Le crime contre l'identité : Évaluation de la menace

Rapport pour l'Attorney General des États-Unis et le ministre de la Sécurité publique du Canada

Novembre 2010

Table des matières

Résumé

Dans les dix dernières années, le crime contre l'identité – qu'on appelle parfois « vol d'identité » ou « fraude d'identité » – s'est répandu au point de devenir un problème majeur non seulement en Amérique du Nord, mais dans le monde entier.

En 2003, le Forum sur la criminalité transfrontalière a commandé à son sous-groupe de la fraude par marketing de masse une évaluation de cette menace[1]. En 2008, voyant que le crime contre l'identité continuait de se répandre, il a demandé au sous-groupe de mettre l'évaluation à jour.

La présente évaluation de la menace se concentre sur cinq aspects du crime contre l'identité tel qu'il touche le Canada et les États-Unis : (1) sa portée et son étendue; (2) ses visées; (3) les catégories de personnes qui le commettent ou qui en sont victimes; (4) ses méthodes et ses techniques; (5) les façons d'y répondre. L'évaluation a pour but d'isoler et de décrire les traits les plus problématiques du crime contre l'identité, ainsi que les méthodes que les deux pays emploient pour le combattre.

Chaque année, le crime contre l'identité, sous une forme ou une autre, frappe une part non négligeable des populations américaine et canadienne. Le caractère vulnérable ou peu sécuritaire de beaucoup de modes de paiement et de pièces d'identité demeure parmi les obstacles qui le rendent difficile à combattre. Les criminels et les organisations criminelles le pratiquent abondamment : fraude, obtention illicite de biens, de services ou d'avantages aux dépens du secteur public ou privé, etc.

Les particuliers, aussi bien que les secteurs public et privé, peuvent faire beaucoup pour combattre le crime contre l'identité, et pour en réduire le risque. Chaque pays devrait non seulement se doter d'outils législatifs utiles et efficaces pour les enquêtes et les poursuites, mais aussi éduquer sa population et lui offrir des mécanismes pour reprendre le dessus ou pour obtenir de l'aide après avoir été fraudée.

D'année en année, le vol d'identité et les personnes et organisations qui le commettent se complexifient, devenant capables de s'adapter rapidement selon l'évolution des circonstances. Les gouvernements (tout particulièrement les forces de l'ordre) et les entités du secteur privé dans les deux pays doivent tenir le rythme. À l'heure où le vol d'identité occasionne chaque année des pertes pour les particuliers, pour les entreprises et pour les gouvernements qui se chiffrent – en comptant les dégâts pour la réputation et les coûts pour réparer ou rétablir les identités volées – en dizaines de milliards de dollars, les secteurs public et privé ne manquent pas de raisons pour travailler ensemble et pour tendre la main à leurs homologues étrangers afin d'enrayer ce problème.

[1] *Voir* Groupe de travail binational sur les fraudes transfrontalières par marketing de masse, Rapport sur le vol d'identité : rapport présenté à la ministre de la Sécurité publique et de la Protection civile du Canada et à l'Attorney General des États-Unis (octobre 2004), *disponible au* http://www.securitepublique.gc.ca/prg/le/bs/report-fra.aspx.

Introduction

Dans les dix dernières années, le crime contre l'identité – qu'on appelle parfois « vol d'identité » ou « fraude d'identité » – s'est répandu au point de devenir un problème majeur non seulement en Amérique du Nord, mais dans le monde entier. En 2003, le Forum sur la criminalité transfrontalière a commandé à son sous-groupe de la fraude par marketing de masse une évaluation de cette menace[2]. En 2008, voyant que le crime contre l'identité continuait de se répandre, au Canada et aux États-Unis comme ailleurs, il a demandé au sous-groupe de mettre l'évaluation à jour.

La présente évaluation de la menace se concentre sur cinq aspects du crime contre l'identité tel qu'il touche le Canada et les États-Unis : (1) sa portée et son étendue, y compris ses conséquences pour les particuliers, pour les entreprises et pour les gouvernements; (2) ses visées; (3) les catégories de personnes qui le commettent ou qui en sont victimes; (4) ses méthodes et ses techniques; (5) les façons dont les secteurs public et privé y répondent. L'évaluation a pour but d'isoler et de décrire les traits les plus problématiques du crime contre l'identité, ainsi que les méthodes qu'emploient les forces de l'ordre, les gouvernements et les sociétés privées des deux pays pour le combattre.

Définir le crime contre l'identité

Régulièrement au cours de l'Histoire, des criminels ont cherché à s'arroger l'identité d'autrui et à s'en servir pour obtenir des avantages auxquels ils n'avaient pas droit. Cette pratique, en plus de cacher la véritable identité du contrevenant, peut amener les forces de l'ordre à prendre la victime pour le criminel.

À la fin des années 90, le mésusage des cartes de crédit et autres modes de paiement à distance à des fins criminelles a crû avec leur popularité; les gouvernements, le public et les médias américains se sont mis à parler de « vol d'identité »[3]. Si au Canada comme aux États-Unis ce terme fait maintenant partie du langage courant[4], on emploie aussi « fraude d'identité » pour désigner différents aspects du problème[5]. Attention toutefois, les deux vocables ne sont pas

---

[2] *Voir* Groupe de travail binational sur les fraudes transfrontalières par marketing de masse, Rapport sur le vol d'identité : rapport présenté à la ministre de la Sécurité publique et de la Protection civile du Canada et à l'Attorney General des États-Unis (octobre 2004), *disponible au* http://www.securitepublique.gc.ca/prg/le/bs/report-fra.aspx.

[3] *Voir*, *e.g.*, Identity Theft and Assumption Deterrence Act of 1998, Pub. L. (30 octobre 1998), *codified*, 18 U.S.C. 1028(a)(7).

[4] *Voir*, *p. ex*, Ministère de la Justice Canada, Communiqué (8 janvier 2010) (rapport médiatique sur l'adoption du projet de loi S-4), *disponible au* http://www.justice.gc.ca/fra/nouv-news/cp-nr/2010/doc_32470.html ; Federal Trade Commission, Identity Theft, *disponible au* http://www.ftc.gov/bcp/edu/microsites/idtheft/.

[5] *Voir, p. ex.* Australian Institute of Criminology, Identity fraud, *disponible au* http://www.aic.gov.au/crime_types/economic/idfraud.aspx; CIFAS, Identity Fraud, *disponible au* http://www.cifas.org.uk/default.asp?edit_idem=566-56; Directgov, Identity fraud, *disponible au* http://www.direct.gov.uk/en/CrimeJusticeAndTheLaw/Typesofcrime/DG_174616; Gendarmerie royale du Canada,

synonymes. Les définitions populaires et juridiques du vol d'identité tendent à mettre l'accent sur l'abus de l'identité de personnes réelles. Or, depuis quelques années, les autorités observent un recours accru aux identités synthétiques – c'est-à-dire à des données apocryphes n'ayant rien à voir avec qui que ce soit de réel – pour la fraude. De plus, « fraude d'identité » désigne parfois l'ensemble des fraudes impliquant l'usage malveillant d'identités réelles ou synthétiques. Finalement, depuis janvier 2010, le droit canadien définit le vol d'identité comme la possession, le commerce ou l'utilisation illégaux de données personnelles, et la fraude d'identité comme l'usage frauduleux de l'identité d'autrui pour obtenir des avantages, se procurer des biens, désavantager quelqu'un, éviter l'arrestation ou entraver le cours de la justice[6].

Par souci d'uniformité, le terme « crime contre l'identité » englobera le vol d'identité et la fraude d'identité (dans leurs acceptions juridique et pratique) dans toute la présente évaluation de la menace. Son équivalent anglais, « identity-related crime », les englobe d'ailleurs dans les travaux de plusieurs instances internationales s'occupant d'exécution de la loi, comme le groupe des ministres de la Justice et des Affaires intérieures du G8[7] et le Core Group of Experts on Identity-Related Crime[8] du United Nations Office on Drugs and Crime.

I. La portée et l'étendue du crime contre l'identité

Le crime contre l'identité, dont nous allons faire plus loin une description plus exhaustive, peut se définir comme un cycle en cinq phases : (1) acquisition illicite ou non autorisée de renseignements personnels ou de pièces d'identité (cartes, autres documents, etc.); (2) transfert de ceux-ci; (3) manipulation des données ou des articles (modification, compilation, contrefaçon, etc.); (4) transfert des données ou des articles manipulés; (5) utilisation des données ou des articles par un criminel qui souhaite commettre une fraude ou cacher sa propre identité[9].

À ce jour, les gouvernements canadien et américain n'ont que très peu étudié la portée et l'étendue du crime contre l'identité en Amérique du Nord. Aux États-Unis, le Bureau of Justice Statistics (BJS) du département de la Justice recueille depuis 2004 des données nationales sur les

---

Vol d'identité et fraude d'identité, *disponible au* http://www.rcmp-grc.gc.ca/scams-fraudes/idem-theft-vol-fra.htm); U.S. Department of Justice, Identity Theft and Identity Fraud, *disponible au* http://www.justice.gov/criminal/fraud/websites/idtheft.html.

[6] *Voir* Projet de loi S-4, Loi modifiant le Code criminel (vol d'identité et inconduites connexes) *disponible à* http://www.justice.gc.ca/fra/nouv-news/cp-nr/2010/doc_32471.html.

[7] *Voir* G8 Justice and Home Affairs Ministerial Meeting – Concluding Declaration (13 juin 2008), *disponible au* http://g8.gc.ca/about/past-summits/ministerial-meetings-2008/justice-home-affairs/.

[8] *Voir, p. ex.* United Nations Commission on Crime Prevention and Criminal Justice, Third meeting of the Core Group of Experts on Identity-Related Crime (Vienne, Autriche, 20-22 janvier 2009), *disponible au* http://www.unodc.org/documents/treaties/organized_crime/ECN152009_CRP12.pdf.

[9] *Voir* Criminal and Legal Affairs Subgroup, G8 Lyon-Roma Anti-Crime and Terrorism Group, Essential Elements of Criminal Laws to Address Identity-Related Crime (février 2009) (Annexe).

ménages victimes de vols d'identité[10]. La Federal Trade Commission a fait mener deux sondages nationaux sur le vol d'identité, en 2003 et en 2006 respectivement, auprès d'un échantillon aléatoire composé d'Américains adultes (18 ans et plus)[11]. Plus récemment, en appliquant une méthodologie de la Federal Trade Commission, la firme Javelin Strategy & Research a établi qu'en 2009, 11,1 millions d'Américains adultes (soit 4,81 % de la population totale) avaient été victimes d'une fraude quelconque d'identité, les pertes totales (personnes physiques et morales confondues) se chiffrant à 54 G$US[12]. En chiffres absolus comme en pourcentage de la population, les victimes n'avaient jamais été aussi nombreuses depuis le premier sondage annuel de Javelin sur le sujet en 2003[13].Un sondage mené en 2008 par l'Université McMaster auprès des consommateurs canadiens a révélé que 1,7 million de personnes (6,5 % de la population) avaient été victimes d'une fraude d'identité dans la dernière année[14].

En examinant les plaintes des consommateurs dans les deux pays, on peut apprécier mieux encore la portée et l'étendue du problème. En 2009, 278 078 des plaintes de consommateurs pour fraude reçues par la Federal Trade Commission (FTC) des États-Unis portaient sur des vols d'identité – cette catégorie remportait la palme, et de loin (21 %). Le chiffre était inférieur à celui de 2008 (314 484), mais supérieur à celui de 2007 (259 314)[15]. Le Centre antifraude du Canada (CAFC), anciennement le projet PhoneBusters, est une opération conjointe de la Gendarmerie royale du Canada (GRC), du Bureau de la concurrence Canada et de la Police provinciale de l'Ontario; il a annoncé avoir reçu en 2009 11 979 plaintes pour vol d'identité, mettant en jeu 11 909 victimes. Encore une fois, les chiffres étaient inférieurs à ceux de 2008 (12 232 plaintes et 11 463 victimes), mais supérieurs à ceux de 2007 (10 637 plaintes et 10 328 victimes)[16]. Selon

---

[10] *Voir* Bureau of Justice Statistics, Identity Theft Reported by Households, 2007- Statistical Tables (le 30 juin 2010), *disponible au* http://bjs.ojp.usdoj.gov/content/pub/pdf/itrh07st.pdf. En 2008, le BJS a aussi recueilli des données nationales sur le nombre de vols d'identité, le coût de ceux-ci et la réponse des victimes. Il a interrogé un échantillon représentatif de répondants ayant 16 ans et plus. Les résultats sont attendus pour la fin de 2010.

[11] *Voir* Federal Trade Commission, 2006 Identity Theft Survey Report (novembre 2007), *disponible au* http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf.

[12] Voir JAVELIN STRATEGY & RESEARCH, 2010 IDENTITY FRAUD SURVEY REPORT, 7 (février 2010).

[13] *Voir idem.*, 8.

[14] *Voir* Susan Sproule et Norm Archer, Measuring Identity Theft in Canada: 2008 Consumer Survey - Working Paper #23, *disponible au* http://www.merc-mcmaster.ca/working-papers/measuring-identity-theft-in-canada-2008-consumer-survey/.

[15] Voir FEDERAL TRADE COMM'N, CONSUMER SENTINEL DATA BOOK FOR JANUARY – DECEMBER 2009, 4-5 (février 2010), *disponible au* http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2009.pdf.

[16] *Voir* GROUPE DE L'ANALYSE DES RENSEIGNEMENTS CRIMINELS DU CENTRE ANTIFRAUDE DU CANADA, RAPPORT STATISTIQUE ANNUEL 2009 ACTIVITÉS DE FRAUDE EN MARKETING DE MASSE ET DE VOL D'IDENTITÉ http://www.phonebusters.com/francais/documents/AnnualStatisticalReport2009fr_000.pdf.

le CAFC, les victimes auraient déclaré des pertes de presque 10,9 M$CAN – donc supérieures à celles de 2008 (plus de 9,6 M$CAN) et de 2007 (presque 6,5 M$CAN)[17].

Certaines données portent à croire que les pertes directes (bancaires et financières à long terme, etc.) imputables aux fraudes d'identité vont en diminuant pour les consommateurs. Javelin écrit dans son rapport que le coût moyen de la fraude d'identité pour chaque consommateur a chuté brusquement de 2008 à 2009, passant de 498 à 373 $, une baisse de 25 %[18]. Elle en induit que [traduction] « l'industrie [financière] absorbe une plus grande portion des pertes pour épargner les consommateurs. Par exemple, la feuille de pointage de Javelin est éloquente : en 2009, elle a révélé que pour la première fois, 100 % des 25 grandes institutions financières sondées accompagnaient leurs cartes débit d'une garantie de responsabilité nulle en cas de fraude[19] ».

Or, les pertes financières directes sont souvent moins graves pour les victimes que les problèmes indirects découlant de l'utilisation, par les voleurs d'identité, de leurs renseignements personnels pour obtenir des biens, des services, ou alors des avantages publics ou privés. Toujours selon le rapport Javelin, aux États-Unis en 2007, les ouvertures de comptes frauduleuses (c'est-à-dire l'exploitation des renseignements d'une victime pour obtenir de nouvelles cartes de paiement, ouvrir de nouveaux comptes bancaires ou contracter des prêts) avait augmenté de 38 % ou 6 G$US, ce qui en faisait [traduction] « le principal facteur de croissance de la fraude en valeur absolue[20] ». Si l'ouverture de comptes frauduleuse n'enlève rien dans les comptes légitimes des victimes, elle implique en revanche une mauvaise utilisation des renseignements personnels, à la suite de laquelle des prêteurs ou d'autres entreprises pourraient prendre des décisions préjudiciables à la victime, lui refusant des crédits et ternissant sa réputation.

En outre, il semble que les victimes de fraudes contre l'identité aient à assumer plus que leur juste part des coûts et des efforts pour rétablir leur réputation et leur cote de crédit. Au Canada, un sondage de l'Université McMaster nous révèle qu'en 2008, les victimes de fraudes contre l'identité ont dépensé 150 M$CAN à même leur avoir personnel et consacré 20 millions d'heures à réparer les dégâts des fraudes commises dans la dernière année[21]. Aux États-Unis, selon le sondage 2010 de Javelin cette fois, la moyenne se serait élevée en 2009 à 373 $ et à 21 heures par victime[22].

---

[17] *Voir idem.*

[18] *Voir* JAVELIN STRATEGY & RESEARCH, *supra* note 12, 8.

[19] *Idem*.

[20] *Idem.*, 10.

[21] *Voir* Canwest News Service, *Identity theft plagues Canadians as online shopping grows*, Canada.com, 18 septembre 2008, *disponible au* http://www.canada.com/story.html?idem=b7f81191-421a-48f5-abc3-8b156c8f6fc2.

[22] *Voir* JAVELIN STRATEGY & RESEARCH, *supra* note 12, 7.

II. Les visées du crime contre l'identité

A. Fraude

Les criminels s'adonnent au crime contre l'identité avant tout pour commettre des fraudes, c'est-à-dire pour se servir d'identités synthétiques ou de l'identité véritable d'autrui afin de s'enrichir en obtenant illégitimement des biens, des services ou des avantages auprès des secteurs public et privé. Les plaintes déposées au Canada comme aux États-Unis montrent que le crime contre l'identité donne lieu à des fraudes très diverses.

Le CAFC nous dit qu'au Canada en 2009, les voleurs d'identité ont exploité des renseignements personnels pour obtenir des avantages bancaires et financiers (comptes bancaires, prise de contrôle, argent comptant, chèques, cartes de crédit, demandes de comptes frauduleuses, marges de crédit, prêts et hypothèques), des avantages des secteurs public et privé (permis de conduire, cartes santé, assurances, passeports et acheminement du courrier), des emplois, de la marchandise et des services de téléphonie (cellulaires, demandes frauduleuses de téléphones cellulaires, numéros de téléphone[23]). Javelin a fait des constatations similaires aux États-Unis : selon elle, les voleurs d'identité auraient commis des fraudes par carte (76 %), en matière de téléphonie ou de services publics (11 %), bancaires (14 %), liées à Internet ou aux comptes centralisateurs (15 %), liées aux prêts (7 %), ainsi que d'autres types de fraude (4 %) : prestations du gouvernement, services médicaux, emploi, etc.[24].

B. Dissimulation de l'identité

Or, le crime contre l'identité rapporte aussi à ses auteurs des avantages non pécuniaires appréciables. Ainsi, certains criminels utilisent des papiers d'identité volés ou obtenus frauduleusement pour faciliter leurs déplacements pendant ou après leurs délits; d'autres compliquent délibérément les enquêtes des autorités en impliquant plusieurs districts judiciaires.

- En 2008, un citoyen canadien a tenté d'entrer aux États-Unis depuis le Canada; or l'inspection a révélé qu'il portait sur lui huit fausses cartes de crédit (dont les numéros avaient été volés au Canada) et un faux permis de conduire québécois. Après avoir admis qu'il avait eu l'intention d'utiliser les fausses cartes aux États-Unis, il a plaidé coupable en

[23] *Voir* GROUPE DE L'ANALYSE DES RENSEIGNEMENTS CRIMINELS DU CENTRE ANTIFRAUDE DU CANADA, *supra* note 16, 24.

[24] *Voir* JAVELIN STRATEGY & RESEARCH, *supra* notes 12, 12, 29, 35 et 39. Ces pourcentages portent sur tous les comptes, les nouveaux comme les autres.

cour fédérale américaine à des accusations de vol d'identité, pour finalement recevoir sa sentence[25].

- En 2009, un individu s'est caché derrière le nom et le grade d'un officier dans l'équipe de démonstration des Snowbirds, 431e escadron, pour échafauder une escroquerie en ligne où il prétendait vendre une voiture depuis le Royaume-Uni[26].

- En 2010, la cour fédérale américaine a accusé trois Bulgares, dont deux habitaient Toronto, d'utilisation de fausses cartes de guichet bancaire, de fraude bancaire et de vol d'identité avec circonstances aggravantes relativement à un écrémage où ils auraient compromis de nombreux guichets automatiques dans tout l'Est du Massachusetts, volant plus de 120 000 $[27].

D'autres encore utilisent consciemment l'identité d'autrui pour abuser de comptes financiers ou pour toucher des avantages de l'État sous le nom de leurs victimes, aiguillant les autorités policières et judiciaires sur de fausses pistes.

- En 2002, une Floridienne a été arrêtée et placée en détention en vertu d'un mandat d'arrêt pour vol de voiture. Il s'est toutefois avéré qu'une autre femme, qui avait séjourné quatre fois dans les pénitenciers de Floride, avait volé la voiture sous l'identité de sa victime, donnant le nom de cette dernière à son arrestation. Elle a conservé ce nom pendant sa mise en accusation pour vol de voiture, qu'elle n'a aucunement contestée, pour finalement se retrouver sous probation pendant trois ans. Même son agent de probation la connaissait sous sa fausse identité. Or, le jour de l'arrestation, la véritable voleuse purgeait une peine de huit ans en Floride pour une série de délits. La victime, qui lui ressemblait à certains égards, a été relâchée moins d'une journée après son arrestation par erreur[28].

- En 2006, un homme s'est fait accuser de vol à l'étalage dans un Wal-Mart près de Carbonear (Terre-Neuve), bien qu'il n'eût jamais visité ni le magasin ni la ville. Il a obtenu le retrait des accusations après avoir dit à la police et aux médias qu'on lui avait volé son portefeuille plusieurs mois auparavant, lors d'une entrée par effraction au

---

[25] *Voir* U.S. Attorney's Office, Northern District of New York, communiqué de presse (4 janvier 2010), *disponible au* http://www.justice.gov/usao/nyn/NewsReleases/Attachments/144-129-1731359488.pdf.

[26] *Voir* Stephen Pate, *Canadian Snowbirds victim of identity theft in car scam*, NJN Network, 26 juin 2009, *disponible au* http://njnnetwork.com/2009/06/exclusive-canadian-snowbirds-victim-of-identity-theft-in-car-scam/.

[27] *Voir* U.S. Attorney's Office, District of Massachusetts, communiqué de presse (24 janvier 2010), *disponible au* http://www.justice.gov/usao/ma/Press%20Office%20-%20Press%20Release%20Files/Feb2010/IndictmentPR.html.

[28] *Voir* Rene Stutzman, *Innocent woman sues after identity theft leads to jailing, strip search*, Palm Beach Post, 7 septembre 2010, *disponible au* http://www.palmbeachpost.com/news/crime/innocent-woman-sues-after-identity-theft-leads-to-900829.html.

restaurant où il travaillait. En revanche, l'arrestation lui a valu de se retrouver sur une liste de personnes interdites de vol[29].

C. Appui à des organisations criminelles

1. Crime organisé

Bien que tous les crimes contre l'identité ne soient pas imputables aux organisations criminelles – en réalité, beaucoup sont le fait de personnes isolées ou de petits groupes avec peu de cohésion[30] –, il faut reconnaître que ces dernières jouent un rôle non négligeable dans le vol d'identité et dans la fraude d'identité. Extrait du *Rapport sur le crime organisé* de 2010, produit par le Service canadien de renseignements criminels (SCRC) :

> Les groupes du crime organisé produisent, vendent et utilisent de fausses identités. L'abondance de données personnelles et commerciales en ligne en facilite énormément le vol et l'exploitation. Les criminels organisés privilégient trois méthodes : modification d'un aspect de leur propre identité; création de toute pièce d'une identité; vol de l'identité d'une personne, vivante ou décédée. Grâce à ces fausses identités, les criminels peuvent se soustraire à la détection par la police, surtout dans leurs déplacements, ou protéger leurs biens contre la confiscation. Ils utilisent également de fausses identités pour exécuter ou faciliter des activités criminelles où des preuves d'identité sont nécessaires, dont la fraude, les crimes financiers ou la traite de personnes. Ils peuvent aussi recourir à d'autres moyens de représentation frauduleuse, entre autres, de faux renseignements sur une entreprise, un véhicule, une consignation, des comptes commerciaux ou des transactions[31].

---

[29] *Voir St. John's identity theft victim faces new frustrations*, CBC, 25 janvier 2010, *disponible au* http://www.cbc.ca/canada/newfoundland-labrador/story/2010/01/25/nl-theft-norman-012510.html.

[30] En 2005 par exemple, deux individus (ils étaient frère et sœur, et l'un d'eux venait du Nigéria) ont employé un stratagème élaboré consistant à obtenir frauduleusement des renseignements personnels auprès d'entreprises comme ChoicePoint Service pour voler leur identité à des centaines de victimes. La sœur se faisait passer pour une agente immobilière afin de pouvoir ouvrir des comptes auprès de firmes tenant des registres publics en bases de données, obtenant de ce fait des renseignements personnels sur des milliers de personnes. Elle revendait ensuite ces renseignements à son frère ainsi qu'à d'autres individus au pays, pour un prix variant entre 40 et 65 $. Aidé d'elle, son frère a ouvert à Beverly Hills et à Encino des « points de livraison » où il détournait le courrier envoyé par les compagnies de cartes de crédit des victimes. Sitôt les numéros de cartes en main, il s'empressait de faire des achats et d'obtenir des avances de fonds. *Voir* U.S. Attorney's Office, Central District of California, communiqué de presse (7 mars 2005), *disponible au* http://www.justice.gov/usao/cac/pressroom/pr2005/042.html.

[31] SERVICE CANADIEN DE RENSEIGNEMENTS CRIMINELS, RAPPORT SUR LE CRIME ORGANISÉ 2010, *disponible au* http://www.cisc.gc.ca/annual_reports/annual_report_2010/fundamentals1_2010_f.html.

Aux États-Unis, alors qu'il témoignait devant le Congrès en 2009, un représentant du département de la Justice a cité l'implication des groupes criminels, en sol américain comme ailleurs, parmi les principales causes de l'explosion récente des crimes contre l'identité[32]. Dans ce pays, les organisations criminelles ne se limitent plus au vol d'identité et aux fraudes par carte de paiement; elles se sont lancées dans la fraude en soins de santé, volant l'identité de médecins pour des facturations frauduleuses à grande échelle[33]. De surcroît, dans une évaluation internationale de la menace posée par la fraude par marketing de masse (2010), on peut lire : [traduction] « les enquêtes policières au Canada et aux États-Unis ont aussi mis au jour des entreprises criminelles virtuelles dont les membres sont répartis dans le monde entier et, bien qu'ils communiquent exclusivement par des tribunes en ligne, s'adonnent à des escroqueries et à des vols d'identité organisés[34]. »

2. Terrorisme

Le recours à la fraude contre l'identité pour financer le terrorisme reste une préoccupation de taille pour les autorités des deux pays[35]. En 2007 par exemple, trois Britanniques se sont vu infliger des peines variant entre 6,5 et 10 ans de prison après avoir plaidé coupable à des accusations selon lesquelles ils avaient recouru à l'hameçonnage[36], à des virus informatiques et à

---

[32] *Voir* Statement of Jason M. Weinstein, Deputy Assistant Attorney General, Criminal Division, U.S. Dep't of Justice, Before the Subcommittee on Oversight and Information Policy, Census and National Archives of the House of Representatives Committee on Oversight and Government Reform (17 juin 2009), *disponible au* http://www.justice.gov/criminal/pr/speeches-testimony/documents/06-17-2009weinstein.pdf.

[33] *Voir* Allan Chernoff et Sheila Steffen, *Organized crime's new target: Medicare*, CNN, 24 octobre 2009, *disponible au* http://www.cnn.com/2009/CRIME/10/22/medicare.organized.crime/.

[34] INTERNATIONAL MASS-MARKETING FRAUD WORKING GROUP, MASS-MARKETING FRAUD: A THREAT ASSESSMENT, (16 juin 2010), *disponible au* http://www.stopfraud.gov/news/immfta.pdf.

[35] *Voir, e.g.,* Gendarmerie royale du Canada, *Vol d'identité et fraude d'identité, disponible au* http://www.rcmp-grc.gc.ca/scams-fraudes/idem-theft-vol-fra.htm.

[36] Le Anti-Phishing Working Group, coalition interne d'organismes gouvernementaux et d'entreprises dédiée à la lutte contre la fraude et le vol d'identité en ligne, définit l'hameçonnage comme suit :

> [Traduction]
> « Mécanisme criminel combinant ingénierie sociale et subterfuges techniques pour voler les renseignements personnels et financiers des consommateurs. L'ingénierie sociale consiste à envoyer des courriels trompeurs sous le nom d'une entreprise ou d'un organisme légitime pour diriger les consommateurs vers des sites Web factices où ils seront invités à divulguer des renseignements financiers : noms d'utilisateur, mots de passe, etc. Quant aux subterfuges techniques, ils consistent à installer des maliciels sur les ordinateurs personnels pour voler les données financières directement, souvent en interceptant les noms d'utilisateur et les mots de passe, ou en corrompant les structures de navigation locales pour diriger les consommateurs vers des sites Web factices (ou alors vers des sites authentiques via des mandataires contrôlés par l'hameçonneur, qui surveillent et interceptent les frappes).

des cartes de crédit volées pour tisser un réseau de tribunes en ligne et de sites Web [traduction] « où l'on trouvait de tout, des guides pratiques pour le piratage informatique jusqu'aux vidéos de décapitations et d'attentats-suicides survenus en Irak[37] ». Plus récemment, en 2009, une Californienne qui dirigeait une compagnie d'immatriculation de véhicules a été accusée par les autorités locales et fédérales d'exploiter un vaste réseau de fraude impliquant plusieurs employés du département des Véhicules moteurs qu'elle soudoyait régulièrement pour qu'ils produisent des permis, entre autres documents. Et selon un agent de police, le nom d'au moins un de ses clients aurait circulé dans des enquêtes en cours relatives à la sécurité nationale[38].

III. Auteurs et victimes du crime contre l'identité

Dans le domaine des crimes contre l'identité, il n'existe pas d'auteur ni de victime type. Les auteurs vont du délinquant primaire au criminel de carrière. Quant aux victimes, elles vont du nouveau-né (à qui ses parents, par exemple, auront volé son numéro de sécurité sociale (États-Unis) ou son numéro d'assurance sociale (Canada)) à l'aîné. Contrairement à certains types de fraude qui visent un groupe d'âge ou un groupe ethnique en particulier, le crime contre l'identité touche tous les segments démographiques. Le rapport de sondage sur la fraude publié en 2010 par Javelin porte qu'en 2009, 3,2 % des personnes âgées entre 18 et 24 ans ont été victimes de vol d'identité, contre 5,9 % dans la tranche des 25 à 34 ans, 5,3 % dans la tranche des 35 à 44 ans, 6,2 % dans celle des 45 à 54 ans, 4,3 % dans celle des 55 à 64 ans et 2,9 % dans celle des 65 ans et plus[39]. Quant aux données du CAFC, elles se ventilent comme suit : les 19 ans et moins ont été victimes d'à peine 2 % des fraudes contre l'identité, contre 17 % pour les gens dans la vingtaine, 22 % pour ceux dans la trentaine, 25 % pour ceux dans la quarantaine, 18 % pour ceux dans la cinquantaine, 10 % pour ceux dans la soixantaine et environ 7 % pour les 70 ans et plus[40].

De surcroît, le crime contre l'identité cible les entreprises aussi bien que les particuliers. Pour crédibiliser leurs escroqueries, certains criminels n'hésitent pas à utiliser des noms et des numéros de comptes d'entreprises. Ainsi, des fraudes par frais d'emprunt payables à l'avance dans le monde entier fonctionnent de la façon suivante : les fraudeurs présentent de faux chèques à leurs victimes pour les convaincre qu'elles ont gagné un tirage, gagné à la loterie, ou reçu le

---

ANTI-PHISHING WORKING GROUP, PHISHING ACTIVITY TRENDS REPORT: 4TH QUARTER 2009, 2 (2010), *disponible au* http://www.antiphishing.com/reports/apwg_report_Q4_2009.pdf.

[37] Brian Krebs, *Terrorism's Hook Into Your Inbox*, Washington Post, 5 juillet 2007, *disponible au* http://www.washingtonpost.com/wp-dyn/content/article/2007/07/05/AR2007070501153.html. *Voir* Nicola Woolcock, *Three students jailed for inciting terrorism on 'Holy War' websites*, The Times, 6 juillet 2007, *disponible au* http://www.timesonline.co.uk/tol/news/uk/crime/article2034011.ece.

[38] *Voir* Joel Rubin, *Counter-terrorism investigators find alleged identity theft ring*, Los Angeles Times, 26 juillet 2009, *disponible au* http://articles.latimes.com/2009/jul/26/local/me-fraud26.

[39] *Voir* JAVELIN STRATEGY & RESEARCH, *supra* note 12, 73,

[40] Ce renseignement est une gracieuseté du Centre antifraude du Canada.

paiement pour une vente en ligne.[41] Les chèques sont contrefaits, mais ils portent souvent le nom, l'adresse et le numéro de compte d'entreprises légitimes. S'ils portaient plutôt le nom et le numéro de compte de personnes réelles, nul doute que ce mésusage de renseignements personnels serait punissable en tant que vol d'identité en vertu des lois en vigueur dans plusieurs pays.

IV. Méthodes et techniques du crime contre l'identité

Le rapport du groupe de Rome-Lyon du G8 sur les éléments de droit essentiels pour enrayer le crime contre l'identité définit celui-ci comme un cycle à cinq phases : (1) acquisition illicite ou non autorisée de renseignements personnels ou de pièces d'identité (cartes, autres documents, etc.); (2) transfert de ceux-ci; (3) manipulation des données ou des articles (modification, compilation, contrefaçon, etc.); (4) transfert des données ou des articles manipulés; (5) utilisation des données ou des articles par un criminel qui souhaite commettre une fraude ou cacher sa propre identité[42]. La présente section de l'évaluation de la menace va aborder brièvement chacune de ces phases.

A. Acquisition de renseignements personnels

Les crimes contre l'identité commencent toujours de la même façon : avant toute chose, des criminels acquièrent des renseignements personnels précieux. Ils ont différentes façons d'y parvenir; tout dépend de leur raffinement, de leurs aptitudes technologiques, ainsi que du mode de stockage et d'accessibilité des données. Certains cherchent à consulter illégitimement de vastes dépôts de renseignements personnels, ou à bâtir leurs propres dépôts pour ensuite revendre des renseignements à des fins criminelles. Ils peuvent faire appel à leurs aptitudes technologiques pour pirater des bases de données ou y accéder avec des antiprogrammes, ou bien faire de l'ingénierie sociale pour amener les gens à divulguer leurs propres renseignements ou se lier d'amitié avec des travailleurs d'entreprises ou des fonctionnaires ayant accès à de vastes dépôts de données. Finalement, ils peuvent combiner les deux méthodes. D'autres criminels moins doués se contenteront de méthodes plus élémentaires : entrées par effraction, vols à la tire, vol de courrier, persuasion pour amener les gens à divulguer leurs propres renseignements, etc. Voici quelques exemples récents :

- En 2010, un grand jury fédéral de St. Louis a porté contre un individu plusieurs chefs d'accusation liés à la fraude : vol de cartes de crédit et de cartes de débit dans des véhicules, modification du NIP et de l'adresse associés aux comptes, puis obtention de plus de 45 000 $ au moyen de retraits et d'avances de fonds par guichet automatique dans

---

[41] *Voir* INTERNATIONAL MASS-MARKETING FRAUD WORKING GROUP, *supra* note 34, à 4, 10.

[42] *Voir* Criminal and Legal Affairs Subgroup, G8 Lyon-Roma Anti-Crime and Terrorism Group, *supra* note 9, Annexe.

les comptes de sept personnes, et par l'achat de marchandises et de cartes-cadeaux. Selon la poursuite, l'accusé et ses complices auraient rôdé dans les stationnements lors d'événements publics majeurs, repérant les conducteurs qui laissaient des portefeuilles ou des sacs à main dans leur véhicule, puis attendant leur départ pour forcer les véhicules et y prendre cartes de crédit, cartes de débit et papiers d'identité avec numéros de sécurité sociale, tout en laissant les portefeuilles et les sacs à main intacts[43].

- En 2010, quelqu'un aurait volé dans un hôpital de Colombie-Britannique un ordinateur portable contenant des données sur plus de 600 patients : noms, dates de naissance, numéros de cartes santé, etc. Il semblerait que les données n'étaient protégées ni par chiffrement ni par mot de passe[44].

- En 2010, une cour fédérale d'Albany (État de New York) a condamné un individu à 70 mois de prison pour son implication dans un réseau de voleurs d'identité, après qu'il a plaidé coupable à des accusations de fraude par papiers d'identité, de fraude électronique et de vol d'identité avec circonstances aggravantes. Selon les documents judiciaires, l'individu se serait avoué chef d'équipe dans une opération de type « aveuglé-piqué-signé » (flip, bite and write) qui ciblait des vieilles dames dans les supermarchés. L'équipe commençait par se rendre dans un magasin, le plus souvent un supermarché, à proximité de commerces vendant de l'électronique : Best Buy, Circuit City, Sears, etc. Un complice distrayait la vieille dame (« aveuglé »), tandis que l'accusé lui volait ses cartes de crédit (« piqué »). Ensuite, l'accusé allait s'installer dans son véhicule à proximité; avec un ordinateur portable et une imprimante à pièces d'identité, il produisait une fausse pièce d'identité (permis de conduire, carte des forces armées, etc.). Finalement, l'accusé et son équipe achetaient des appareils électroniques coûteux, différents biens de consommation et des cartes cadeaux, signant le nom de la victime sur les reçus de cartes de crédit (« signé »).

- En 2010, un grand jury fédéral d'Atlanta a accusé deux individus d'avoir volé plus de 80 identités dans la région métropolitaine d'Atlanta pour ouvrir des comptes de cartes de crédit, contracter des prêts et ouvrir des comptes bancaires. Selon la poursuite, l'une des accusées aurait obtenu un emploi de factrice sous le nom d'une autre femme dont elle avait volé l'identité avant d'entrer aux États-Unis en 2004. Plus de 80 personnes habitant le long de son itinéraire ont déclaré que quelqu'un leur avait volé leur identité pour ouvrir des comptes financiers[45].

---

[43] *Voir* U.S. Attorney's Office, Eastern District of Missouri, communiqué de presse (19 août 2010), *disponible au* http://www.justice.gov/usao/moe/press_releases/archived_press_releases/2010_press_releases/august/parker_jerod.html.

[44] *Voir 600 B.C. patients' data in stolen laptop*, CBC News, 2 septembre 2010, *disponible au* http://www.cbc.ca/health/story/2010/09/02/bc-stolen-laptop-patient-data.html.

[45] *Voir* U.S. Attorney's Office, Northern District of Georgia, communiqué de presse (12 mai 2010), *disponible au* http://www.justice.gov/usao/gan/press/2010/05-12-10.pdf.

- En 2010, la Cour de justice de l'Ontario a rallongé la peine d'un détenu après que ce dernier a plaidé coupable à des accusations de fraude. Il avait eu l'intention de voler leurs renseignements personnels à plus de 1 400 codétenus, pour ensuite demander des remboursements de taxe sur les produits et services (TPS), amassant en quelques années plus ou moins 1,8 M$. Il aurait persuadé ses codétenus de le laisser faire leurs déclarations de TPS, pour qu'ils puissent toucher des remboursements. En réalité, l'accusé changeait l'adresse postale de ses victimes pour que lui et ses complices puissent produire les déclarations au nom des victimes, mais encaisser les chèques eux-mêmes[46].

B. Transfert des articles ou des données

Il est rare que les cartes, données ou documents sur lesquels un voleur d'identité vient de faire main basse puissent servir immédiatement. Selon la façon dont il entend profiter de son crime, le voleur d'identité peut soit rassembler les données et les articles pour ensuite les envoyer ailleurs physiquement, soit en extraire les éléments pertinents, qu'il enverra ensuite électroniquement. Ainsi, dans beaucoup de cas d'hameçonnage, les criminels installent sur les ordinateurs visés des codes qui non seulement enregistreront les frappes de grande valeur (noms d'utilisateur et mots de passe pour services bancaires en ligne, etc.), mais expédieront aussi l'information à une adresse électronique choisie par le criminel.

- En 2006, dans une cour fédérale à Richmond en Virginie, un accusé a plaidé coupable à des accusations de fraude informatique et de vol d'identité avec circonstances aggravantes. Dans sa déposition, il a expliqué comment il avait installé des espions de clavier sur les ordinateurs d'une université, puis recueilli dans plusieurs comptes de courriel les données envoyées par ces espions. Les données lui avaient ensuite permis d'accéder à plusieurs systèmes informatiques universitaires protégés par mot de passe, ainsi qu'aux boîtes de courriel d'autres étudiants et de membres du personnel[47].

C. Manipulation des articles ou des données transférées

Avant que les articles ou les données volées puissent leur servir, les criminels doivent souvent commencer par effectuer l'une des trois manipulations suivantes : (1) modification (p. ex. des renseignements de base ou de l'adresse sur un relevé de compte bancaire ou de carte de crédit, ou alors des données figurant sur des chèques ou sur des papiers d'identité); (2) compilation (p. ex. assemblage de données pour revente sur des sites de fraude aux cartes bancaires[48] ou collecte de

---

[46] *Voir* Tony Van Alphen, *Inmate earned thousands filing fake tax forms from prison*, Toronto Star, 16 septembre 2010, *disponible au* http://www.thestar.com/business/article/861943--inmate-earned-thousands-filing-fake-tax-forms-from-prison?bn=1.

[47] *Voir* U.S. Attorney's Office, Eastern District of Virginia, communiqué de presse (27 septembre 2006), *disponible au* http://www.justice.gov/usao/vae/Pressreleases/09-SeptemberPDFArchive/06/20060927owusu_georgenr.pdf.

cartes de paiement volées, qu'ils distribueront ensuite à des complices avec de fausses cartes d'identité); (3) falsification ou contrefaçon (p. ex. création d'adresses de courriel pour ensuite tenter de frauder des gens sur Internet, ou fabrication de cartes de paiement dont les bandes magnétiques contiendront des données tirées de cartes légitimes).

- Cet été, lors de trois incidents distincts survenus sur autant de semaines, la police d'une collectivité de Colombie-Britannique a récupéré des clés USB et des terminaux de points de vente volés qui contenaient des données compromises tirées de plus de 20 000 cartes de paiement. L'un des suspects arrêtés disposait de presque tout le matériel nécessaire pour contrefaire des cartes; un autre avait en sa possession 34 cartes qui n'étaient pas à son nom[49].

D. Transfert des données ou des articles manipulés

Parfois, le criminel qui planifie des transactions frauduleuses réparties sur une vaste zone géographique (utilisation de cartes de paiement contrefaites à des guichets automatiques situés dans plusieurs villes, etc.) doit transférer les cartes ou documents modifiés à des complices, ou bien les données manipulées à des vendeurs, par exemple des sites dédiés à la fraude aux cartes de paiement.

- Sur plus de cinq mois en 2009, les données d'environ 5 000 cartes de paiement ont été écrémées dans un restaurant de Colombie-Britannique. Elles ont servi à contrefaire des cartes, qu'une organisation criminelle a ensuite utilisées frauduleusement et systématiquement à Montréal (Québec) et à Toronto (Ontario). L'opération d'une demi-heure à peine a généré des pertes supérieures à 250 000 $[50].

E. Utilisation des articles ou des données

Finalement, bien sûr, les criminels utilisent les données ou les articles pour commettre des fraudes (voir les descriptions plus haut); pour perpétrer d'autres délits contre des particuliers, des entreprises, des organismes gouvernementaux; ou pour s'adonner à d'autres activités, comme le voyage, pour lesquelles ils doivent cacher leur véritable identité de criminels.

---

[48] *Voir, p. ex.* Statement of Rita M. Glavin, Acting Assistant Attorney General, Criminal Division, U.S. Department of Justice, Before the Subcommittee on Emerging Threats, Cybersecurity, and Science & Technology of the House of Representatives Committee on Homeland Security, 4 (31 mars 2009), *disponible au* http://www.justice.gov/criminal/cybercrime/glavinStatement.pdf.

[49] *Voir* Kelly Sinoski, *Massive credit card fraud ring suspected in Abbotsford*, 11 août 2010, *disponible au* http://www.cbc.ca/consumer/story/2010/03/11/consumer-credit-card-scams.html.

[50] Exemple de fraude par carte de crédit du type « détournements avec fuite » fourni par la Sous-direction des infractions commerciales.

- En 2010, un Californien qui se disait associé à une bande clandestine de pirates informatiques s'est fait arrêter pour des accusations d'extorsion sous le régime des lois fédérales. Selon la plainte, il aurait piraté des douzaines d'ordinateurs, obtenu des renseignements personnels sur leurs usagers, puis exigé des vidéos pornographiques à ses victimes féminines, menaçant de divulguer leurs renseignements personnels si elles refusaient[51].

- En 2010, six résidents d'Edmonton ont été accusés d'exploiter un réseau de falsification ayant volé des centaines d'identités. Les perquisitions dans un domicile du centre-ville ont mis au jour du matériel de contrefaçon ainsi que des centaines de cartes et de documents falsifiés. L'un des suspects travaillait à falsifier des cartes qui auraient permis à leurs titulaires d'acheter frauduleusement des armes à feu et des munitions. Les enquêteurs ont aussi saisi une panoplie de cartes de crédit, de cartes de membres de supermarchés, de cartes de récompenses et de cartes magnétiques d'employés, qui auraient pu servir pour des confirmations d'identité à des fins d'emprunt frauduleux[52].

V. Efforts de lutte au crime contre l'identité

A. Signaler les crimes contre l'identité

Il existe au Canada deux principaux mécanismes fédéraux pour encourager les gens à signaler les crimes contre l'identité. Le premier s'appelle le Centre antifraude du Canada (CAFC). Établi en 1993, il est l'organisme central chargé de recueillir, auprès des victimes ou consommateurs nord-américains, de l'information et des renseignements criminels sur la fraude par marketing de masse (télémarketing) et par frais d'emprunt payables à l'avance (p. ex. ouest-africaine), sur la fraude en ligne et sur les crimes contre l'identité qui comportent des éléments canadiens. Géré conjointement par la GRC, la Police provinciale de l'Ontario et le Bureau de la concurrence Canada, le CAFC ne mène pas d'enquêtes, mais il apporte une assistance précieuse aux forces de l'ordre du monde entier, jouant un rôle de premier plan dans l'éducation du public sur tel ou tel stratagème de fraude, et dans la divulgation d'information, de statistiques et de documentation sur les victimes pour aider les organismes d'exécution de la loi dans leurs enquêtes. Les données rassemblées et analysées par le CAFC sont précieuses pour évaluer les effets de différents types de fraude sur le public, et pour empêcher que pareils délits se reproduisent[53].

Le deuxième est un mécanisme en ligne, offert par la GRC et autrefois disponible sur le site Web Signalement en direct des délits économiques (Centre RECOL). En visitant RECOL, les

---

[51] *Voir* U.S. Attorney's Office, Central District of California, communiqué de presse (22 juin 2010), *disponible au* http://www.justice.gov/usao/cac/presssroom/pr2010/097.html.

[52] *Voir* Conal Piers, *Six charged in Edmonton identity theft ring*, Edmonton Journal, 24 juin 2010, *disponible au http://www.edmontonjournal.com/business/charged+Edmonton+identity+theft+ring/3192865/story.html.*

[53] *Voir à propos du Centre anti-fraude du Canada, disponible au* www.centreantifraude.ca/french/aboutus.html.

membres du grand public pouvaient déposer des rapports de fraude, qui allaient être lus par des analystes, versés dans l'une des bases de données de renseignement nationales de la GRC, et transmis aux services de police compétents. Dans un souci de performance et d'élimination des redondances, on a fusionné les fonctions des deux sites (celui de RECOL et celui du CAFC). Aujourd'hui, le public n'a qu'un site à visiter, www.antifraudcentre.ca, pour voir les statistiques sur la fraude et sur le crime contre l'identité, pour obtenir des outils d'éducation et de sensibilisation, et pour découvrir les nombreuses façons de signaler les fraudes et les crimes contre l'identité, notamment par Internet[54].

Le gouvernement fédéral américain exploite lui aussi différents mécanismes pour encourager ses citoyens à signaler les cas présumés de crimes contre l'identité. Premièrement, l'article 5 de la *Identity Theft and Assumption Deterrence Act* (1998)[55] autorise la Federal Trade Commission (FTC) à tenir l'Identity Theft Data Clearinghouse, une base de données où le public peut déposer des plaintes par téléphone ou par Internet. L'Identity Theft Assistance Center et les autorités locales alimentent aussi cette base de données; les procureurs généraux des États (qui ont leurs propres bases de données) et l'Internet Crime Complaint Center vont commencer à en faire autant d'ici peu. De 2008 à 2009 inclusivement, la FTC a reçu 592 562 plaintes pour vols d'identité. Son Identity Theft Data Clearinghouse est accessible gratuitement aux responsables canadiens et américains de l'exécution des lois civiles et pénales, via sa base de données sécurisée en ligne, le Consumer Sentinel Network, qui fonctionne 24 heures sur 24. Deuxièmement, le FBI et le National White Collar Crime Center exploitent conjointement l'Internet Crime Complaint Center (IC3), portail où le public peut signaler n'importe quelle infraction en ligne, crimes contre l'identité compris[56]. Troisièmement, les règlements fédéraux sur les services bancaires obligent les institutions financières assurées par l'État fédéral ou régies par une charte fédérale à déposer un rapport d'incident suspect auprès de l'État fédéral chaque fois qu'elles sont victimes d'une activité possiblement criminelle, comme un crime contre l'identité. De plus, l'Identity Theft Assistance Center, organisme privé, vient en aide aux victimes de vols d'identité; il communique aux autorités certaines données sur la situation de ces dernières[57].

B. Coordination nationale, binationale et multinationale

1. Coordination nationale

Chaque pays possède certains mécanismes établis pour faciliter la coordination interorganismes en matière de crime contre l'identité. Au Canada, le Groupe de travail national sur la fraude par

---

[54] *Voir* http://www.centreantifraude.ca (français).

[55] Pub. L. 105-318, 112 Stat. 3007 (30 octobre 1998), *disponible au* http://www.ftc.gov/os/statutes/itada/itadact.htm.

[56] *Voir* Internet Crime Complaint Center, http://ic3.gov.

[57] *Voir* Identity Theft Assistance Center, *disponible au* http://www.identitytheftassistance.org/.

marketing de masse (ci-après « le groupe de travail ») existe depuis septembre 2005. En janvier 2006, il a élaboré une stratégie nationale devant être révisée après trois ans. Celle-ci reposait sur quatre piliers : une répression plus vigoureuse, une sensibilisation accrue, le resserrement des conséquences judiciaires, et l'amélioration des données nationales. Le groupe de travail l'a révisée comme prévu en janvier 2009, apportant certaines modifications selon les réalisations antérieures, les lacunes existantes, et la situation d'alors quant à la fraude et aux crimes contre l'identité. Résultat : une stratégie nouvelle, révisée et bien centrée, fondée sur trois piliers. Le groupe a désigné comme pilier central le renseignement, qu'il estimait essentiel au succès de la stratégie et déterminant pour l'orientation des deux autres piliers : répression et poursuites, et prévention par l'éducation et la sensibilisation. Au Canada, le crime contre l'identité se répand et fait énormément de dégâts. Une bonne coopération entre les forces de l'ordre, les partenaires des secteurs public et privé et les citoyens est essentielle à une lutte et à une prévention efficace. Les intervenants ont donc dressé le cadre commun qui servira à définir une nouvelle stratégie nationale inspirée de la Stratégie nationale sur la fraude par marketing de masse; chacun d'eux possédait d'ailleurs une compréhension unique des défis posés par le crime contre l'identité. Tenant compte de leur point de vue et de la stratégie initiale, la stratégie nationale sur le crime contre l'identité repose sur trois piliers : 1) renseignement criminel et analyse du crime; 2) prévention par l'éducation et la sensibilisation; 3) répression, perturbation et poursuites efficaces. À chaque pilier correspondent plusieurs objets de préoccupation, ainsi que des objectifs avec des mesures névralgiques pour les réaliser. Par exemple, l'un des buts consiste à améliorer la collecte et l'échange des renseignements sur les crimes contre l'identité aussi bien entre les forces de l'ordre qu'entre les partenaires des secteurs public et privé. Globalement, la stratégie vise à outiller le Canada pour prévenir les crimes contre l'identité, pour les détecter, pour les décourager et pour enquêter sur eux. En elle-même, la stratégie pose les bases du changement et de l'amélioration.

Pour leur part, les États-Unis ont depuis octobre 2008 l'Identity Theft Enforcement Interagency Working Group. Présidé par la section antifraude du département de la Justice, division pénale, le groupe se réunit chaque mois à Washington pour que tous les principaux départements et organismes fédéraux responsables de l'exécution de la loi et de la réglementation puissent échanger sur les tendances et sur l'évolution du crime contre l'identité. Pour se tenir à jour, le groupe de travail entend chaque mois les exposés (en personne ou par vidéoconférence) des procureurs généraux adjoints de différents districts, qui ont parfois à leurs côtés des représentants de bureaux sur le terrain des organismes d'enquête fédéraux. De plus, il parle des faits nouveaux quant à la réponse des forces de l'ordre aux crimes contre l'identité, aux problèmes des victimes, aux considérations juridiques et législatives, ainsi qu'à la formation et aux autres activités qui pourraient intéresser les membres des organismes.

En 2008, le bureau de l'Attorney General des États-Unis pour le district est de la Pennsylvanie, en collaboration avec plusieurs organismes dont le US Postal Inspection Service, a annoncé le lancement du National Identity Crime Law Enforcement (NICLE) Network. Chaque jour depuis, les organismes concernés envoient au NICLE, par l'intermédiaire du réseau informatique MAGLOCLEN, leurs données sur le vol et l'usage criminel de renseignements personnels. Ces données viennent des organismes locaux, étatiques et fédéraux d'exécution de la loi (qui peuvent

aussi les consulter); il peut s'agir également de données bancaires acheminées par un centre d'échanges de l'industrie, l'Identity Theft Assistance Center. Pour consulter les données, les organismes membres emploient une connexion Internet sécurisée, fournie par le réseau Regional Information Sharing System (RISS). Dépôt central de données sur le crime contre l'identité, le NICLE permet aux organismes de savoir immédiatement quels renseignements ou pièces d'identité (permis de conduire, cartes de crédit, adresses, numéros de sécurité sociale, etc.) ont été déclarés volés, ou bien ont servi à commettre des infractions. Il nomme aussi les personnes affectées à chaque enquête, de sorte que les organismes et départements compétents puissent harmoniser leur travail quand ils travaillent à des affaires mettant en jeu des identités ou des numéros de cartes de crédit identiques ou connexes[58].

Au Canada en juillet 2007, le Groupe de travail sur la gestion de l'identité et de l'authentification a publié son rapport définitif, intitulé *A Pan-Canadian Strategy for Identity Management and Authentication*[59]. Selon ses propres termes, le rapport [traduction] « fournit la stratégie, les recommandations et le plan d'action nécessaires à l'instauration d'un cadre d'authentification et de gestion de l'identité qui permettra une prestation de service interprovinciale, à plusieurs facettes et axée sur le client pour les citoyens et les entreprises ». La stratégie a l'avantage de proposer un cadre pour la collaboration et la coopération entre les gouvernements et ordres de gouvernement, avec des éléments communs pour l'identification et l'authentification. Outre le risque de compromission réduit, elle présente pour les citoyens des avantages multiples : non seulement une plus grande sécurité, mais aussi un traitement et une authentification plus productifs des pièces d'identité. À titre d'exemple, la plupart des provinces impriment maintenant leurs certificats de naissance sur le même papier polymérique difficile à imiter, avec des symboles graphiques et des éléments de sécurité similaires.

2. Coordination binationale

Actuellement, un seul mécanisme existe au niveau stratégique pour l'échange périodique de renseignements sur le crime contre l'identité : le sous-groupe de la fraude transfrontalière du Forum sur la criminalité transfrontalière (FCT). À la formation du FCT en 1998, le sous-groupe avait pour cible principale la fraude transfrontalière par télémarketing, mais différents facteurs l'ont poussé à prendre en charge des projets variés sur le vol d'identité, notamment son évaluation en 2003 de la menace posée par le vol d'identité et ses avis de sécurité spéciaux au public sur différentes tendances en matière de vol d'identité.

Au niveau tactique, il arrive parfois que des partenaires dans le domaine de l'exécution de la loi, comme le FBI, la GRC, le Bureau de la concurrence Canada, la Federal Trade Commission, le US Postal Inspection Service ainsi que différentes entités étatiques, provinciales et municipales

---

[58] *Voir* U.S. Attorney's Office, Eastern District of Pennsylvania, communiqué de presse (10 juillet 2008), *disponible au* http://www.justice.gov/usao/pae/News/Pr/2008/jul/niclerelease.pdf.

[59] *Voir* Inter-jurisdictional Identity Management and Authentication Task Force's Final Report: A Pan-Canadian Strategy for Identity Management and Authentication, juillet 2007, http://www.cio.gov.bc.ca/local/cio/idim/documents/idma_final_report.pdf

s'échangent des renseignements et collaborent pour des enquêtes isolées sur des vols d'identité. Le plus souvent, les affaires visées mettent en jeu des vols d'identité assortis de fraude par marketing de masse.

3. Coordination internationale

Au niveau international, on a vu certains efforts visant à faire traiter le vol d'identité comme un enjeu d'intérêt mutuel, mais ils n'ont pas fait long feu. Premièrement, l'Union européenne (UE) et la Commission européenne affichent un intérêt actif pour la question; à preuve, l'UE a tenu une première conférence sur le vol d'identité à Tomar en 2007. Deuxièmement, le United Nations Office on Drugs and Crime (UNODC) travaille activement à l'élaboration de documents et de pratiques exemplaires sur le vol d'identité, soutenu par un groupe d'experts en la matière (le Core Group of Experts on Identity-Related Crime) qu'il a recrutés dans différents pays et disciplines justement à cette fin. Troisièmement, le groupe de travail de Rome-Lyon du G8 a publié en 2009 un rapport sur la criminalisation du vol d'identité, expliquant aux autres pays du monde comment évaluer leur code criminel et juger si des révisions s'imposeraient pour combattre le vol d'identité sous tous ses aspects.

C. Prévention et atténuation

1. Limiter l'accès aux données et aux documents

Comme l'a fait remarquer en 2007 le President's Identity Theft Task Force, l'une des meilleures façons de prévenir le vol d'identité et d'en réduire les dégâts consiste à protéger ses renseignements personnels des criminels en ne divulguant pas inutilement, par exemple, son numéro de sécurité sociale; en renforçant les mesures de sécurité des données dans les secteurs public et privé; et en montrant aux organismes et aux entités privées comment protéger leurs données[60]. De plus, sous le régime de la *REAL ID Act* promulguée en 2005, le département de la Sécurité intérieure a fixé définitivement des normes de base pour les cartes d'identité et permis de conduire délivrés par les États. Ces normes doivent amener les États à respecter la *REAL ID Act*, notamment sur les points suivants : (1) données et éléments de sécurité particuliers sur chaque carte; (2) preuve de l'identité et du statut juridique des demandeurs; (3) vérification des documents sources fournis par un demandeur; (4) normes de sécurité pour les bureaux qui délivrent des permis et des cartes d'identité[61].

Au Canada, les directives du Groupe de travail sur la gestion de l'identité et de l'authentification en matière d'authentification et d'éléments de sécurité ont mené à la normalisation des certificats

---

[60] Voir PRESIDENT'S IDENTITY THEFT TASK FORCE, COMBATING IDENTITY THEFT: A STRATEGIC PLAN, 22-30 (23 avril 2007), *disponible au* http://www.idtheft.gov/reports/StrategicPlan.pdf.

[61] *Voir* Dep't of Homeland Security, *REAL IDEM Final Rule*, *disponible au* http://www.dhs.gov/files/laws/gc_1172765386179.shtm.

de naissance, normalisation qui pourrait s'étendre plus tard à d'autres papiers d'identité, comme les permis de conduire et les cartes santé.

2. Sensibilisation du public (avis de sécurité, guides, etc.)

Toujours au Canada, les principaux organismes qui sensibilisent le public au crime contre l'identité sont le Forum sur la prévention de la fraude et ses membres, dont l'Association des banquiers canadiens, la Banque du Canada, les grandes banques et autres institutions financières, les émetteurs de cartes de paiement, les bureaux de crédit, les bureaux d'éthique commerciale, et les forces de l'ordre. Aperçu de la portée des mesures prises :

- Présidé par le Bureau de la concurrence Canada, le Forum sur la prévention de la fraude mène chaque année en mars une initiative connue sous le nom de Mois de la prévention de la fraude, qui s'étend à tout le pays, emploie tous les médias de communication existants et mobilise plus d'une centaine d'organisations membres et de services de police. Il y a quelques années déjà que le forum s'efforce de prévenir le crime contre l'identité.
- La Banque du Canada et ses partenaires ont produit un DVD informatif, qu'ils ont ensuite distribué aux entreprises canadiennes en plus de 150 000 exemplaires. Parmi les vidéos de la série *Échec à la fraude*, l'une porte sur le vol d'identité. On peut aussi la visionner en ligne[62].
- Pour sa part, la GRC a produit un document complet téléchargeable : *Protection des renseignements personnels et protection contre l'escroquerie – Guide pratique canadien*[63].

Aux États-Unis, la FTC joue un rôle de premier plan dans la prévention et l'éducation contre le vol d'identité, notamment parce qu'elle élabore et distribue nationalement des documents et parce qu'elle entretient un site Web exhaustif sur la façon de reconnaître le vol d'identité et d'y réagir. D'autres entités fédérales, comme les organismes de services bancaires et la Social Security Administration, ont aussi l'habitude de mettre le public en garde contre différentes formes de vol d'identité, par l'intermédiaire de leur site Web.

Le département de la Justice met lui aussi sa pierre à la prévention et à l'éducation. Son Office for Victims of Crime (OVC) et son Office of Juvenile Justice and Delinquency Prevention (OJJDP) ont parrainé ensemble des tribunes Web pour l'échange d'information et de pratiques exemplaires sur le vol d'identité, y compris l'identité d'enfants. Par ailleurs, l'OVC réunit des experts pour diriger les efforts du Département dans un tout nouveau domaine : la protection et les besoins des enfants victimes de vol d'identité. Il cherche le moyen d'aider les enfants qui se sont fait voler leurs renseignements personnels au détriment de leur cote de crédit, de leurs

---

[62] *Voir* Fighting Fraud on the Front Lines: A Retailer's Guide, *disponible au* http://www.bankofcanada.ca/en/video_corp/dbo/dvd_fraud.html , *Voir* Échec à la fraude : à vous de jouer! *disponible* à http://www.banqueducanada.ca/fr/video_corp/dbo/dvd_fraude-f.html

[63] *Voir* Protection des renseignements personnels et protection contre l'escroquerie - Guide pratique canadien *disponible à* http://www.rcmp-grc.gc.ca/scams-fraudes/canad-practical-pratique-guide-fra.htm

perspectives d'emploi et de leurs libertés civiles futures. Son travail consiste aussi à cerner les questions méritant des recherches.

3. Formation des forces de l'ordre

Pour contrer le vol d'identité, l'État doit certes sensibiliser ses citoyens, mais cela ne suffit pas. Les organismes d'exécution de la loi ont eux aussi besoin de formation, par exemple sur la détection des faux papiers et sur différentes méthodes et techniques d'enquête. Aux États-Unis, non seulement le département de la Justice organise chaque année à son National Advocacy Center des séminaires sur le vol d'identité pour les procureurs fédéraux, mais il coparraine aussi des séminaires périodiques d'une journée pour les autorités étatiques et locales sur tout le territoire américain. Le National White Collar Crime Centre (NW3C) propose lui aussi une panoplie de cours sur le vol d'identité.

Au Canada, la GRC propose à ses membres depuis 2002 un cours en ligne sur la fraude par cartes de paiement. Les autres corps de police canadiens peuvent eux aussi en profiter depuis 2006. Il y a plus de 15 ans que le cours pour les enquêteurs de monnaie contrefaite (offert par la GRC) aborde l'écrémage des cartes de paiement et la contrefaçon.

De même, le cours d'enquête sur les délits commerciaux aborde le vol d'identité depuis 2004. En juillet 2010, la GRC a lancé un cours qu'elle avait elle-même conçu, Documents de voyage et d'identité contrefaits; la police canadienne peut y accéder en ligne par le Réseau canadien du savoir policier[64]. De plus, on a vu ces dernières années plusieurs conférences régionales sur le crime contre l'identité.

4. Aide aux victimes (p. ex. conseils juridiques et pratiques)

Encore aujourd'hui, toutes les victimes de vol d'identité ne se font pas offrir la même assistance, à supposer qu'elles s'en fassent offrir. La FTC leur propose toute une gamme de documents pour s'aider elles-mêmes, mais point de conseils ou de services juridiques complets pour réparer leur nom ou leur cote de crédit si elles en ont besoin. À l'intention de l'aide juridique, des services juridiques, des avocats bénévoles et des conseillers de l'aide aux victimes, elle a publié le *Guidebook for Assisting the Victims of Identity Theft*. Celui-ci contient des instructions ainsi que des modèles de lettres et de formulaires utiles pour une aide directe de courte durée aux victimes capables de prendre elles-mêmes les mesures pour se rétablir. S'y ajoutent des explications juridiques détaillées, des dispositions législatives et réglementaires, et des modèles de lettres servant à intervenir au nom des personnes qui ne peuvent se rétablir elles-mêmes[65]. Certaines organisations régionales du secteur privé, comme l'Identity Theft Resource Center de San Diego,

---

[64] *Voir* Nouvellement disponible : Coach Officer Training et Documents de voyage et d'identité contrefaits - 9 juillet 2010 *disponsible au* http://www.cpkn.ca/news_f.html.

[65] *Disponible au* www.idtheft.gov/probono.

donnent des conseils plus poussés aux victimes. Mentionnons que l'assistance et l'intervention nécessaires sont parfois plus importantes pour certains groupes d'âge (jeunes enfants et personnes âgées) que pour d'autres.

La situation au Canada est sensiblement la même. Les institutions financières, les banques, les bureaux de crédit et les organismes d'exécution de la loi ont lancé sur Internet quelques guides devant aider les victimes de vols d'identité à se rétablir. Bien que le Canada ne possède pour le moment aucune organisation semblable à l'Identity Theft Resource Center, une équipe de projet du secteur privé a entrepris de créer un organisme à but non lucratif qui s'appellera le Canadian Identity Theft Support Centre (centre canadien d'assistance aux victimes de vols d'identité). Elle travaille avec l'Identity Theft Resource Center et avec des intervenants canadiens de premier plan, entre autres partenaires. L'inauguration officielle du centre doit avoir lieu en 2011[66].

D. Répression

1. Groupes de travail

Les deux pays ont opté pour la formule des groupes de travail, qui a déjà fait ses preuves dans la lutte à la fraude par marketing de masse et qui permet une mise en commun des ressources policières pour les enquêtes et les poursuites. Aux États-Unis, les groupes interorganismes dédiés partiellement ou entièrement au vol d'identité se comptent aujourd'hui par douzaines.

Bien que par nature les crimes contre l'identité transcendent souvent les territoires judiciaires, ils constituent au Canada des infractions au *Code criminel*, dont la répression incombe aux provinces – donc, dans les faits, aux unités des polices provinciales ou municipales qui s'occupent des infractions commerciales ou de la lutte antifraude. Certains services de police locaux se sont créé des unités distinctes chargées du vol d'identité ou des cartes de paiement contrefaites. Reconnaissant le lien étroit entre les crimes contre l'identité, les cartes de paiement contrefaites et le faux-monnayage, la GRC préfère généralement recourir aux Sections des infractions commerciales, ou bien envoyer des enquêteurs dans les Équipes intégrées de lutte contre la contrefaçon, qui sont établies dans les trois grands centres urbains du Canada.

E. Mesures législatives

1. Canada

Entré en vigueur le 8 janvier, le projet de loi S-4, selon Justice Canada :

> « …[crée] trois nouvelles infractions « fondamentales » pour vol d'identité, qui [ciblent] directement les premières étapes d'un crime lié d'identité, toutes assujetties à des peines maximales de cinq ans d'emprisonnement :

[66] Canadian Identity Theft Support Centre, Executive Overview, juillet 2010.

- **l'obtention et la possession de renseignements sur l'identité** dans l'intention de les utiliser de façon trompeuse, malhonnête ou frauduleuse pour commettre un crime;
- **le trafic de renseignements sur l'identité**, infraction ciblant ceux qui cèdent ou vendent des renseignements à un tiers en sachant que les renseignements pourraient être utilisés à des fins criminelles ou en faisant preuve d'insouciance à cet égard;
- **la possession ou le trafic illégal de documents d'identité** émis par le gouvernement qui renferment les renseignements d'une autre personne.

Par ailleurs, un nouveau pouvoir permettrait au tribunal d'ordonner, dans le cadre d'une peine, à un contrevenant de dédommager la victime de vol d'identité ou de fraude d'identité dans les cas où elle a engagé des dépenses liées au rétablissement de son identité, comme les coûts des cartes et des documents de remplacement et les coûts liés à la correction de son dossier de crédit. Cette disposition viendrait compléter les dispositions actuelles qui permettent d'ordonner un dédommagement en cas de pertes pécuniaires comme telles ou d'autres pertes de biens[67] ».

Déposé au Parlement du Canada au début de 2010, le projet de loi C-29, intitulé *Loi modifiant la* Loi sur la protection des renseignements personnels et les documents électroniques *(LPRPDL) (Loi protégeant les renseignements personnels des Canadiens)*, doit ajouter à la LPRPDL des dispositions exigeant la déclaration des « atteintes importantes ». Ainsi, les organisations assujetties à la loi devraient déclarer au commissaire à la protection de la vie privée toute atteinte importante aux mesures de sécurité protégeant les renseignements personnels en leur possession. Elles devraient aussi prévenir les principaux intéressés advenant « que l'atteinte présente un risque réel de préjudice grave à [leur] endroit ». Préjudice grave s'entend ici de pertes financières, de vol d'identité ou de détérioration de la cote de crédit. Finalement, les organisations devraient aussi, sans le consentement des intéressés, prévenir toute institution gouvernementale capable de réduire le risque de préjudice pour ces derniers ou d'atténuer ce préjudice[68].

2. États-Unis

Depuis 2007, les législateurs américains ont modifié le droit pénal afin de faciliter les poursuites pour vol d'identité. Inspirés des recommandations du plan stratégique 2007 du President's

---

[67] *Voir* Ministère de la Justice Canada, Communiqué, APPLICATION DE LOIS PLUS STRICTES VISANT LE VOL D'IDENTITÉ (8 janvier 2010), *disponible au* http://www.justice.gc.ca/fra/nouv-news/cp-nr/2010/doc_32470.html.

[68] *Voir* Résumé législatif du projet de loi C-29 : Loi modifiant la Loi sur la protection des renseignements personnels et les documents électroniques, *disponible au* http://www2.parl.gc.ca/Content/LOP/LegislativeSummaries/40/3/c29-f.pdf.

Identity Theft Task Force[69], les modifications étaient enchâssées dans l'Identity Theft Enforcement and Restitution Act (ITERA)[70], entrée en vigueur le 26 septembre 2008. Dans les grandes lignes, cette loi élargit et clarifie les domaines de compétence quant à différents cybercrimes, elle oriente la United States Sentencing Commission quant aux peines à infliger pour le vol d'identité, et elle autorise les tribunaux fédéraux à exiger, dans leurs sentences pour les grandes catégories de vol d'identité[71], que le contrevenant [traduction] « rembourse à la victime la valeur du temps qu'elle a raisonnablement pu passer à tenter de réparer les préjudices que l'infraction visait à lui causer, ou qu'elle lui a véritablement causés[72] ».

Dans les 18 derniers mois, au moins deux verdicts de tribunaux fédéraux ont fait jurisprudence quant à l'infraction fédérale 18 U.S.C. § 1028A, ou vol d'identité avec circonstances aggravantes. Ainsi en 2009, dans l'affaire *Flores-Figueroa v. United States*[73], la cour suprême des États-Unis a statué que l'État ne pouvait faire condamner un accusé de vol d'identité avec circonstances aggravantes sans prouver que ce dernier savait, quand il les avait en sa possession ou quand il les a transférés ou utilisés, que les renseignements signalétiques (nom, numéro de sécurité sociale, numéro de carte de crédit, etc.) appartenaient à une autre personne [réelle][74]. Plus récemment, dans l'affaire *United States v. Magassouba*[75], la United States Court of Appeals for the Second Circuit a statué que dans un procès en vertu de la disposition 1028A, le tribunal compétent pour juger l'acte délictueux grave sur lequel repose l'accusation de vol d'identité avec circonstances aggravantes (fraude postale, fraude électronique, etc.) est aussi compétent pour juger l'infraction distincte (transfert, possession ou utilisation consciente des renseignements signalétiques d'une autre personne aux fins et pendant la première infraction) même si rien n'indique qu'elle (la seconde infraction) se soit produite dans le même district judiciaire[76]. Ce verdict établit un précédent important, car il permet d'accuser efficacement les individus dont les vols d'identité et les infractions connexes débordent sur plusieurs territoires judiciaires.

VI. Conclusion – Perspectives d'avenir : défis et recommandations

---

[69] *Voir* PRESIDENT'S IDENTITY THEFT TASK FORCE, COMBATING IDENTITY THEFT: A STRATEGIC PLAN (23 avril 2007), *disponible au* http://www.idtheft.gov/reports/StrategicPlan.pdf.

[70] *Voir* Pub. L. 110-326, Title II, §§ 201-209 (26 septembre 2008), *disponible au* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_public_laws&docid=f:publ326.110.pdf.

[71] 18 U.S.C. §§ 1028(a)(7) et 1028A(a).

[72] Pub. L. 110-326, Title II, § 202(3) (26 septembre 2008), *codified*, 18 U.S.C. § 3663(b)(6).

[73] 129 S. Ct. 1886 (2009).

[74] *Idem*., 1888.

[75] N° 09-3035-cr, slip op. (2d Cir., décision rendue le 31 août 2010).

[76] *Idem.*, 2.

A. Sécurité et intégrité des données et des documents

Un obstacle persistant gêne les secteurs public et privé dans leur lutte contre le vol d'identité : l'insécurité et la vulnérabilité qui caractérisent encore tant de mécanismes de paiement et de papiers d'identité. Les faiblesses tiennent d'une part à la nature même des mécanismes et des documents, et d'autre part à la multiplicité des entités qui les établissent ou les délivrent. Aux États-Unis, selon la National Association of Public Health Statistics and Information Systems (NAPHSIS), quelque 6 400 instances étatiques et locales délivrent certificats de naissance, certificats de décès et autres documents officiels. De surcroît, pour beaucoup de ces documents, il n'existe pas de modèle normalisé commun à tous les États, et encore moins d'éléments de sécurité pour compliquer la tâche aux criminels.

Assurément, les particuliers peuvent faire beaucoup pour atténuer les risques de vol d'identité. Des précautions simples comme déchiqueter les relevés financiers dont on n'a pas besoin ou utiliser des logiciels de sécurité Internet entre autres outils en ligne sont faciles à prendre, et recommandables pour tout le monde. Malheureusement, il arrive de plus en plus souvent que des criminels compromettent des renseignements personnels précieux en grande quantité, soit en compromettant des personnes bien placées, soit par des attaques externes (piratage, hameçonnage, etc.). Il est irréaliste de s'attendre à ce que les particuliers arrêtent seuls la vague de vols d'identité. Tous les ordres de gouvernement, sans oublier les secteurs d'activité comme les services bancaires et financiers, l'informatique et les paiements, doivent reconnaître qu'ils ont un travail considérable à réaliser en ce sens, et que leurs rôles se complètent.

B. Détection des données et des papiers d'identité frauduleux

Puisque les papiers d'identité et les banques de données demeurent relativement peu sécuritaires, les secteurs public et privé des deux pays se doivent de chercher ou de créer des façons de mieux détecter les cartes de paiement et les papiers d'identité frauduleux ou falsifiés. Les nouvelles technologies offrent une bonne solution à court terme, car elles facilitent beaucoup l'authentification de ces articles même sans éléments de sécurité robustes.

Aux États-Unis, plusieurs affaires récentes ont montré la valeur de la reconnaissance faciale dans la lutte au vol d'identité par permis de conduire. En août 2010, le gouverneur de l'État de New York, David A. Paterson, a annoncé les premiers résultats de l'usage de cette technologie par le département des Véhicules moteurs (DMV) pour détecter la fraude. Selon lui, le logiciel du DMV :

> [traduction]
> « […] en deux mots, convertit les photos signalétiques numériques du Département en algorithmes mathématiques. Le logiciel soumet à des employés qualifiés les images photographiques correspondant à des algorithmes similaires qu'il aura récupérés parmi les photos prises chaque jour au DMV, ou dans la banque du Département, qui contient quelque 15 millions de photos. Jamais une photo ne servira à créer de nouvelles pièces d'identité si des personnes qualifiées

n'ont pas d'abord évalué les correspondances possibles. Le DMV s'efforce de ne délivrer qu'un seul permis par personne; quiconque tente d'en obtenir un second commet forcément une infraction, car il ou elle doit soumettre un instrument frauduleux[77]. »

Cette technologie a permis de cerner plus de 1 000 cas de fraude potentielle, et d'arrêter pour actes délictueux graves plus de 100 personnes, notamment un Égyptien qui détenait quatre permis sous autant de noms différents, dont un apparaissait sur la liste des personnes interdites de vol établie par le gouvernement fédéral; un ancien tueur à gages récemment sorti de prison qui cherchait à se créer une deuxième identité; et un individu recherché pour un vol de banque dans le comté de Nassau (État de New York) dans les années 90. Les autres personnes arrêtées s'étaient fait suspendre leur permis, ou bien avaient accumulé les contraventions et les accidents sous une panoplie d'identités[78]. La Federal Motor Carrier Safety Administration, qui relève du département fédéral des Transports, subventionne ce genre de projets dans les DMV.

C. Mécanismes de déclaration

Comme nous l'avons déjà dit, le Canada comme les États-Unis possèdent des centres nationaux chargés de recevoir, d'examiner et d'utiliser les plaintes du public en matière de vol d'identité. Les autorités des deux pays travaillent déjà à l'échange de renseignements, mais elles devraient, dans le respect de leurs lois respectives et dans un esprit transfrontalier, chercher des moyens pour que ces centres de déclaration, entre autres entités des secteurs public et privé, puissent échanger en temps utile des renseignements pertinents sur les grandes tendances du vol d'identité, et sur les plaintes individuelles.

D. Coordination des échanges de renseignements, coopération entre les organismes d'exécution de la loi, éducation du public

Il faut aussi que les deux pays cherchent des occasions de mieux coordonner leurs enquêtes et leurs renseignements sur les crimes contre l'identité, et d'accroître la coopération entre leurs organismes d'exécution de la loi aux niveaux infranational, national et international :

- Au niveau infranational, les corps de police et autres organismes d'exécution de la loi ayant souvent reconnu leur utilité dans la lutte à la fraude et au vol d'identité, il y a tout lieu d'encourager les liens étroits et les mécanismes d'échange d'information (p. ex. groupes de travail interorganismes), pour optimiser l'échange en temps utile de renseignements tactiques et stratégiques sur le vol d'identité.

- Au niveau national, la plupart des organismes d'enquête s'intéressent au vol identité, mais la loi n'autorise aucun d'eux à prendre lui-même en charge une enquête sur des méfaits survenus dans plusieurs États ou dans plusieurs provinces. Cela dit, coordination et

[77] Office of the Governor, New York State, communiqué de presse (10 août 2010), *disponible au* http://www.ny.gov/governor/press/081010Dmv.html.
[78] *Idem*.

échange de renseignements sont de mise entre les organismes nationaux, pour que toute entité possédant l'expertise et les attributions pertinentes puisse maximiser sa productivité. Aux États-Unis, le Consumer Sentinel's Identity Theft Data Clearinghouse de la FTC et le réseau National Identity Crime Law Enforcement (NICLE) donnent aux organismes de tous les niveaux et de tous les États un accès en temps réel à des données substantielles qui peuvent devenir des pistes d'enquête majeures et des occasions de collaboration interorganismes[79].

- Finalement, puisque le vol d'identité se mondialise, la police, des organismes d'enquête et les services de poursuite pénale doivent créer des mécanismes transnationaux qui rendront possible un échange opportun de renseignements stratégiques et tactiques sur les tendances et opérations en la matière qui transcendent les frontières. Bien que les règles sur la protection des renseignements personnels puissent varier considérablement d'un système juridique à l'autre, les forces de l'ordre doivent se donner les moyens de dépister et de juguler le vol d'identité au niveau transnational. En fait, elles peuvent très bien y arriver tout en respectant leurs systèmes juridiques respectifs. Depuis septembre 2009 par exemple, les autorités canadiennes, britanniques et américaines discutent d'un éventuel groupe de travail international sur le crime contre l'identité. Ce groupe deviendrait une tribune où les trois pays (voire d'autres pays) se retrouveraient régulièrement pour échanger des renseignements, pour discuter et pour trouver des occasions de collaborer bilatéralement ou multilatéralement pour combattre le vol d'identité.

En outre, les autorités canadiennes et américaines vont devoir chercher et saisir les possibilités d'enseigner à tous les segments pertinents du public (c'est-à-dire non seulement au grand public, mais aussi aux médias, au monde des affaires et à tous les organes gouvernementaux) les problèmes causés par le vol d'identité, et les façons dont particuliers et entités peuvent lutter contre ce fléau. Certains organismes des deux pays font régulièrement de la prévention et de la sensibilisation auprès du public; en revanche, il n'y a toujours aucune recherche concertée d'uniformité et de cohérence pour le message à adresser aux particuliers, aux entreprises et au secteur public.

E. Examen et amélioration constants des cadres législatifs

Les deux pays seraient très avisés de porter attention à leurs systèmes juridiques, et d'en dégager les points à réviser. En 2007 par exemple, le President's Identity Theft Task Force a recommandé au Congrès de modifier les infractions fédérales liées au vol d'identité, pour rendre possible la poursuite en justice des individus s'étant approprié les renseignements d'entreprises

---

[79] *Voir* Audit Division, Office of Inspector General, U.S. Department of Justice, The Department of Justice's Efforts to Combat Identity Theft, Audit Report 10-21, (14 mars 2010), *disponible au* http://www.justice.gov/oig/reports/plus/a1021.pdf. En date d'août 2009, NICLE [traduction] « contenait 6,5 millions de dossiers. Quelque 190 corps de police en faisaient usage, de même que 26 entités propres à cinq États, et 12 organismes fédéraux ». *Idem*.

ou d'autres organisations[80]. Les législateurs n'ont pas tenu compte de cette recommandation dans leur Identity Theft Enforcement and Recovery Act de 2008; les criminels continuent d'employer noms d'entreprises, numéros de comptes et autres données pour commettre une panoplie de fraudes contre les particuliers et les entreprises.

De même, le Canada et les États-Unis doivent encourager les autres pays à réviser leurs propres cadres législatifs afin que ceux-ci prévoient des sanctions pénales pour toutes les étapes du vol d'identité, de l'acquisition initiale à l'utilisation finale. Beaucoup de pays, s'ils définissent des infractions générales (fraude, usage de faux-semblants, etc.) applicables aux fraudes qui accompagnent le vol d'identité, n'ont en revanche aucun mécanisme comme le projet de loi S-4 du Canada pour tuer le crime contre l'identité dès ses premiers stades. Le G8 a publié en 2009 un rapport sur les outils juridiques essentiels à la lutte au crime contre l'identité[81], qui donne de bons conseils aux autres pays pour la révision de leur code criminel; les représentants canadiens et américains ont beaucoup fait pour en élaborer les concepts, pour en produire l'ébauche, et pour la faire adopter par les chefs de délégations.

F. Publiciser l'aide aux victimes et la rendre plus accessible

Pour que la lutte au crime contre l'identité réussisse, il faut que les pays non seulement disposent de bons outils juridiques pour les enquêtes et les poursuites, mais offrent à leur population les mécanismes nécessaires pour que les victimes de vols d'identité arrivent à se rétablir, soit par leurs propres moyens, soit en demandant de l'aide. Voilà qui n'est pas facile, car on peut se faire voler son identité peu importe où l'on vit ou travaille, peu importe son revenu ou sa profession, et aucune composante de l'identité n'est à l'abri (comptes bancaires, cartes de crédit, numéro d'assurance sociale ou de sécurité sociale, etc.). Le Canada et les États-Unis doivent néanmoins se retrousser les manches.

Une mesure concrète consisterait par exemple à s'assurer que les organisations publiques et privées conseillent adéquatement les victimes de vols d'identité sur la façon d'accéder aux renseignements et de se rétablir. Aux États-Unis, la Federal Trade Commission (FTC) publie des guides complets, sur papier comme en version électronique. D'autres personnes et entités en font autant dans leur État respectif, les procureurs généraux par exemple. Au Canada, comme nous l'avons déjà mentionné, plusieurs organisations proposent de l'aide aux victimes, notamment la GRC qui, en 2010, a publié un guide pour les victimes sur son site Web[82].

Une autre mesure concrète serait de miser sur les juristes, pour que les victimes puissent obtenir des conseils juridiques fiables. Souvent, les victimes s'interrogent sur leurs droits et sur la meilleure façon de faire corriger leurs dossiers chez les organismes publics et privés. De surcroît,

---

[80] Voir PRESIDENT'S IDENTITY THEFT TASK FORCE, *supra* note 60, 67.

[81] Criminal and Legal Affairs Subgroup, G8 Lyon-Roma Anti-Crime and Terrorism Group, *supra* note 9.

[82] *Voir* Guide pour les victimes de fraude ou vol d'identité *disponible au* http://www.rcmp-grc.gc.ca/scams-fraudes/victims-guide-victimes-fra.htm.

beaucoup n'ont pas les moyens d'engager un avocat qui puisse les représenter et les guider dans le rétablissement de leur identité. En 2007, le President's Identity Theft Task Force a recommandé que le barreau des États-Unis, avec l'aide du département de la Justice, [traduction] « mette sur pied un programme d'avocats bénévoles pour aider les victimes de vols d'identité à se rétablir[83] ». En 2008, le barreau a adopté une résolution en ce sens. Pour faciliter l'application du programme, la FTC vient de publier en collaboration avec le département de la Justice un guide à l'intention des associations étatiques du barreau, pour les avocats bénévoles aidant des victimes de vol d'identité[84].

* * *

D'année en année, le vol d'identité et les personnes et organisations qui le commettent se complexifient, devenant capables de s'adapter rapidement selon l'évolution des circonstances. Les gouvernements (tout particulièrement les forces de l'ordre) et les entités du secteur privé dans les deux pays doivent tenir le rythme. À l'heure où le vol d'identité occasionne chaque année des pertes pour les particuliers, pour les entreprises et pour les gouvernements qui se chiffrent – en comptant les dégâts pour la réputation et les coûts pour réparer ou rétablir les identités volées – en dizaines de milliards de dollars, les secteurs public et privé ne manquent pas de raisons pour travailler ensemble et pour tendre la main à leurs homologues étrangers afin d'enrayer ce problème.

---

[83] PRESIDENT'S IDENTITY THEFT TASK FORCE, *supra* note 60, 49.

[84] *Voir* Federal Trade Comm'n, Guidebook for Assisting Identity Theft Victims (2010), *disponible au* http://www.idtheft.gov/probono/docs/i.%20Table%20of%20Contents.pdf.