CONFÉRENCE POUR L'HARMONISATION DES LOIS AU CANADA

RAPPORT DU GROUPE DE TRAVAIL CONJOINT SUR LE VOL D'IDENTITÉ DE LA SECTION PÉNALE ET DE LA SECTION CIVILE : DOCUMENT DE DISCUSSION

Veuillez noter que les idées et conclusions formulées dans ce document, ainsi que toute terminologie législative proposée et tout commentaire ou recommandations, n'ont peut-être pas été adoptés par la Conférence pour l'harmonisation des lois au Canada. Ils ne reflètent pas nécessairement le point de vue de la Conférence et de ses participants. Veuillez consulter les résolutions concernant ce thème qui ont été adoptées par la Conférence lors de la réunion annuelle.

Charlottetown

Île-du-Prince-Édouard

Septembre 2007

INTRODUCTION

[1] Le vol ou l'usurpation d'identité[1] cause des pertes financières considérables, voire souvent, en fin de compte, un préjudice indirect permanent à ses victimes. Ce sujet a fait l'objet d'études approfondies par une multitude de groupes, d'organisations et de gouvernements, et ce, tant au Canada qu'à l'étranger.

[2] La Conférence s'est aussi beaucoup intéressée à ce thème. Dernièrement, soit en 2006, la résolution suivante a été adoptée par la section pénale :

> a) *Le Groupe de travail fédéral-provincial-territorial sur le vol d'identité devrait examiner la question de savoir quelles ordonnances ou déclarations accessoires pourraient être prononcées dans le contexte d'une poursuite pénale pour aider la victime dans ce processus.* [réintégration de l'aspect financier et des autres aspects de leur identité]. *(AB2006-03)*

[3] La section civile a aussi étudié la question du préavis obligatoire ou de l'« avis d'atteinte » à la sécurité des renseignements personnels. Un groupe de travail conjoint a donc été formé pour, entre autres, rédiger un document de discussion sur ces questions; il devait établir les aspects qui méritaient une recherche et un examen plus approfondis. Le groupe de travail se compose des membres suivants :

1)	Josh Hawkes	procureur en appel, ministère de la Justice de l'Alberta
2)	John Gregory	avocat général, Division des politiques, Ontario
3)	Jeanne Proulx	avocate-légiste, Québec
4)	Wilma Hovius	avocate, Section des politiques en matière de droit public, Justice Canada
5)	Erin Winocur	avocate, Direction des politiques en matière criminelle, Ontario
6)	Joanne Klineberg	avocate, Section de la politique en matière de droit pénal, Justice Canada
7)	Joe Pendleton	directeur, unité des enquêtes spéciales, Solliciteur général de l'Alberta

L'ampleur du problème :

[4] Selon les preuves statistiques qui émanent du Canada, des États-Unis, du Royaume-Uni et de l'Australie, le vol d'identité est un problème qui touche un grand nombre de victimes. Il a des répercussions marquées pour les victimes sur le plan

financier ou autre et pour bon nombre d'organisations qui sont chargées de les aider. Toutefois, de par les différences existant entre les méthodes de déclaration, entre autres, il est difficile de faire une comparaison exacte entre ces différents pays. Vous trouverez ciaprès un résumé de certains renseignements qui montre l'ampleur du problème.

Canada

[5] PhoneBusters est un centre d'appel antifraude national qui est dirigé par la Police provinciale de l'Ontario et la Gendarmerie royale du Canada. PhoneBusters est l'organisme central chargé de recueillir des renseignements sur le vol d'identité. Les chiffres fournis par l'organisme montrent qu'entre 2002 et 2006, 54 920 personnes ont porté plainte pour vol d'identité, ce qui totalise des pertes de l'ordre de 77 610 779 $[2]. En raison du faible taux de signalement des vols d'identité, l'organisme estime que ce chiffre ne représente peut-être que 5 % du total réel[3], ce qui semble être appuyé par un sondage Ipsos Reid, réalisé en 2003, et d'après lequel, neuf pour cent de la population canadienne ont été victime de vol d'identité au cours de leur vie[4]. Les chiffres recensés aux ÉtatsUnis confirment que le faible taux de signalement, tant à la police qu'aux agences d'évaluation du crédit, pose un grave problème. Selon ce que montrent certaines études, la plupart des victimes de vol d'identité ne communiquent ni avec la police ni avec les agences d'évaluation du crédit[5].

[6] D'après les renseignements transmis par les deux principales agences canadiennes d'évaluation du crédit et par le Conseil canadien des bureaux d'éthique commerciale, la fréquence des vols d'identité est bien supérieure à celle que montrent les données de PhoneBusters. Ces groupes estiment que les pertes engendrées par le vol d'identité en 2002 se chiffrent à 2,5 milliards de dollars[6]. Le fait que le vol d'identité puisse être signalé à différents organismes, chacun ayant des définitions et des normes de données divergentes, complique davantage la tâche qu'est la collecte de renseignements statistiques précis[7].

États-Unis

[7] Selon une enquête nationale sur les victimes de la criminalité réalisée en 2004, 3,6 millions de ménages (ce qui représente 3 % de tous les ménages américains) avaient signalé qu'au moins un membre de leur famille avait été victime d'un vol d'identité au cours des six derniers mois. Les pertes financières afférentes aux vols d'identité sont estimées à quelque 3,2 milliards de dollars[8]. Les plaintes pour vol d'identité représentent 37 % (ou 255 000) des plaintes déposées auprès de la Commission fédérale du commerce en 2005[9]. Selon le Rapport de 2006 sur l'étude sur la fraude identitaire, bien que le nombre de victimes sait passé de 10,1 millions en 2003 à 8,9 millions en 2006, le nombre total des pertes est passé de 53,2 milliards en 2003 à 56,6 milliards en 2006[10]. Une enquête réalisée en 2007 et financée par le secteur d'activités a montré une chute des pertes totales attribuables au vol d'identité, mais elle a été controversée et vivement contestée[11].

Royaume-Uni

[8] Selon une étude réalisée en 2002 par le Cabinet Office, le coût associé au vol d'identité était estimé à 1,3 milliard de livres par année[12]. Le chiffre a été révisé en 2006 et il indique que les coûts seraient de 1,7 milliard de livres par année[13]. Toutefois, ces chiffres comprennent les coûts estimatifs pour divers ministères et organismes chargés de l'application de la loi[14], qui pourraient bien ne pas avoir été inclus dans les estimations des autres ressorts dont il a été question ci-dessus. Le CIFAS, un consortium sans but lucratif composé de groupes sectoriels et autres, a signalé 66 000 cas de fraude identitaire en 2005, comparativement à 9 000 en 1999[15].

Australie

[9] Les chiffres totaux pour tous les types de fraude montrent que le vol d'identité est l'une des principales activités criminelles en Australie. Selon une estimation, le vol d'identité coûte environ 5 milliards de dollars par année[16]. Le vol d'identité représente une grande part de ce total, avec un coût estimatif annuel variant entre 2 et 3,5 milliards de dollars. De plus, plusieurs administrations ont remarqué que l'usurpation d'identité

pouvait être liée à une autre activité criminelle et donner lieu à des préoccupations visant la sécurité nationale[17].

Répercussions sur la victime

[10] En règle générale, les répercussions du vol d'identité peuvent se classer dans deux grands groupes : les préjudices financiers directs et les préjudices indirects concernant les cotes de crédit et la réputation financière. Dans certains cas, il peut même y avoir, par erreur, un casier judiciaire qui soit créé au nom de la victime[18].

[11] Dernièrement, deux enquêtes successives publiées par le centre des ressources sur le vol d'identité (Identiy Theft Resource Center) aux États-Unis ont permis de fournir des renseignements détaillés sur les répercussions du vol d'identité sur une personne. En 2003 et en 2004, les victimes de vol d'identité ont reçu un questionnaire qui visait à établir et à décrire les répercussions de ce crime. Dans les deux enquêtes, l'échantillon était de petite taille (180 et1 97, respectivement). Le centre a reconnu les limites inhérentes aux échantillons pour les deux enquêtes et a laissé entendre qu'il fallait faire une recherche plus approfondie. À cette réserve près, les enquêtes permettent de bien illustrer la nature et la durée des répercussions engendrées par ce crime. Une enquête plus vaste a été entreprise pour le compte de la Commission fédérale du commerce des ÉtatsUnis en 2003, cette fois avec des entrevues menées sur un échantillon aléatoire de plus de quatre mille personnes. Certains des résultats de ces trois enquêtes peuvent être résumés comme suit :

Découverte du vol d'identité

> [TRADUCTION]
> *Lorsque nous avons demandé aux personnes interrogées comment elles avaient découvert que leur identité avait été volée, les réponses ont été plus variées que les deux douzaines de réponses possibles de l'enquête. Comme ce fut le cas en 2003, quelque 85 % des victimes ont découvert le crime parce qu 'elles en ont été victimes, autrement dit, seulement quelque 15 % de toutes les victimes de vol d'identité ont pu découvrir le crime grâce aux mesures proactives adoptées par les entreprises*[19].

Lorsque le vol d'identité s 'était limité à l 'utilisation inappropriée des comptes existants, 20 % des victimes avaient été informées par les ban ques ou les compagnies émettrices de cartes de crédit. Toutefois, lorsque le vol avait entraîné l 'ouverture de nouveaux comptes ou un autre type de fraude, 8 % seulement des victimes avaient été informées par les ban ques ou les compagnies émettrices de cartes de crédit.Dix-huit pour cent de ces victimes avaient été informées par d 'autres parties, notamment des agents de recouvrement et des organismes gouvernementaux[20].

Temps consacré par les victimes à rétablir ou à rectifier les antécédents financiers

[TRADUCTION]
Le centre des ressources sur le vol d'identité a déclaré qu 'en 2004, la moitié des victimes avaient consacré moins de 100 heures (médiane) à ces tâches. Toutefois, la moitié des victimes avaient consacré plus de 100 heures. Lorsque nous calculons la moyenne des heures totales consacrées à la réparation des dommages causés par le voleur (sans cas particuliers), le résultat est de 330 heures (moyenne). Le nombre d'heures total déclaré se situe entre 3 heures et 5,840 heures[21].

Selon le rapport d'enquête sur le vol d'identité publié par la Commission fédérale du commerce en 2003, les victimes ont déclaré, en moyenne, avoir consacré 30 heures à la résolution des problèmes liés au vol d'identité. Les victimes pour lesquelles de nouveaux comptes ont été ouverts à la suite d 'un vol d 'identité ont consacré 60 heures à régler ce pro blème[22].

Pour les deux années 2003 et 2004, 26 à 32 % des victimes ont répondu avoir consacré de quatre à six mois pour régler ce problème. Quelque 17 % des victimes ont déclaré y avoir consacré entre 13 et 23 mois. Toutefois, un nombre plus élevé de répondants en 2003 (23 %) par rapport à 2004 (11 %) a déclaré y avoir consacré entre sept mois et un an. Un nombre plus élevé de répondants a déclaré y avoir consacré plus de quatre ans en 2004, comparativement à ceux ayant répondu au sondage en 2003[23].

Conséquences du vol d'identité

[TRADUCTION]
D 'autres formes de vol d 'identité ont également été signalées par les répondants dans le cadre de l 'enquête menée par la Commission fédérale du commerce. Douze pour cent des victimes ont déclaré que les voleurs avaient commis des crimes financiers ayant donné lieu à la délivrance d'un mandat au nom de la victime, tandis que 18 % des victimes qui ont laissé entendre qu 'un permis de conduire avait été obtenu en utilisant les renseignements les concernant[24]*. Quinze pour cent des victimes ont déclaré que leurs renseignements personnels avaient été utilisés à des fins*

inappropriées de manière autre que financière. Quatre pour cent des personnes de ce groupe ont déclaré que leur identité avait été utilisée par une personne lorsqu 'elle avait été arrêtée par les autorités chargées de l'application de la loi ou inculpée d'un crime, savoir le plus souvent le fait d'avoir présenté une fausse pièce d'identité au moment de son arrestation par les autorités chargées de l'application de la loi[25].

Soixante-quatre pour cent des victimes de vol d 'identité pour lesquelles de nouveaux comptes ont été ouverts ou d'autres fraudes ont été commises ont signalé des problèmes liés à un certain nombre d'autres domaines, notamment des difficultés en matière de crédit, problèmes bancaires, difficultés avec les agences de recouvrement, poursuites civiles, refus de contrat d'assurance ou de prêt. Quatorze pour cent des victimes ont déclaré avoir fait l 'objet d'une enquête criminelle à la suite du vol d 'identité[26].

Le centre des ressources sur le vol d 'identité a également signalé que les victimes d 'un vol d 'identité ont déclaré un certain nombre d 'autres incidences négatives, notamment des difficultés à obtenir du crédit, de graves ennuis pour clarifier leurs antécédents en matière de crédit et des pro blèmes pour contracter une assurance. Près des deux tiers des répondants ont déclaré avoir eu de la difficulté à clarifier leurs antécédents en matière de crédit. Dans vingt-sept pour cent des cas, des renseignements défavorables ont été inscrits dans les antécédents en matière de crédit des victimes et, dans 25 % des cas, ces renseignements n 'ont pas été supprimés d'emblée. Une autre difficulté a eu lieu lorsque des renseignements précis ont été vendus à des agences de recouvrement ou lorsque des « alertes à la fraude » inscrites aux dossiers de crédit n 'ont pas été prises en compte et qu 'un nouveau crédit a été abusivement accordé[27].

Avantages de la découverte rapide du vol

[TRADUCTION]
Les coûts associés à un vol d 'identité sont considérablement moindres si le vol est découvert rapidement. Lorsque l 'utilisation inappropriée a été découverte dans les cinq mois, la valeur obtenue par le fraudeur était inférieure à 5 000 $, et ce, dans 82 % des cas. Lorsque le vol a été découvert dans les six mois ou plus, la valeur totale était d'au moins 5 000 $, et ce, dans 44 % des cas. La découverte rapide a également fait diminuer les frais et les heures consacrés par les victimes à rétablir leurs antécédents en matière de crédit[28].

LES PROBLÈMES

Aide aux victimes grâce au droit pénal

Approche adoptée dans les autres ressorts :

[12] Le groupe de travail a examiné deux options pour venir en aide aux victimes en vertu du droit pénal. La première est une approche générale de l'aide aux victimes dans le contexte du vol d'identité. La deuxième est une approche plus restreinte visant à aider les victimes lorsque le vol d'identité a entraîné, par erreur, la création de casiers judiciaires ou d'autres entrées dans les dossiers ou les bases de données des organismes chargés de l'application de la loi ou du gouvernement.

Approche générale

[13] En 2003, l'État de l'Australie-Méridionale a adopté une loi selon laquelle est remis un certificat conçu pour aider les victimes de vol d'identité. Par souci de commodité, la disposition figure ci-après.

Certificat remis aux victimes de vol d'identité

[TRADUCTION]

[14] Le tribunal qui déclare une personne coupable d'une infraction visant

a) l'appropriation de l'identité d'une autre personne;

b) l'utilisation des renseignements d'identification personnelle d'une autre personne;

peut, à la demande de la victime de l'infraction, délivrer un certificat en vertu du paragraphe (2).

[TRADUCTION]

[15] Le certificat doit indiquer de manière détaillée

a) l'infraction;

b) le nom de la victime;

c) toute autre question considérée pertinente par le tribunal[29].

[16] Par la suite, l'État de Queensland a adopté une disposition semblable, et le comité des avocats en droit pénal modèle (Model Criminal Law Officers Committee) du comité

permanent des procureurs généraux (Standing Committee of Attorneys General)[30] a ensuite emboîté le pas.

[17] Le comité a signalé des lacunes qui tenaient à cette approche, y compris le fait que le certificat n'est pas, en soi, un recours[31], mais tout simplement un formulaire pratique servant à résumer les conclusions pertinentes du tribunal. À la suggestion du comité, les certificats devraient peut-être être prévus même en l'absence de déclaration de culpabilité, lorsqu'il existe des preuves suffisantes que l'identité d'une personne a été utilisée de manière inappropriée ou en dépit de l'acquittement du défendeur si l'utilisation de l'identité de la victime est prouvée selon la prépondérance des probabilités[32].

[18] D'autres groupes ont également trouvé des lacunes dans le système de certificat. Par exemple, le centre australien des recherches stratégiques a constaté que ces certificats ne pouvaient être délivrés qu'à la suite d'une déclaration de culpabilité et qu'avec les années, il pouvait y avoir beaucoup moins d'avantages à utiliser ce type de document. L'une des solutions de rechange proposée consistait à donner aux autorités chargées de l'enquête le pouvoir de délivrer à diverses étapes de l'enquête, un certificat où serait présenté le point de vue de la police, savoir que selon la prépondérance des probabilités, la personne avait été une véritable victime de vol d'identité. Toutefois, deux services de police se sont opposés à cette modification. Malgré ces lacunes, ils ont retenu le modèle de la remise d'un certificat à la victime comme il est décrit dans les lois résumées ci-dessus[33].

[19] Une approche similaire à la modification envisagée par le centre australien des recherches stratégiques a été proposée dans la loi sur la protection du consommateur du Michigan. En 2003, le sénat d'état a entériné un projet de loi prévoyant qu'une personne ayant été victime d'un vol d'identité peut demander au procureur de comté ou au procureur général de délivrer un certificat l'attestant. La demande doit être faite par écrit et sous serment. Le certificat comprendrait, entre autres, une déclaration selon laquelle il a été jugé que la personne a été victime d'un vol d'identité. Le certificat serait également considéré comme un dossier public officiel. Bien qu'il ait été entériné par le sénat, le projet de loi n'a été ni adopté par la chambre ni déposé[34].

Approche restreinte

[20] L'État de la Californie a adopté une approche plus restreinte en matière d'utilisation de certificats pour venir en aide aux victimes de vol d'identité. L'État a défini le « vol d'identité criminel » comme un vol d'identité qui a lieu quand le suspect d'une enquête criminelle s'identifie en utilisant l'identité d'une autre personne innocente. Il peut en découler la création par les services de police et le tribunal de dossiers où la victime est faussement identifiée comme étant la personne arrêtée, libérée sous conditions ou assujettie à un mandat d'arrêt ou à une déclaration de culpabilité[35].

[21] La victime d'un vol d'identité criminel peut demander à recevoir une déclaration d'innocence factuelle, ou le poursuivant ou le tribunal peut chercher à obtenir une déclaration accélérée à cet effet. Selon les circonstances, la procédure peut être complexe, et le requérant peut avoir le fardeau de prouver qu'il n'existe aucun motif raisonnable de croire qu'il a commis l'infraction en question. Si la demande est accordée, l'ordonnance rendue exigera l'apposition du sceau et la destruction des dossiers en cause[36]. De plus, tout rapport ou dossier des services de police qui fait référence aux rapports d'arrestation scellés doit comprendre une note selon laquelle la personne a été disculpée[37].

[22] Une fois que la demande de déclaration d'innocence factuelle est accordée, la victime peut demander qu'elle soit versée au registre des vols d'identité. Le registre peut alors être consulté par la victime ou les personnes et organismes autorisés par la victime, ainsi que par les organismes du système de justice pénale afin de vérifier que la personne a bel et bien été victime d'un vol d'identité[38].

[23] Plusieurs États, notamment le Colorado, l'Illinois, la Caroline du Nord et le Connecticut, utilisent également le modèle de la déclaration d'innocence factuelle. Des dispositions semblables ont également été adoptées au Minnesota, au Wyoming et en Arizona[39]. Au Connecticut, les dispositions légales permettent au tribunal de rendre une ordonnance exigeant la suppression des renseignements erronés des documents publics[40]. Cette approche a également été recommandée par les groupes de recherche sur l'intérêt public de la confédération d'états et est incluse dans la loi intitulée *Model State Clean Credit and Identity Theft Protection Act.*

Applicabilité de l'une ou l'autre des approches dans le contexte canadien

Approche générale

[24] À travers l'histoire, l'approche de l'aide aux victimes préconisée dans le *Code criminel* a toujours eu une portée étroite. Les articles 738 et 741.2 portent sur les cas où une ordonnance de dédommagement peut être rendue, soit pour le compte de la victime, soit pour celui d'autres personnes, ainsi que de l'exécution de ces ordonnances et de la relation entre ces dispositions et d'autres recours civils.

[25] La répartition constitutionnelle des pouvoirs entre la compétence fédérale en droit criminel et celle des provinces en matière de propriété et de droits civils constitue à la fois un cadre contraignant et nécessaire dans lequel le pouvoir discrétionnaire conféré par ces articles doit être exercé[41]. Consciente de cette contrainte, la Cour a fait remarquer que les dispositions sur le dédommagement ne devaient pas servir à résoudre des questions complexes ou contestées sur la valeur de la propriété ou la perte, ou sur l'interprétation des ententes ou des documents écrits[42]. La Cour a également signalé que la demande de dédommagement était directement associée à la sentence imposée « *à titre de réprobation publique de l 'infraction* »[43].

[26] La réalité de cette contrainte constitutionnelle doit être examinée attentivement quand il s'agit d'adopter toute forme d'approche générale, qu'elle soit déjà utilisée ou que son adoption soit recommandée en Australie. Cette contrainte peut à tout le moins limiter l'incidence de tout certificat à une simple déclaration. Comme nous l'avons déclaré ci-dessus, le fait de limiter le certificat de cette manière a été critiqué en Australie. Il se peut que l'adoption d'un recours d'une utilité si restreinte n'en vaille pas la peine du tout.

[27] De plus, les limites inhérentes à toute ordonnance liée au processus pénal doivent être attentivement examinées. Comme il a été dit ci-dessus, une approche liée à une poursuite criminelle serait trop longue en raison du temps nécessaire pour mener à terme la procédure, ainsi que des délais d'appel. Ces retards peuvent avoir une incidence particulièrement importante pour ce qui est de la réhabilitation des antécédents en matière de crédit de la victime et aussi pour la limite du montant des pertes. Les enquêtes

réalisées auprès des victimes montrent que si l'on tarde trop, ces objectifs ne peuvent plus être atteints.

[28] Tout examen d'un recours lié au processus pénal passe aussi par une réflexion approfondie sur le très faible taux de signalement des vols d'identité dont il a été question auparavant. Si la plupart des cas de vol d'identité ne sont même pas signalés aux autorités, un recours qui ne serait ouvert que sur condamnation au criminel ne serait utile qu'à un petit nombre de victimes. Enfin, il faut analyser toute recommandation d'un recours qui soit lié au processus pénal en fonction des pratiques et procédures civiles existantes. Par exemple, bon nombre de ressorts canadiens préconisent l'utilisation d'une « déclaration de vol d'identité » normalisée pour communiquer avec les agences d'évaluation du crédit et les autres intervenants, quand il s'agit de réparer un vol d'identité[44]. Il faut bien veiller à assurer que tout certificat ou déclaration supplémentaire obtenu dans le cadre du processus pénal ne devienne pas la norme de fait qui supplante les pratiques et les procédures actuelles ou réduise leur efficacité.

[29] Incidemment, il convient de signaler que le groupe de travail n'a pas examiné les autres utilisations potentielles du pouvoir de l'ordonnance de dédommagement dans le *Code criminel*. Les questions qui entourent les autres utilisations de l'ordonnance de dédommagement dans le contexte du vol d'identité ne sont pas visées par le mandat de ce groupe.

Approche restreinte

[30] Le vol d'identité qui donne lieu à un processus pénal ou à une condamnation au criminel au nom d'une partie innocente constitue un grave problème. À cet égard, notons le fait que le nom d'une partie innocente figure dans les dossiers ou les bases de données d'un service de police local ou national lorsque la partie faisant l'objet d'une enquête a utilisé l'identité d'une personne innocente. Ces problèmes peuvent être aggravés par l'échange de renseignements entre les ressorts ou les entités, et ce, au Canada ou au niveau international.

[31] Bien qu'il s'agisse, à n'en pas douter, d'un problème grave, il est nécessaire de procéder à une recherche plus approfondie pour déterminer dans quelle me sure le vol d'identité entraîne l'inscription de renseignements erronés dans les bases de données des

organismes chargés de l'application de la loi et dans celles d'autres organismes au Canada. De plus, il faudrait étudier avec soin le contexte constitutionnel et réglementaire qui régit ces ressources. Enfin, toute solution envisagée devra être évaluée par rapport aux pratiques actuelles afin de bien établir s'il convient d'adopter une approche similaire au Canada.

Obligation de notifier

[32] Le groupe de travail était aussi chargé d'examiner les questions juridiques et politiques afférentes à l'obligation de signaler toute perte de données. Il s'agit d'une question plus généralement connue comme l'« avis d'atteinte à la sécurité des renseignements personnels », c'est-à-dire le fait que les gardiens ou les détenteurs des renseignements personnels doivent donner un avis en cas de perte de renseignements personnels ou si la sécurité de ces renseignements est compromise.

[33] L'un des principaux objectifs de la règle de l'obligation de notifier est de permettre aux victimes éventuelles d'un vol d'identité de se protéger des risques subis du fait de la perte des renseignements personnels les concernant. Cet avis peut permettre aux personnes de prendre des mesures pour se prémunir contre le vol d'identité, notamment une surveillance plus attentive de leurs renseignements financiers, un suivi actif de leur cote de solvabilité, la communication avec les agences d'évaluation du crédit ou la modification par leurs soins des numéros de cartes de crédit ou de comptes bancaires, etc. Il y a toujours un débat quant à savoir quelles sont les mesures les plus efficaces pour réduire les risques de vol d'identité.

[34] Les sociétés émettrices de cartes de crédit, les banques ou les autres groupes peuvent également prendre des mesures pour réagir lorsqu'ils se rendent compte que les renseignements personnels afférents à leurs clients ou consommateurs peuvent avoir été divulgués ou trouvés de manière inappropriée. Par exemple, la Banque Canadienne Impériale de Commerce a, récemment, émis de nouvelles cartes Visa avec des numéros différents lorsqu'une filiale de la banque a craint que des renseignements personnels n'aient été perdus.

[35] Ces mesures, qu'elles soient prises par une personne, par les sociétés émettrices de cartes, par les banques ou par les autres groupes, entraînent des coûts à la fois directs et indirects. De plus, d'autres coûts seront engagés par le gardien ou le détenteur des renseignements personnels en cause qui peuvent prendre la forme des coûts directs engagés pour atténuer les dommages et pour protéger la réputation du gardien ou du détenteur des données contre un préjudice à long terme. Ces coûts peuvent être onéreux, et les éventuels coûts à long terme peuvent obliger les parties à faire plus attention à la sécurité des renseignements personnels.

[36] La présente partie du rapport recense certaines des grandes questions juridiques et politiques auxquelles il faudrait répondre pour ce qui est de la question de l'obligation de notifier.

[37] Il faut poser, dès le départ, qu'il ne s'agit pas d'une question nouvelle en droit ou en ce qui a trait aux politiques en la matière. La plupart des États américains, à commencer par la Californie en 2002, ont adopté des lois exigeant une certaine forme de notification en cas d'atteinte à la sécurité des renseignements personnels. Au niveau fédéral, plusieurs projets de loi ont été présentés, mais sans succès[45].

[38] Au Canada, seule la *Loi de 2004 sur la protection des renseignements personnels sur la santé*[46] de l'Ontario a une disposition portant sur la notification. Certains gouvernements ont des politiques à ce sujet, et des commissaires à la protection de la vie privée ont pris part à la discussion. Plusieurs groupes de défense de l'intérêt public ont également fait la promotion de la notification[47].

[39] Dans cette partie du document de discussion, il sera question de quatre aspects précis afférents à l'avis d'atteinte à la sécurité des renseignements personnels, ainsi que d'autres recours civils disponibles en cas d'atteinte à la sécurité des données. Ces recours pourraient aider les personnes dont les données sont en cause et les autres personnes visées par l'atteinte. En conclusion, il sera question des mesures pour protéger les données personnelles contre toute atteinte.

i) Que signifie l'« atteinte »?

ii) Qui juge s'il y a eu atteinte?

iii) Qui reçoit l'avis?

iv) À quelle réforme du droit faut-il procéder?

i) Que signifie l'« atteinte »?

[40] La fixation de la limite à laquelle la notification est nécessaire est une question délicate. L'avis d'atteinte à la sécurité des renseignements personnels peut avoir d'importantes ramifications pour les personnes et les organismes. La fixation de la limite appropriée pour ce qui est de la notification impose de prendre en compte une vaste gamme de situations où il peut y avoir eu perte de renseignements personnels ou dans lesquelles la sécurité de ces renseignements peut être compromise.

[41] À une extrémité du spectre se trouvent les cas où les données personnelles ont délibérément été ciblées et copiées à partir des bases de données. La situation est moins claire dans les cas où le support d'enregistrement, notamment les bandes, les disques durs externes ou les ordinateurs portatifs, comprenant des renseignements personnels, a été volé. Ce type de vol fait la une des journaux.

[42] Ces derniers cas soulèvent un certain nombre de questions en ce qui concerne le risque réel de diffusion des renseignements personnels en cause. Par exemple, la cible réelle du vol était-elle l'information, l'ordinateur ou l'unité de stockage? Étant donné toute la publicité entourant l'atteinte à la protection des données et la valeur des renseignements personnels, il semble improbable que bon nombre de voleurs ne connaissent pas la valeur éventuelle de ces renseignements.

[43] Des questions encore plus difficiles sont soulevées lorsque la sécurité des renseignements personnels est << compromise >> sans qu'il n'y ait eu vol pur et simple. Il peut être difficile, voir impossible, de déterminer si les renseignements personnels ont été consultés ou copiés dans le cadre d'un accès non autorisé à un système informatique ou une base de données. D'autres événements connexes, notamment l'inhibition des systèmes de sécurité ou de contrôle d'accès, peuvent conduire à se poser la question de l'accès non autorisé. La bonne définition des cas donnant lieu à l'obligation de notifier comporte des difficultés, tant du point de vue technique que juridique. De plus, il faut s'assurer que les limites sont posées en << termes neutres sur le plan technologique >> de

manière à éviter d'être sans cesse en train d'apporter des modifications pour suivre le rythme des progrès de la technologie.

[44] La nature des renseignements personnels en cause peut également être prise en compte quand il s'agit de fixer le seuil approprié pour ce qui est de l'obligation de notifier. Les renseignements financiers personnels, ou le numéro d'assurance sociale, qui peuvent être utilisés pour générer d'autres pièces d'identité, peuvent être plus délicats qu'un simple nom, une adresse et un numéro de téléphone. Les renseignements personnels sur la santé peuvent être très délicats et faire l'objet d'abus.

[45] En ce qui concerne le classement de la nature délicate des renseignements personnels en question, il conviendrait peut-être de tenir compte de la nature des risques qu'entraîne la perte de renseignements. Par exemple, la perte de renseignements peut donner lieu aux problèmes suivants :

> inquiétudes d'ordre physique : que les renseignements puissent être utilisés pour trouver l'adresse du domicile de la personne,
>
> inquiétudes d'ordre opérationnel : que les renseignements puissent être utilisés pour obtenir du crédit ou faire d'autres opérations au nom de la personne,
>
> inquiétudes d'ordre informationnel : que les renseignements puissent être utilisés pour révéler certains faits privés ou personnels, notamment sur l'état de santé ou autres questions personnelles délicates.

[46] Du fait que l'objectif visé par la notification d'une atteinte à la sécurité des renseignements est de permettre de réduire les risques d'utilisation inappropriée des données, bon nombre des lois sur le sujet, notamment le modèle phare de la Californie, dispensent les organisations de l'obligation de notifier si les renseignements ne sont pas susceptibles de porter préjudice à quiconque, notamment du fait qu'ils sont chiffrés. Le fait de stocker des données personnelles sous forme codée est une bonne façon d'obvier à l'obligation de notifier. La plupart des lois américaines ne précisent pas le type de chiffrement nécessaire. Certains systèmes sont beaucoup plus sécuritaires que d'autres.

[47] En l'absence d'une législation, mais pour promouvoir une pratique exemplaire, la commissaire à l'information et à la protection de la vie privée de l'Ontario a récemment publié des documents[48] sur les normes requises pour chiffrer des renseignements personnels sur des appareils mobiles (les appareils les plus susceptibles d'être perdus ou volés). Elle a vivement recommandé de ne pas stocker ce type de renseignements sur ces appareils, mais elle a déclaré qu'autrement, en cas de nécessité, seul serait acceptable du point de vue des normes le chiffrement de grande puissance. La fiche de renseignements est un abécédaire utile sur les différentes méthodes de chiffrement et leurs points faibles. Il faudrait examiner la possibilité que ces normes puissent figurer dans une loi portant sur l'avis d'atteinte à la sécurité des renseignements personnels ou, à tout le moins, dans un règlement d'application.

(ii) Qui juge s'il y a eu atteinte?

[48] Qui décide si l'atteinte est suffisante pour justifier la remise d'un avis? Faudrait-il imposer une exigence concernant l'avis d'atteinte à la sécurité des renseignements personnels dès lors que la sécurité est « compromise » ou éventuellement compromise? Le gardien des données devrait-il être autorisé à décider si l'incident a causé un risque suffisant pour en informer les personnes concernées? On ne devrait pas causer d'inquiétudes et d'inconvénients pour rien. Par ailleurs, la mauvaise publicité qui découle de la notification de personnes incitera fortement à ne pas divulguer et peut altérer le jugement en ce qui concerne la gravité de l'atteinte.

[49] La plupart des lois américaines ne confèrent pas de pouvoir discrétionnaire au gardien des données si la sécurité a été compromise ou si l'atteinte correspond à la définition donnée dans la loi. Toutefois, il existe des différences marquées dans la législation, et des combinaisons diverses de définitions et d'obligations peuvent avoir différents effets.

(iii) Qui reçoit l'avis?

[50] La plupart des lois portant sur le sujet, notamment la *Loi de 2004 sur la protection des renseignements personnels sur la santé* de l'Ontario, exigent qu'un avis soit remis à

la personne dont la sécurité des renseignements personnels a été compromise. Toutefois, certaines lois exigent qu'un avis soit également remis aux organismes de réglementation en matière de protection de la vie privée. Au printemps 2007, le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique fédéral a fait le rapport de son examen quinquennal sur la *Loi sur la protection des renseignements personnels et les documents électroniques*[49]. Le Comité permanent a recommandé que l'avis de violation aux termes de la *Loi sur la protection des renseignements personnels et les documents électroniques* ne soit remis qu'au commissaire à la protection de la vie privée du Canada, et non pas directement à la personne qui pourrait être touchée. Le commissaire étudierait les circonstances et déterminerait s'il est nécessaire d'aviser la personne visée, ainsi que les conditions pertinentes. Ainsi, la décision ne serait pas entièrement laissée aux gardiens des renseignements qui, comme nous l'avons dit, peuvent décider de ne rien dire. On peut se demander, toutefois, si le commissaire devrait intervenir dans la décision de savoir si la personne a besoin d'être protégée d'une atteinte à la sécurité des renseignements la concernant. Pourquoi ne pas laisser la personne décider directement, une fois que le détenteur des données l'a avisée de ce qui s'est produit? Le filtre vise-t-il à éviter que les personnes ne soient indûment bouleversées[50] ou à protéger les gardiens des données de la mauvaise publicité découlant de l'atteinte?

[51] D'autres questions connexes doivent également être examinées, notamment quant à savoir la forme de l'avis et quels autres renseignements doivent y être joints. Par exemple, est-il suffisant de faire paraître un avis dans le journal, ou une autre forme d'avis personnel est-elle nécessaire?

iv) A quelle réforme du droit faut-il procéder?

[52] Cette question comporte deux éléments. Premièrement, faut-il avoir une loi sur l'avis d'atteinte à la sécurité des renseignements personnels ou d'autres solutions de rechange suffisent-elles? Deuxièmement, s'agit-il d'un rôle unique pour cette Conférence, compte tenu des efforts continus de bon nombre d'autres groupes et organisations gouvernementaux et non gouvernementaux dans ce domaine?

a) Faut-il avoir une loi?

[53] On peut dire que la réponse acceptée consiste dans une notification en cas d'atteinte à la sécurité. C'est certainement le cas aux États-Unis. Les entreprises qui ne communiquent pas rapidement une atteinte à la sécurité subissent des conséquences négatives, tant sur le marché des valeurs mobilières que dans les relations avec les clients. De plus, comme il est expliqué de manière plus détaillée ci-dessous, il existe de plus en plus de recommandations et de guides qui émanent d'organismes gouvernementaux et des commissaires à la protection de la vie privée sur ce sujet.

[54] La principale autorité de réglementation en matière de politiques concernant la protection des renseignements personnels au niveau fédéral américain est la Commission fédérale du commerce (bien qu'il y ait des organismes sectoriels dans des domaines dotés de leur propre législation relative à la protection de la vie privée). La Commission fédérale du commerce recommande que les entreprises avisent les organismes chargés de l'application de la loi et les personnes et entreprises visées par une atteinte à la sécurité lorsque la perte de renseignements risque de leur porter préjudice. Elle énumère aussi les facteurs à prendre en compte au moment de décider s'il faut ou non aviser les personnes touchées[51].

[55] La Californie, qui est un pionnier dans le domaine des avis d'atteinte à la sécurité des renseignements personnels, a publié des lignes directrices sous le titre *Recommended Practices on Notice of Security Breach Involving Personal Information*[52].

[56] Au Canada, selon le rapport du Comité permanent portant sur la *Loi sur la protection des renseignements personnels et les documents électroniques*, le commissaire

à la protection de la vie privée discute déjà des atteintes à la sécurité avec les entreprises et les conseille sur la divulgation. Le commissaire a publié un guide en rapport avec cette pratique[53].

[57] Les lignes directrices sur les atteintes à la vie privée publiées par le Conseil du Trésor portent sur les atteintes à la sécurité des renseignements dont dispose le gouvernement et à la libération des obligations du gouvernement en vertu de la *Loi sur la protection des renseignements personnels.* Les lignes directrices comprennent une longue liste de renseignements qu'il est << fortement recommandé >> de divulguer aux victimes, et ce, << dans la mesure du possible >>.

[58] Au niveau provincial, la commissaire à l'information et à la protection de la vie privée de l'Ontario et son homologue de la Colombie-Britannique ont publié un document intitulé *Breach Notification Assessment Tool*[54]. Il y est écrit que [TRADUCTION]<< les organisations qui recueillent et détiennent des renseignements personnels sont tenues d'aviser les victimes en cas d'atteinte à la vie privée. >> Aucun fondement juridique n'est donné à cette déclaration. Il est ensuite question, dans le document, de l'analyse de six facteurs de risque qui devrait être faite au moment de décider de remettre un avis ou non. Le document comprend également une liste de facteurs à prendre en compte au moment de décider comment aviser les personnes (directement ou indirectement) et quels renseignements inclure dans l'avis. Pour finir, le document comprend une liste d'autres personnes avec qui communiquer éventuellement, à commencer par les agents chargés de l'application de la loi, ainsi que le(s) commissaire(s) à la protection de la vie privée approprié(s). D'autres ressources sont disponibles auprès du commissaire de la Colombie-Britannique, notamment le document intitulé *Key Steps in Responding to Privacy Breaches* et le formulaire intitulé *Privacy Breach Notification Form* qui sert à aviser le commissaire d'une atteinte[55]. La commissaire à la protection de la vie privée de l'Ontario a également publié des lignes directrices destinées aux gouvernements qui ont été victimes d'une atteinte à la protection des données[56].

[59] À l'heure actuelle, les opinions sont partagées quant à la nécessité d'imposer la notification. Par exemple, ni le commissaire à la protection de la vie privée fédéral ni celui de la Colombie-Britannique n'ont recommandé une notification obligatoire

lorsqu'ils ont témoigné au cours du récent examen parlementaire de la *Loi sur la protection des renseignements personnels et les documents électroniques*. Le commissaire de la Colombie-Britannique a dit ceci, en particulier : « nous devrions attendre d'avoir plus d'expérience dans l'application de la loi pour déterminer si une notification obligatoire constitue un moyen efficace et économique de réduire les risques d'usurpation d'identité pouvant découler de fuites de renseignements personnels »[57].

[60] Des préoccupations ont également été exprimées en ce qui concerne l'incidence de l'avis d'atteinte à la sécurité des renseignements personnels sur la responsabilité des détenteurs de données pour toute perte pouvant découler d'une atteinte. On irait à l'encontre du but recherché si l'effet de la notification était de fournir une protection au détenteur des données qui transfèrerait toute la responsabilité de l'atténuation des pertes aux victimes de l'atteinte. Il est nécessaire de faire d'autres études sur cette question afin de déterminer l'incidence ultime des mécanismes d'avis d'atteinte à la sécurité des renseignements personnels à cet égard.

[61] Toutefois, la commissaire de l'Ontario est en faveur de mesures législatives de cet ordre[58], tout comme bon nombre de groupes d'intérêt public, notamment le Centre pour la défense de l'intérêt public[59] et la Clinique d'intérêt public et de politique d'internet du Canada[60]. Un de leurs grands arguments tient à l'uniformisation des pratiques. Un régime facultatif, bien qu'il soit persuasif, crée une incertitude quant à l'interprétation et à l'application et peut, du moins à court terme, aboutir à récompenser les gardiens actuels ou futurs des renseignements personnels qui soient peu scrupuleux.

b) Le rôle éventuel de la Conférence pour l'harmonisation des lois

[62] La deuxième question de la présente partie du document consiste à savoir si la Conférence pour l'harmonisation des lois aura un rôle à jouer dans ce processus. Divers aspects du vol d'identité font actuellement l'objet d'une étude par plusieurs groupes de travail, groupes d'intérêt public et commissaires à la protection de la vie privée, et ce, au Canada et dans d'autres pays.

[63] Par exemple, le Comité des mesures en matière de consommation fédéral-provincial-territorial a publié un long document de discussion intitulé *Travailler*

ensemble pour pré venir le vol d'identité[61]. Ce document aborde bon nombre des questions examinées dans le présent document. À l'heure actuelle, le Comité n'a formulé aucune recommandation, tout comme Industrie Canada, le ministère parrain du Comité à Ottawa, au Comité permanent pour ce qui est de son examen de la *Loi sur la protection des renseignements personnels et les documents électroniques*. Une étude réalisée en 2005 par le gouvernement albertain montre que quinze comités gouvernementaux et groupes de travail différents ont étudié cette question, en plus de quatorze autres groupes industriels ou groupes de réglementation dotés de politiques sur le sujet ou prévoyant en avoir sous peu. La législature du Québec a adopté plusieurs dispositions dans son cadre juridique concernant la législation en matière de technologie de l'information, de protection de la vie privée et de consommation, et ce, pour empêcher l'usurpation d'identité. Ces dispositions entraînent aussi des obligations qui peuvent mener à des recours civils et à des sanctions pénales. Le Québec participe également au Groupe de travail intergouvernemental de la gestion de l'identité et de l'authentification afin de concevoir un moyen, notamment des méthodes de gestion des risques, pour prévenir l'usurpation d'identité.

[64] Toutefois, nous estimons qu'il est possible de militer avec raison en faveur d'une approche cohérente à cette question par tous les ordres de gouvernement. Bon nombre d'organisations au Canada exploitent des activités dans plusieurs provinces ou territoires et détiennent des données sur des personnes qui sont dans plusieurs ressorts. Ces organisations tireraient grandement profit de l'adoption de règles uniformes sur l'intervention en cas d'atteinte aux données, même en l'absence d'une législation uniforme globale.

[65] Quoi qu'il en soit, le gouvernement fédéral pourrait tirer profit de l'élaboration d'une politique pancanadienne à ce sujet. Cela aurait également pour avantage de faciliter l'harmonisation des lois provinciales, territoriales et fédérales, permettant ainsi d'éviter des questions constitutionnelles délicates sur la portée idéale des obligations statutaires de chaque ordre de gouvernement.

[66] De plus, la *Loi sur la protection des renseignements personnels et les documents électroniques* ne traite pas de plusieurs types importants de renseignements, notamment les renseignements intraprovinciaux sur l'emploi, l'utilisation des renseignements à une

fin autre que commerciale ou les actes des gouvernements en tant que détenteurs ou gardiens des données. L'élaboration de politiques avec une approche multijuridictionnelle uniforme permettrait de donner une plus grande portée à la protection cohérente dans tout le pays.

CONCLUSION

[67] Le vol d'identité est un problème grave qui croît en importance. Il cause d'importantes pertes financières et, dans bon nombre de cas, des préjudices permanents aux victimes. Compte tenu de ces faits, il n'est pas étonnant que ce sujet ait fait l'objet de plusieurs études par des groupes de travail existants, notamment un Groupe de travail fédéral-provincial-territorial (le groupe de travail du Comité des mesures en matière de consommation), qui a récemment terminé un examen parlementaire de la *Loi sur la protection des renseignements personnels et les documents électroniques,* ainsi que plusieurs commissaires à la protection de la vie privée, et plusieurs initiatives lancées par les divers gouvernements provinciaux. La communauté internationale, notamment le comité des avocats en droit pénal modèle (Model Criminal Law Officers Committee) de l'Australie, travaille également sur la question.

[68] Les travaux entrepris par chacun de ces groupes devront être supervisés pour éviter tout chevauchement ou double emploi avec tout futur travail entrepris par la présente Conférence. Le présent groupe de travail a reçu le mandat d'examiner deux questions précises. Comme on peut en juger d'après le nombre de pages du présent rapport, ces questions précises ont soulevé des questions complexes exigeant un examen plus détaillé. Il faudra donc aussi veiller à ce que la portée des mandats à venir soit assez claire pour permettre un examen détaillé opportun.

[69] Trois grandes conclusions peuvent être tirées de l'expérience du présent groupe de travail afin d'aider à préciser les mandats du groupe de travail en cours ou à venir :

[70]

1) Certaines recherches empiriques montrent que le vol d'identité est très peu signalé aux services de police ou aux autres organismes et que les délais sont de

rigueur pour ce qui est de fournir une aide efficace aux victimes et de leur permettre de contrer les répercussions du vol d'identité. De ce fait, on peut dire qu'à l'exception de l'approche de la déclaration d'innocence factuelle décrite ci-dessus, les recours civils peuvent offrir une aide plus efficace et plus opportune que les ordonnances rendues accessoirement dans le cadre du processus pénal.

2) En plus de l'examen continu des questions recensées concernant l'avis d'atteinte à la sécurité des renseignements personnels, **d'autres recours civils et sanctions pénales devraient être examinés, notamment ceux qui existent déjà dans les divers ressorts pour ce qui est de leurs lois sur la protection de la vie privée ou autrement.** Que ce soit au Canada, aux États-Unis ou ailleurs dans le monde, il existe une vaste gamme d'autres recours civils qui ont été adoptés, notamment le droit à des rapports de solvabilité gratuits, au gel de l'accès aux dossiers de crédit et à des dommages-intérêts légaux précis en cas d'atteinte à la sécurité des données. L'examen des recours civils et des approches devrait être axé d'abord sur les domaines les plus utiles pour les victimes d'un vol d'identité. Il pourrait s'agir, entre autres, de recours qui permettent la découverte rapide d'un éventuel vol d'identité, ainsi que de mesures à adopter pour réduire le risque ultime de vol ou les préjudices portés aux antécédents en matière de crédit ou aux autres aspects de l'identité personnelle touchés de façon néfaste.

3) La Conférence devrait tenir compte de la possibilité de procéder à un examen des mesures pouvant être adoptées pour accroître la sécurité des renseignements personnels et des mesures et pratiques qui réduiraient les risques de vol d'identité. De telles mesures préventives font partie intégrante de bon nombre des interventions législatives dans le cadre d'un vol d'identité.

[71] Compte tenu de ces conclusions et de l'avantage qu'il y a à une grande participation ou représentation de plusieurs ressorts, le groupe de travail recommande que tous les ressorts prennent part aux travaux permanents envisagés par le groupe, plus précisément :

1) que le groupe de travail élabore un cadre fondé sur des principes pour le régime de l'avis d'atteinte à la sécurité des renseignements personnels, lequel pourrait être utilisé dans tous les ressorts, en plus de procéder à un examen des recours et processus civils connexes;

2) que le groupe de travail procède à un examen détaillé des recours et des processus disponibles pour venir en aide aux victimes de vol d'identité lorsque des casiers judiciaires ou d'autres dossiers officiels ont, par erreur, été créés au nom de la victime;

3) que l'objectif à long terme du groupe soit d'examiner l'atteinte à la sécurité de l'identité et les mesures à prendre pour améliorer la sécurité des pièces d'identité et des pratiques afin de réduire le risque de vol d'identité.

---

[1] L'expression courante << vol d'identité >> ne fait pas l'unanimité. Le Groupe de travail reconnaît que dans ce contexte, le terme << vol >> peut être inexact, car il évoque effectivement des notions d'<< identité >> à titre de propriété et de << vol >> à titre de privation. La victime d'un vol d'identité n'est pas privée de son identité, bien qu'elle ait pu perdre son argent, son temps et sa réputation. Toutefois, << vol d'identité >> est l'expression courante. Cette expression est utilisée dans le présent rapport, sous réserve de cette mise en garde.

[2] Ces statistiques sont disponibles à l'adresse suivante : http://www.phonebusters.com/francais/statistics_E02.html.

[3] *L 'abc du vol d 'identité,* publié par le Commissariat à la protection de la vie privée du Canada et disponible à l'adresse suivante : http://www.privcom.gc.ca/id/primer_f.asp.

[4] *L 'abc du vol d 'identité,* précité.

[5] *Federal Trade Commission – Identity Theft Survey Report,* Synovate Research, pages 9, 50.

[6] *Rapport sur le vol d 'identité,* Groupe de travail binational sur les fraudes transfrontalières par marketing de masse, octobre 2004, disponible à l'adresse suivante : http://www.securitepublique.gc.ca/prg/le/bs/report-fr.asp.

[7] *Travailler ensemble pour prévenir le vol d'identité : Document de discussion aux fins de consultation publique,* Comité des mesures en matière de consommation, page 2. Certaines de ces difficultés peuvent être surmontées par l'initiative envisagée par Statistique Canada dans le rapport intitulé *Rapport sur la faisabilité d'améliorer la mesure de la fraude au Canada* disponible à l'adresse suivante : http://www.statcan.ca/francais/freepub/85-569-XIF/85-569-XIF2006001.htm.

[8] BAUM, Katrina. *First Estimates from the National Crime Victimization Survey: Identity Theft,* 2004, Bureau of Justice Statistics, disponible à l'adresse suivante : http://www.ojp.usdoj.gov/bjs/////////pub/pdf/it04.pdf.

[9] << FTC Releases Top 10 Consumer Fraud Complaint Categories >>, 25 janvier 2006, disponible à l'adresse suivante : http://www.ftc.gov/opa/2006/01/topten.shtm.

[10] Selon le résumé de Privacy Rights Clearinghouse, mise à jour de février 2006, disponible à l'adresse suivante : http://www.privacyrights.org/ar/idtheftsurveys.htm.

[11] Une version gratuite de l'étude est disponible à l'adresse suivante : http://www.javelinstrategy.com/research/2. Certaines des controverses entourant ces conclusions sont résumées à l'adresse suivante : http://blog.washingtonpost.com/thecheckout/2007/02/is identity theft decreasing.html.

[12] *Identity Fraud: A Study*, Cabinet Office, juillet 2002, disponible à l'adresse suivante : http://www.identitycards.gov.uk/downloads/id_fraud-report.pdf.
[13] Home Office Identity Fraud Steering Committee, disponible à l'adresse suivante : http://www.identitytheft.org.uk/what-is-being-done.htm.
[14] *Updated Estimate of the Cost of Identity Fraud to the UK Economy*, février 2006, disponible à l'adresse suivante : http://www.identitytheft.org.uk/ID%20fraud%20table.pdf.
[15] *How Serious is the Problem*, CIFAS Online, disponible à l'adresse suivante : http://www.cifas.org.uk/identity_fraud_is_theft_serious.asp.
[16] *Fraud and Identity Theft*, document préparatoire rédigé par Roza Lozusic, Parlement de la Nouvelle-Galles du Sud, Australie, disponible à l'adresse suivante : http://www.parliament.nsw.gov.au/prod/parlment/publications.nsf/0/08ACDBBA372ED89DCA256ECF0007C146.
[17] *Fraud and Identity Theft*, précité. Voir également le *Rapport sur le vol d 'identité*, précité.
[18] *Rapport sur le vol d 'identité*, précité.
[19] *Identity Theft: The Aftermath 2004*, Identity Theft Resource Center, page 12. Les rapports de 2003 et de 2004 sont disponibles à l'adresse suivante : http://www.idtheftmostwanted.org/artman2/publish/lib_survey/index.shtml. Il n'est pas facile de savoir quelle incidence ont eu les exigences législatives en matière d'avis d'atteinte à la sécurité des renseignements personnels sur ces chiffres.
[20] *Identity Theft Survey Report*, précité, page 40.
[21] *Identity Theft: The Aftermath 2004*, précité, pages 2, 13 et 14.
[22] *Identity Theft Survey Report*, précité, pages 6, 45 et 46.
[23] *Identity Theft: The Aftermath 2004*, précité, page 14.
[24] *Identity Theft: The Aftermath 2004*, précité, pages 8 et 9.
[25] *Identity Theft Survey Report*, précité, pages 6 et 37.
[26] *Identity Theft Survey Report*, précité, pages 46 et 47.
[27] *Identity Theft: The Aftermath 2004*, précité, pages 14 et 15.
[28] *Identity Theft Survey Report*, précité, pages 8,41, 43, 45 et 46.
[29] Article 54, *Criminal Law (Sentencing) Act 1988.*
[30] La justification sous-jacente aux certificats figure dans le document intitulé *Discussion Paper: Identity Crime*, Model Criminal Law Officers Committee, page 28. Ce document est disponible à l'adresse suivante : http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(4341200FE1255EFC59DB7A1770C1D0A5)~MCLOC-draft-identity-crime-discussion-paper-march+2007.pdf/$file/MCLOC-draft-identity-crime-discussionpaper-march+2007.pdf.
[31] Cette limite a également été prise en compte par d'autres observateurs. Voir, par exemple, STEWARD, Jeremy Douglas. « South Australian Laws Target Identity Theft », [2004], *Privacy Law and Policy Reporter* 8, disponible à l'adresse suivante : http://www.austlii.edu.au//cgi-bin/disp.pl/au/journals/PLPR/2004/8.html?query=identity%20theft.
[32] Discussion Paper, précité, page 28.
[33] BLINDELL, James. *Review of the Legal Status and Rights of Victims of Identity Theft in Australia*, Australian Centre for Policing Research, 2006.
[34] Projet de loi 794 du sénat du Michigan, disponible à l'adresse suivante : http://www.legislature.mi.gov/(S(jh22nhnfwzfnxv55jlvhts45))/mileg.aspx?page=getObject&objectName=2003-SB-0794.
[35] La nature, la portée et la fonction de ces dispositions sont décrites dans certains documents disponibles auprès du bureau de la protection de la vie privée du ministère de la protection du consommateur de la Californie. Un aperçu de ces éléments figure dans le document intitulé *How to Use the California Identity Theft Registry: A Guide for Victims of « Criminal » Identity Theft*, disponible à l'adresse suivante : http://www.privacy.ca.gov/cover/identitytheft.htm.
[36] Article 530.6 et alinéas 851 .8*a)* et *d)* du code pénal de la Californie.
[37] Alinéa 851 .8*h)* du code pénal de la Californie.
[38] Article 530.7 du code pénal de la Californie.
[39] Minnesota HF 1943, Séance 84, Sénat du Wyoming, dossier SF0053, Arizona HB 2716.

[40] Statistiques comparées de l'Illinois § 5/16G-30; 2005, N.C. ALS 414, Statistiques générales du Connecticut § 54-93a.
[41] ***R. c. Zelensky,*** [1978] CarswellMan 51 au paragraphe 4 (C.S.C.) au paragraphe 33.
[42] ***Zelensky,*** précité, au paragraphe 34. Un autre exemple peut être celui de l'incapacité d'utiliser ces dispositions pour récupérer les coûts de renonciation, plutôt que les pertes plus directes – ***R. v. Brunner,*** (1995) 97 C.C.C. (3d) 31 (C.A. Alta.).
[43] ***Zelensky,*** précité, paragraphe 28.
[44] Voir, par exemple, la trousse d'information sur le vol d'identité des consommateurs produite par le groupe de travail sur le vol d'identité du Comité des mesures en matière de consommation disponible à l'adresse suivante : http://cmcweb.ca/epic/site/cmc-cmc.nsf/fr/fe00084f.html.
[45] Consulter la page Web portant sur l'atteinte à la sécurité des renseignements affichée sur le site de la Conférence nationale des législatures d'État pour obtenir les liens vers la législation et les ressources afférentes, et ce, à l'adresse suivante : http://www.ncsl.org/programs/lis/cip/priv/breach.htm, ainsi que l'annexe de l'étude réalisée par la CIPPIC, citée ci-après, à la note 47.
[46] L.O. 2004, chapitre 3, annexe A, par. 12(2). Disponible en ligne à l'adresse suivante : http://www.e-laws.gov.on.ca/DBLaws/Statutes/French/04p03_f.htm.
[47] Voir notamment le document publié par la Clinique d'intérêt public et de politique d'internet du Canada (CIPPIC) intitulé *Approaches to Security Breach Notification: A White Paper*, 9 janvier 2007, disponible à l'adresse suivante : http://www.cippic.ca/en/bulletin/BreachNotification_9jan07-web.pdf.
[48] Commissaire à l'information et à la protection de la vie privée (Ontario), *Safeguarding Privacy in a Mobile Workplace: Protect the Information you keep on your laptops, cellphones and PDAs* (juin 2007), disponible à l'adresse suivante : http://www.ipc.on.ca/images/Resources/up-mobilewkplace.pdf. Voir également *Fact Sheet: Encrypting Personal Health Information on Mobile Devices*, mai 2007, disponible à l'adresse suivante : http://www.ipc.on.ca/images/Resources/up-1fact_12_e.pdf.
[49] L.C. 2000 ch. 5, partie 1. Le rapport peut être consulté en ligne à l'adresse suivante : http://cmte.parl.gc.ca/cmte/CommitteePublication.aspx?COM=0&SourceId=204322&SwitchLanguage=1.
[50] Le Comité a entendu parler d'un cas en Colombie-Britannique où les données illégalement divulguées étaient des renseignements sur la santé de patients atteints de maladie mentale qui vivaient en établissement. Le commissaire de la Colombie-Britannique a dû examiner l'incidence de cette divulgation sur ces personnes vulnérables. (Délibérations du 6 décembre 2006.)
[51] Sur le vol d'identité en général : http://www.ftc.gov/bcp/edu/microsites/idtheft/index.html (ce document peut également être consulté à l'adresse suivante : http://www.consumer.gov/idtheft). Pour les personnes dont la sécurité des renseignements peut avoir été compromise : *If your information has been compromised, but not yet misused*, disponible à l'adresse suivante : http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/compromised.html. Pour les entreprises : *Information Compromise and the Risk of Identity Theft: Guidance for Your Business*, disponible à l'adresse suivante : http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus59.shtm.
[52] California Office of Privacy Protection, février 2007, *Recommended Practices on Notice of Security Breach Involving Personal Information*, disponible à l'adresse suivante : http://www.privacy.ca.gov/recommendations/secbreach.pdf.
[53] Commissariat à la protection de la vie privée du Canada, *Les entreprises et le vol d'identité*, mars 2007, http://www.privcom.gc.ca/id/business_f.asp.
[54] Décembre 2006, http://www.oipcbc.org/pdfs/Policy/ipc_bc_ont_breach.pdf.
[55] Consulter la liste complète à l'adresse suivante : http://www.oipcbc.org/sector_private/resources/index.htm.
[56] *What to do if a privacy breach occurs: Guidelines for government organizations*, http://www.ipc.on.ca/images/Resources/up-prbreach.pdf. Un document semblable a été publié pour les organisations chargées des renseignements sur la santé, *What to do when faced with a privacy breach: guidelines for the health care sector*, http://www.ipc.on.ca/images/Resources/up-hprivbreach.pdf.
[57] LOUKIDELIS, David. Témoignage devant le comité, 29 novembre 2006.
[58] Commissaire à l'information et à la protection de la vie privée (Ontario), *Do the right thing, Ontario, make a move now to fight ID theft*, communiqué de presse, 6 février 2007, http://www.ipc.on.ca/images/Resources/up-2007_02_06_idtheft.pdf.

[59] Centre pour la défense de l'intérêt public, *Canadian Consumer Initiative Identity Theft Policy Position*, février 2005, http://www.piac.ca/financial/canadian_consumer_initiative_identity_theft_policy_position.

[60] CIPPIC, précité, note 47.

[61] Comité des mesures en matière de consommation, juillet 2005, http://www.cmcweb.ca/epic/site/cmc-cmc.nsf/vwapj/Document%20de%20discussion_Volidentite.pdf/$FILE/Document%20de%20discussion_Volidentite.pdf. Voir les ressources générales sur le vol d'identité du Comité des mesures en matière de consommation destinées aux consommateurs et aux entreprises à l'adresse suivante : http://cmcweb.ca/epic/site/cmc-cmc.nsf/fr/fe00084f.html.