses politiques, programmes et systèmes pour s'assurer que « les normes élevées établies pour protéger la vie privée des contribuables sont communiquées à tous les employés et gestionnaires et [que] le rendement de l'Agence par rapport à ces normes fait l'objet d'une surveillance et de rapports minutieux[420] ». M^me^ Susan Gardner-Barclay, sous-commissaire et chef de la protection des renseignements personnels de la Direction des affaires publiques de l'ARC, a parlé au Comité d'autres initiatives, notamment la création de « 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[421] ». Elle a également parlé des protocoles de communication de renseignements de l'ARC et d'un exercice à l'échelle de l'organisme permettant de vérifier que les évaluations des facteurs relatifs à la vie privée sont à jour. Ces mesures visent à prévenir les fuites de renseignements personnels qui peuvent « représenter un risque que des renseignements servent au vol d'identité ou à d'autres activités criminelles[422] ». Selon M^me^ Gardner-Barclay, ces initiatives, conjuguées aux efforts visant à mettre en garde les Canadiens contre les stratagèmes d'hameçonnage qui présentent faussement l'ARC, démontrent que « l'ARC s'attache à mettre en place des mesures de contrôle, à les évaluer et à les améliorer[423] ».

Des responsables ont dit au Comité que 2 983 atteintes ont été signalées à l'ARC en 2013. Parmi ces atteintes, le courrier mal acheminé constituait « 95 % des atteintes à la sécurité de l'information et des données et à la vie privée de l'ARC ». Néanmoins, « un grand nombre des atteintes à la sécurité des données relevées par l'ARC ne constituent pas des atteintes à la vie privée, puisqu'aucun renseignement personnel n'a été divulgué[424] ». Toutefois, selon les mêmes responsables, les atteintes à la vie privée constituaient 46 % des cas signalés et 479 cas présentaient « un risque plausible de préjudice pour la personne », ce qui a donné lieu à la transmission du dossier au Commissariat à la protection de la vie privée conformément aux lignes directrices du Conseil du Trésor[425]. Dans les cas où l'ARC a communiqué avec un contribuable dont les

---

419 ETHI, *Témoignages*, réunion n^o^ 18, 2^e^ session, 41^e^ législature, 8 avril 2014, 1200 (Susan Gardner-Barclay, sous-commissaire et chef de la protection des renseignements personnels, Direction générale des affaires publiques, Agence du revenu du Canada).

420 *Ibid*, 1110.

421 *Ibid*.

422 *Ibid*.

423 *Ibid*.

424 *Ibid*, 1110 et 1145.

425 *Ibid*, 1145.

renseignements personnels étaient à risque, l'organisme peut « soit lui offrir une aide au moyen d'Equifax, un organisme qui offre des services pour le crédit, et […] accoler un fanion à son dossier pour signaler l'existence d'un risque potentiel de vol d'identité[426] ».

G. L'Évaluation des impacts des mesures de sécurité sur les droits de la personne

Le Comité a entendu le témoignage de M. Philippe Dufresne, à l'époque directeur général et avocat général principal de la Direction générale de la promotion des droits de la personne de la Commission canadienne des droits de la personne. M. Dufresne a parlé des travaux de la Commission relativement à la certification de l'identité 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[427] ». Les travaux de la Commission ont 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* ». Selon M. Dufresne, ce phénomène est attribuable à l'utilisation de méthodes parfois inaccessibles à une personne ou à un groupe de personnes et au fait que les décisions rendues par les agents concernant la validation de l'identité peuvent conduire à de la discrimination[428].

Pour corriger le tir, la Commission canadienne des droits de la personne recommande le recours à des systèmes biométriques multimodaux qui ne se fient pas exclusivement à une forme de certification de l'identité pouvant se révéler discriminatoire. Par exemple, il est possible de conjuguer la prise des empreintes digitales — qui peut ne pas être accessible aux gens qui n'ont pas de doigts — au balayage rétinien pour ainsi offrir un certain degré « d'inclusivité ». Comme l'explique M. Dufresne,

> [l]orsqu'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

426 *Ibid*, 1120 (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).

427 *Ibid*, 1100 (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).

428 *Ibid*.

déployés pour explorer d'autres moyens moins discriminatoires d'en arriver aux mêmes résultats[429].

Dans le cadre de ses efforts pour inciter les organismes à examiner une mesure donnée sous l'angle des droits de la personne, la Commission canadienne des droits de la personne a publié *L'Évaluation des impacts des mesures de sécurité sur les droits de la personne*. Ce guide « 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[430] ». Les quatre étapes — choisir la bonne mesure de sécurité, mettre la mesure à l'essai pour vérifier s'il existe un risque de discrimination, améliorer la mesure de sécurité et faire un suivi pour détecter les cas de discrimination non prévus — établissent une approche proactive qui peut « éviter de perdre du temps et de l'argent, tout en améliorant l'efficacité et l'efficience d'une mesure de sécurité et en gagnant le soutien public pour les initiatives de sécurité, qu'elles soient nouvelles ou déjà en place[431] ».

Le Comité est d'accord avec l'évaluation de M. Dufresne, selon qui la sécurité peut être renforcée par des mesures conformes aux principes des droits de la personne. Le Comité encourage les organismes qui collectent des renseignements personnels — auprès d'institutions gouvernementales ou d'entreprises privées — à envisager de mettre en place des outils tels que *L'Évaluation des impacts des mesures de sécurité sur les droits de la personne* qui peuvent servir à améliorer la création de politiques visant à prévenir le vol d'identité et à y remédier.

H. Soutien aux victimes

Plusieurs témoins ont parlé au Comité du travail qui est accompli pour aider les victimes de vol d'identité. Plusieurs organismes et programmes publics, comme l'ARC, le Bureau de la concurrence et le CAFC, ont mis à la disposition des citoyens des renseignements sur la façon de protéger leur identité et les mesures à prendre s'ils soupçonnent avoir été victimes de ce type d'activité criminelle[432]. Un organisme non gouvernemental dont il est question ci-dessus, le Centre de soutien aux victimes de vol d'identité du Canada, reçoit « des fonds fédéraux pour renseigner et soutenir les victimes de vol d'identité. Son mandat est bien précis et limité […]. Il accompagne les victimes pas à pas, tout le long du processus complexe de recouvrement de leur identité[433] ».

Au cours des témoignages concernant les mesures que prennent les organismes publics pour protéger les Canadiens du vol d'identité, des témoins ont rappelé à maintes

---

429 *Ibid*.

430 *Ibid*. Voir aussi Commission canadienne des droits de la personne, *L'Évaluation des impacts des mesures de sécurité sur les droits de la personne*.

431 Commission canadienne des droits de la personne, *L'Évaluation des impacts des mesures de sécurité sur les droits de la personne*.

432 Voir, par exemple, Agence du revenu du Canada, *Protégez-vous contre le vol d'identité*; Bureau de la concurrence, *Le petit livre noir de la fraude*; et CAFC, *Le vol d'identité : Pourriez-vous en être victime?*

433 ETHI, *Témoignages*, réunion n° 19, 2e session, 41e législature, 29 avril 2014, 1145 (Lawson).

reprises au Comité la nécessité de la formation continue et de la sensibilisation[434]. Les initiatives visant à aider les particuliers à protéger leurs renseignements personnels nécessitent un effort concerté de la part des organismes publics, des acteurs du secteur privé et des organismes non gouvernementaux d'intérêt public. L'éducation et la sensibilisation sont également nécessaires pour aider les victimes de vol et de fraude d'identité. Par ailleurs, des témoins ont également rappelé au Comité la nécessité de mesures concertées et soutenues pour colliger les renseignements et analyser les données sur l'ampleur et les paramètres des crimes liés à l'identité afin de mieux adapter les programmes de prévention et les initiatives de soutien aux victimes[435].

Enfin, on a souligné au Comité qu'« il faudrait adopter une stratégie nationale de soutien aux victimes de vol d'identité qui établira clairement les paramètres de la collaboration entre les divers organismes participant au processus de soutien aux victimes, comme le Centre antifraude du Canada, le Centre de soutien aux victimes de vol d'identité du Canada et les divers organismes de réglementation qui traitent les affaires liées au vol d'identité[436] ». Le Comité est d'avis qu'une telle stratégie pourrait compléter celle que la GRC a mise en place en 2012.

Pour ces motifs, le Comité fait les recommandations suivantes :

Recommandation 6 : Le Comité recommande que le gouvernement du Canada continue de promouvoir les efforts visant à protéger les Canadiens du vol d'identité, à offrir des services de soutien aux victimes de vol d'identité et à poursuivre les auteurs de crimes contre l'identité, et qu'il continue d'affecter des ressources à ces fins.

Recommandation 7 : Le Comité recommande que le gouvernement du Canada trouve des moyens de promouvoir davantage la collaboration entre les acteurs des secteurs privé et public, notamment les organismes de protection des consommateurs et les commissariats à la vie privée de niveaux fédéral et provincial. Une telle collaboration devrait aller au-delà des programmes d'éducation et de sensibilisation de façon à inclure la création de mécanismes de collecte de données fiables et raisonnablement exhaustives sur la fréquence des crimes contre l'identité au Canada, leurs types et les coûts qu'ils représentent,

---

434 ETHI, *Témoignages*, réunion n° 16, 2e session, 41e législature, 1er avril 2014 (Jenkin); ETHI, *Témoignages*, réunion n° 17, 2e session, 41e législature, 3 avril 2014 (Cormier et Currie); ETHI, *Témoignages*, réunion n° 18, 2e session, 41e législature, 8 avril 2014 (Gardner-Barclay et Brown); ETHI, *Témoignages*, réunion n° 19, 2e session, 41e législature, 29 avril 2014 (Fernandez et Lawson); ETHI, *Témoignages*, réunion n° 26, 2e session, 41e législature, 3 juin 2014 (Dorey, Scott et Israel). Voir aussi ETHI, B.C. Freedom of Information and Privacy Association, *Mémoire : le vol d'identité et ses répercussions économiques,* 13 mars 2015.

435 ETHI, *Témoignages*, réunion n° 19, 2e session, 41e législature, 29 avril 2014 (Fernandez et Lawson); ETHI, *Témoignages*, réunion n° 19, 2e session, 41e législature, 1er mai 2014 (Levin); ETHI, *Témoignages*, réunion n° 26, 2e session, 41e législature, 3 juin 2014 (Dorey, Scott et Israel). Voir aussi ETHI, B.C. Freedom of Information and Privacy Association, *Mémoire : le vol d'identité et ses répercussions économiques,* 13 mars 2015.

436 ETHI, *Témoignages*, réunion n° 26, 2e session, 41e législature, 3 juin 2014, 1240 (Israel). Voir aussi ETHI, *Témoignages*, réunion n° 19, 2e session, 41e législature, 29 avril 2014, 1150 (Lawson).

ainsi que la communication de ces données à des fins de recherche et d’analyse.

CONCLUSION ET RECOMMANDATIONS

À la lumière de l'ensemble des témoignages entendus au cours d'une dizaine de réunions tenues entre avril 2014 et février 2015, et des mémoires reçus à ce sujet, de personnes provenant de ministères et d'agences gouvernementales, des forces de l'ordre, de groupes d'intérêt, d'universités, de bureaux d'avocats, d'agences d'évaluation du crédit, de banques et d'entreprises des technologies de l'information, le Comité a formulé les recommandations suivantes :

Recommandation 1 : Le Comité exhorte les agences d'évaluation du crédit des consommateurs à fournir gratuitement aux consommateurs canadiens un accès électronique à leur dossier de crédit, au moins une fois par année.

Recommandation 2 : Le Comité exhorte les banques canadiennes à adopter, comme définition commune du vol d'identité, la définition qui se trouve dans le Code criminel en vigueur au Canada et à compiler des données sur le vol d'identité en conséquence.

Recommandation 3 : Le Comité exhorte les banques canadiennes à rendre publique l'information qu'elles détiennent sur le vol d'identité. L'information publiée devrait notamment porter à la fois sur les tentatives réussies et ratées de voler des renseignements personnels et devrait indiquer la source de l'attaque.

Recommandation 4 : Le Comité invite les banques canadiennes à investir dans des dispositifs technologiques afin de protéger les données de leurs clients. Ces dispositifs devraient notamment comprendre des systèmes de vérification enregistrant le nombre et les types d'accès aux dossiers des clients.

Recommandation 5 : Le Comité recommande que le gouvernement du Canada cherche à obtenir l'appui des provinces et territoires en considérant l'établissement d'une stratégie nationale afin de coordonner les efforts en matière de lutte au vol d'identité et de contrer ce crime plus efficacement.

Recommandation 6 : Le Comité recommande que le gouvernement du Canada continue de promouvoir les efforts visant à protéger les Canadiens du vol d'identité, à offrir des services de soutien aux victimes de vol d'identité et à poursuivre les auteurs de crimes contre l'identité, et qu'il continue d'affecter des ressources à ces fins.

Recommandation 7 : Le Comité recommande que le gouvernement du Canada trouve des moyens de promouvoir davantage la collaboration entre les acteurs des secteurs privé et public, notamment les

organismes de protection des consommateurs et les commissariats à la vie privée de niveaux fédéral et provincial. Une telle collaboration devrait aller au-delà des programmes d'éducation et de sensibilisation de façon à inclure la création de mécanismes de collecte de données fiables et raisonnablement exhaustives sur la fréquence des crimes contre l'identité au Canada, leurs types et les coûts qu'ils représentent, ainsi que la communication de ces données à des fins de recherche et d'analyse.

ANNEXE A :
LISTE DES TÉMOINS

Organismes et individus	Date	Réunion
Ministère de la Citoyenneté et de l'Immigration	2014/04/01	16
Peter Bulatovic, directeur Direction des enquêtes, direction générale de l'intégrité du Programme de passeport		
Lu Fernandes, directeur général Direction générale de l'intégrité du Programme de passeport		
Ministère de l'Emploi et du Développement social		
Louis Beauséjour, sous-ministre adjoint Direction générale des services d'intégrité, Service Canada		
Robert Frelich, directeur Division des Services d'identité des entreprises, Service Canada		
Ministère de l'Industrie		
Michael Jenkin, directeur général Bureau de la consommation		
Gendarmerie royale du Canada	2014/04/03	17
Jean Cormier, directeur Centres de coordination de la police fédérale		
Cameron Miller Centres de coordination de la police fédérale, domestique		
Ministère de l'Industrie		
Morgan Currie, sous-commissaire adjoint intérimaire de la concurrence Bureau de la concurrence, Direction générale des pratiques loyales des affaires Division C		
Thomas Steen, directeur des dossiers spéciaux et conseiller stratégique Bureau de la concurrence, Direction générale des pratiques loyales des affaires		
Agence du revenu du Canada	2014/04/08	18
Helen Brown, directrice générale Direction de la sécurité et des affaires internes, Direction générale des finances et de l’administration		
Susan Gardner-Barclay, sous-commissaire et chef de la protection des renseignements personnels Direction générale des affaires publiques		

Organismes et individus	Date	Réunion
Commission canadienne des droits de la personne	2014/04/08	18
Philippe Dufresne, directeur général et avocat général principal Direction générale de la promotion des droits de la personne		
Maciej Karpinski, analyste principal de recherche Direction générale de la promotion des droits de la personne		
À titre personnel	2014/04/29	19
José Manuel Fernandez, professeur agrégé Département de génie informatique et de génie logiciel, École Polytechnique de Montréal		
Philippa Lawson, avocate-procureure Associée, Clinique d'intérêt public et de politique d'internet du Canada, Université d'Ottawa		
Susan Sproule, professeure adjointe Finances, opération et systèmes d'information, Brock University		
Centre international de criminologie comparée		
Benoît Dupont, directeur		
À titre personnel	2014/05/01	20
Éloïse Gratton, associée et vice-présidente Conformité, McMillan LLP		
Avner Levin, professeur agrégé et directeur Institut de la cybercriminalité et de la vie privée, Ryerson University		
Equifax Canada Co.	2014/05/27	24
Carol Gray, présidente		
John Russo, vice-président, avocat et chef de la protection des renseignements personnels		
Tara Zecevic, vice-présidente Solutions de décisions		
Forrest Green Group of Companies		
Robert K. Groves, représentant Directeur, The Aboriginal Affairs Group Inc.		
Murray Rowe, Jr., président		
TransUnion Canada		
Chantal Banfield, vice-présidente et avocate générale		
Todd Skinner, président		
Banque Canadienne Impériale de Commerce	2014/05/29	25
Philip Fisher, directeur sénior Gestion des risques des canaux électroniques, Services intégrés de contrôle des affaires		

Organismes et individus	Date	Réunion
Banque royale du Canada	2014/05/29	25
Jay Stark, vice-président Services de vérification interne, Services bancaires aux particuliers et aux entreprises		
Banque Scotia		
Jennifer Frook, directrice Services partagés, Bureau de la gestion des fraudes		
BMO Groupe financier		
Ed Rosenberg, vice-président et chef de la sécurité Groupe légal, corporatif et de conformité		
Groupe Financier Banque TD		
Paul Milkman, vice-président sénior Chef de la Gestion du risque technologique et de la Sécurité des systèmes d'information		
Centre de soutien aux victimes de vol d'identité du Canada	2014/06/03	26
James Dorey, directeur principal		
Kevin Scott, président		
Samuelson-Glushko Clinique d'intérêt public et de politique d'Internet du Canada		
Tamir Israel, avocat		
Google inc.	2014/06/05	27
Colin McKay, chef, Politiques publiques et relations gouvernementales		
Rogers Communications inc.		
Kenneth Engelhart, vice-président principal Réglementation et chef de la protection des renseignements personnels		
Aaron Storr, directeur Soutien de l'exécution de la Loi		
À titre personnel	2015/02/23	33
Claudiu Popa, président-directeur général Informatica Corporation		
Crime Prevention Association of Toronto		
Janet Sherbanowski, directrice générale		

ANNEXE B :
LISTE DES MÉMOIRES

Organismes et individus

B.C. Freedom of Information and Privacy Association

Digital ID and Authentication Council of Canada

Gagnon, Maxime

Levin, Avner

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 n^{os} 16-20, 24-27, 33-36) est déposé.

Respectueusement soumis,

Le président,

Pierre-Luc Dusseault

Rapport complémentaire du Nouveau Parti démocratique sur l'étude du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique sur le problème grandissant du vol d'identité et ses répercussions économiques et sociales.

Bien qu'il appuie dans l'ensemble les conclusions et les recommandations du rapport du Comité, le Nouveau Parti démocratique (NPD) croit que le gouvernement a négligé d'aborder certains aspects essentiels du vol d'identité et de ses répercussions.

Le NPD convient que le vol d'identité est un problème croissant que le gouvernement du Canada doit prendre au sérieux. La protection des renseignements personnels et la lutte contre le vol d'identité sont des éléments essentiels de la robustesse de l'économie canadienne. Les Canadiens doivent pouvoir avoir confiance dans les technologies numériques qu'ils utilisent : ils doivent avoir le sentiment que la communication en ligne de leurs renseignements personnels est sécuritaire et qu'ils ne sont pas vulnérables au vol d'identité. C'est au gouvernement que revient la tâche de mettre les renseignements des Canadiens à l'abri du vol et de protéger adéquatement les informations qu'il détient. Il nous faut des mesures de protection et des politiques adaptées au XXI^{e} siècle.

À plus d'un titre, l'étude du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique insiste sur le fait que le gouvernement et les dirigeants de l'industrie doivent s'attaquer au problème grandissant du vol d'identité. C'est dans cet esprit que le NPD fait les recommandations complémentaires sensées suivantes :

Première recommandation complémentaire : Le NPD exhorte les fournisseurs de service Internet et les entreprises de technologie de l'information de faire état publiquement et annuellement de toutes les demandes de communication de renseignements personnels sur les abonnés émanant des organismes gouvernementaux. Leurs rapports devraient indiquer le nombre de demandes, le type de renseignements demandés et les réponses des fournisseurs de service Internet.

Au cours de leur témoignage respectif, les représentants de Rogers et de Google ont indiqué que leur entreprise s'était engagée à faire état publiquement du nombre de demandes de communication de renseignements personnels émanant des organismes gouvernementaux. Le NPD salue cette mesure positive. Il est d'avis que tous les fournisseurs de service Internet et toutes les entreprises de technologie de l'information devraient suivre leur exemple afin d'accroître la transparence relativement aux demandes de communication de renseignements personnels émanant des organismes gouvernementaux. Cette pratique aide les Canadiens à prendre des décisions éclairées et à comprendre les conséquences découlant d'un usage éventuel de leurs renseignements personnels.

Deuxième recommandation complémentaire : Le NPD recommande que le gouvernement publie un rapport annuel indiquant le nombre de demandes de communication de renseignements personnels sur les abonnés présentées aux fournisseurs de service Internet. Les rapports devraient indiquer les demandes, ventilées par organisme gouvernemental, le type de renseignements demandés et l'issue de la demande.
Comme l'ont suggéré les représentants de Rogers au cours de leur témoignage, les organismes gouvernementaux doivent eux aussi faire leur part pour mettre en évidence les millions de demandes qu'envoient chaque année les organismes gouvernementaux aux fournisseurs de service Internet. Le NPD est d'avis que les Canadiens ont le droit d'être au courant des demandes de renseignements personnels que fait le gouvernement à leur endroit. Sur ce plan, il est indispensable d'accroître la transparence.

Troisième recommandation complémentaire : Le NPD recommande que le gouvernement du Canada élabore une stratégie ciblée visant à réduire la fréquence des vols d'identité dans les collectivités des Premières Nations.
Le témoignage de Forest Green devant le Comité est on ne peut plus clair : les Premières Nations sont particulièrement vulnérables au vol d'identité. Le NPD est d'avis que cette vulnérabilité particulière nécessite une stratégie ciblée, car une stratégie globale de lutte contre le vol d'identité répondrait mal aux réalités propres aux collectivités des Premières Nations.

Quatrième recommandation complémentaire : Le NPD recommande que l'Agence du revenu du Canada élabore des lignes directrices concernant l'utilisation des numéros d'assurance sociale par des organismes privés.
À l'heure actuelle, aucune loi n'empêche les organismes privés de demander aux Canadiens leur numéro d'assurance sociale (NAS) à des fins autres que celles liées à l'emploi ou aux impôts. Ce vide politique ouvre la porte à une utilisation abusive des NAS qui est susceptible de causer le vol d'identité.

Cinquième recommandation complémentaire : Le NPD recommande que le gouvernement du Canada envisage des moyens par lesquels il pourrait autoriser les organismes privés à vérifier l'authenticité des cartes d'identité délivrées par les autorités publiques.
Dans leur témoignage, les représentants de TransUnion ont indiqué que les organismes privés n'ont aucun moyen de vérifier l'authenticité des cartes d'identité délivrées par les autorités publiques. La résolution de ce problème contribuera à réduire le recours à des cartes d'identité contrefaites et, par conséquent, à diminuer la fréquence des vols d'identité.

Sixième recommandation complémentaire : Le Comité exhorte les agences d'évaluation du crédit à offrir aux consommateurs un gel de leur crédit.
Comme l'a souligné Philippa Lawson lors de son témoignage, les agences d'évaluation du crédit canadiennes n'offrent pas aux consommateurs la possibilité de geler leur crédit. Une telle pratique les empêcherait de communiquer les antécédents de crédit

d'un client. Les néo-démocrates croient qu'un tel service préviendrait un grand nombre de vols d'identité.

Septième recommandation complémentaire : Le NPD recommande que le gouvernement du Canada modifie la *Loi sur la protection des renseignements personnels* de façon à fixer des exigences en matière de déclaration d'atteinte à l'intégrité des données pour l'ensemble des organismes gouvernementaux.
Si les fuites de données ne sont pas signalées, les Canadiens ne peuvent pas prendre les mesures nécessaires pour se prémunir contre le vol d'identité. En refusant de modifier la *Loi sur la protection des renseignements personnels* de façon à contraindre les ministères à faire état des atteintes à la protection des données, le gouvernement refuse de munir les Canadiens des outils dont ils ont besoin pour se protéger.

Huitième recommandation complémentaire : Le NPD recommande que le gouvernement du Canada habilite le commissaire à la protection de la vie privée à rendre des ordonnances afin d'assurer le respect des lois canadiennes en matière de protection des renseignements personnels, telles que la LPRPDE et la *Loi sur la protection des renseignements personnels*.
Le gouvernement doit donner au commissaire à la protection de la vie privée les outils dont il a besoin pour protéger les renseignements personnels des Canadiens. Malheureusement, le refus du gouvernement d'adapter nos lois sur la protection des renseignements personnels aux réalités du XXI^{e} siècle compromet la protection des renseignements personnels des Canadiens dans l'économie mondiale d'aujourd'hui.

Les recommandations sensées du présent rapport complémentaire soulignent l'appui du NPD à l'égard de mesures qui mettront un terme au problème croissant du vol d'identité et mettront en place un plan exhaustif pour surmonter ce problème.