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 : RAPPORT D'ÉTAPE

Veuillez noter que les idées ou conclusions formulées dans ce document ainsi que les éventuelles propositions de dispositions législatives, recommandations ou commentaires n'ont pas été adoptés par la Conférence pour l'harmonisation des lois au Canada et ne reflètent pas nécessairement le point de vue de la Conférence et de ses participants.

Québec
Août 2008

Rapport du groupe de travail
Août 2008

Introduction

[1] Le vol d'identité, ou usurpation d'identité, constitue un problème majeur qui soulève des questions complexes tant pour les particuliers que pour les gouvernements et le système judiciaire. En 2006, un groupe de travail conjoint de la section pénale et de la section civile a été constitué afin d'examiner certaines de ces questions. Le groupe a présenté son premier rapport lors de la conférence de 2007. À la suite de ce rapport, la Conférence a adopté la résolution suivante :

> *1. que le Groupe de travail conjoint sur le vol d'identité de la section pénale et de la section civile :*
> *a) élabore un cadre fondé sur des principes pour le régime de notification des atteintes à la confidentialité des renseignements personnels, lequel pourrait être utilisé dans tous les ressorts, en plus de procéder à un examen des recours et processus civils connexes;*
> *b) 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.*

[2] Ces deux questions sont abordées dans le rapport qui suit.

[3] Le groupe de travail est formé 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) Gail Mildren – avocate générale, Bureau du contentieux civil, Justice Manitoba
7) Lynne Kohm – procureur principal de la Couronne, Division de l'élaboration et de l'analyse des politiques, Justice Manitoba
8) Joe Pendleton – directeur, unité des enquêtes spéciales, Solliciteur général de l'Alberta

La notification des atteintes à la confidentialité des renseignements personnels : options pour un cadre fondé sur des principes

[4] Lors de la Conférence pour l'harmonisation des lois au Canada de 2007, le groupe de travail sur le vol d'identité a remis un document de discussion sur divers aspects du vol d'identité, qui comprenait une section sur les lois qui imposent aux détenteurs de renseignements personnels de communiquer avec les personnes dont les informations personnelles ont été volées, perdues ou autrement compromises[1]. L'objectif de l'obligation de notifier les atteintes à la confidentialité des renseignements personnels est d'aider les gens à se prémunir contre l'utilisation inappropriée de leurs renseignements personnels lorsque ceux-ci ont été communiqués au-delà de ce à quoi ils ont consenti ou pourraient raisonnablement s'attendre.

[5] Lors d'une séance conjointe des sections pénale et civile de la Conférence, il a été résolu, entre autres choses[2], que « le Groupe de travail conjoint sur le vol d'identité de la section pénale et de la section civile …élabore un cadre fondé sur des principes pour le régime de notification des atteintes à la confidentialité des renseignements personnels, lequel pourrait être utilisé dans tous les ressorts, en plus de procéder à un examen des recours et processus civils connexes… »

[6] Le présent document fait suite à cette résolution : il énumère les options possibles quant à un cadre de principe applicable à un régime de notification des atteintes à la confidentialité des renseignements personnels. Ces diverses possibilités sont présentées sous des titres distincts :

a. Quels sont les renseignements visés par le régime de notification des atteintes à la confidentialité des renseignements personnels?

b. Quels sont les détenteurs de renseignements personnels qui sont visés?

c. Comment détermine-t-on qu'il y a eu atteinte ou que la confidentialité a été compromise?

d. Quand doit-on signaler qu'il y a eu atteinte ou que la confidentialité a été compromise?

e. Qui détermine si une atteinte a eu lieu et si elle doit être signalée?

f. Quelle réponse doit-on apporter à l'atteinte?

g. Que doit indiquer l'avis de notification de l'atteinte?

h. Comment assure-t-on l'application de ces obligations?

i. Que doit-on inclure d'autre dans le cadre en cause?

j. Quelle forme devrait prendre la loi uniforme?

a) Quels sont les renseignements visés par le régime de notification des atteintes à la confidentialité des renseignements personnels?

[7] Le fait que les renseignements visés soient les renseignements personnels qui sont en la possession des détenteurs de ces renseignements ne semble pas être matière à controverse. En théorie, dans les ressorts d'édiction, le législateur adopterait la définition des renseignements personnels prévue dans les lois qui régissent leur protection, pour les fins de la notification des atteintes. Toute mesure législative sur la notification des atteintes devrait être rédigée de manière à pouvoir s'insérer dans la législation sur le respect de la vie privée.

[8] Il est possible que certains ressorts aient adopté des définitions différentes pour différentes fins. À titre d'exemple, toutes les provinces se sont dotées d'une législation qui protège le caractère privé des renseignements personnels dans le secteur public, mais seulement trois d'entre elles disposent d'une législation qui le protège de façon générale dans le secteur privé. Ainsi, dans les sept autres provinces et les trois territoires, l'utilisation commerciale des renseignements personnels relève de la loi fédérale, la *Loi sur la protection des renseignements personnels et les documents électroniques* (LRPDE). La LRPDE peut contenir une définition des renseignements personnels différente de celle qui existe dans la législation relative au secteur public. Les dispositions législatives des trois provinces qui ont adopté leur propre législation relative au secteur privé se sont révélées similaires pour l'essentiel à la LRPDE du point de vue de leur fonctionnement, mais les mêmes problèmes se posent lorsque leur définition des renseignements personnels n'est pas identique.

[9] Cependant, en pratique, il ressort que les définitions de « renseignements personnels » contenues dans l'ensemble des législations canadiennes sur la protection des renseignements

personnels partagent un trait commun : les renseignements relatifs à une personne identifiable. Il existe des différences quant à l'exigence que ces renseignements soient enregistrés pour que la loi s'applique. Les principes exprimés dans ce document sont présumés s'appliquer dans tout le pays sans tenir compte des différences existant entre les diverses définitions législatives.

[10] Il convient de rappeler que certaines provinces disposent d'une législation distincte pour protéger les renseignements personnels sur la santé. Hormis les questions de définition, les renseignements personnels relatifs à la santé doivent-ils être régis par la politique relative à la notification des atteintes à la confidentialité des renseignements personnels? Existe-t-il une raison qui fasse en sorte qu'il soit plus difficile ou moins approprié d'appliquer cette politique aux gardiens ou aux fiduciaires qui détiennent des renseignements personnels en matière de santé? Ces gardiens ou fiduciaires peuvent être des organismes du secteur public, tels que des ministères gouvernementaux et la plupart des hôpitaux, ou des organismes privés, tels que des laboratoires, ou encore des organismes parapublics, tels que des cliniques. Les médecins praticiens appartiennent également pour la plupart au secteur privé. Leur capacité de stockage de renseignements personnels peut être assez diversifiée au sein d'une même province et au sein du pays. De la même manière, leur faculté à analyser les atteintes et à en aviser les personnes concernées peut varier considérablement. Cependant, de telles différences sont mieux traitées au moyen de règles de fond, et non en privant les gens de cette protection en raison du secteur auquel appartient le détenteur de leurs renseignements personnels.

[11] **Recommandation :** le régime de notification des atteintes devrait être applicable à toutes les catégories de renseignements personnels protégés par les lois du ressort d'édiction[3].

b) Quels sont les détenteurs de renseignements personnels qui sont visés?

[12] La réponse à cette question a été envisagée lors de la discussion précédente. Les personnes dont la confidentialité des renseignements personnels a été compromise ont besoin de la même protection, peu importe qui détenait les renseignements personnels à ce moment-là. La loi étant applicable à différents groupes de détenteurs, la forme de celle-ci peut soulever certaines questions. Ce sujet est traité plus loin dans le rapport.

[13] **Recommandation :** la politique devrait être applicable à tous les détenteurs de renseignements personnels qui sont assujettis à la législation sur la protection des renseignements personnels dans le ressort d'édiction.

c) Comment détermine-t-on qu'il y a eu atteinte ou que la confidentialité a été compromise?

[14] Pour pouvoir répondre à cette question, nous devons nous projeter au-delà des exigences de la législation applicable en matière de sécurité des renseignements personnels. Chacune de ces législations fait peser sur le détenteur de renseignements personnels une certaine obligation d'en prendre soin, quoiqu'elle ne donne généralement pas beaucoup d'orientation particulière quant à la conduite ou au comportement à adopter[4]. Il arrive parfois que des normes privées s'appliquent également. Les plus connues sont les normes de sécurité des données de l'industrie des cartes de paiement (ICP), conçues par les principaux émetteurs de cartes[5]. De la même manière, les commissaires à la protection de la vie privée ont proposé des pratiques exemplaires pour les mesures de sécurité[6]. Cependant, même si les normes législatives, réglementaires ou de l'industrie ont été respectées, il est possible que des renseignements personnels soient perdus, volés ou que leur sécurité soit compromise. Après tout, la nécessité pour les personnes visées par les données de se protéger elles-mêmes ne dépend pas du soin avec lequel les renseignements ont été protégés avant d'avoir été perdus, volés ou que leur sécurité ait été compromise[7].

[15] La Conférence pour l'harmonisation des lois au Canada n'a pas pour mission d'élaborer des normes de sécurité des renseignements en vue de protéger leur confidentialité. Il est possible, cependant, d'étudier les principales méthodes en vertu desquelles la sécurité des renseignements personnels peut être compromise, que l'on se fonde sur les principes de base de la gestion de l'information ou sur les rapports d'atteinte à la protection des données qui ont été portés à l'attention du public[8]. Cette liste ne donne qu'une indication du type de situations possibles.

- Une atteinte physique : le ou les ordinateurs dans lesquels sont stockées les données étaient dans une pièce fermée. La serrure a été forcée et les ordinateurs ont été emmenés.

- Une atteinte physique : le ou les ordinateurs dans lesquels sont stockées les données étaient dans une pièce fermée. La serrure a été forcée et les ordinateurs sont toujours là. Il est (n'est pas) possible de dire si les renseignements ont été consultés.
- Une atteinte physique : le ou les ordinateurs dans lesquels sont stockées les données étaient dans une pièce fermée, mais la serrure a été laissée ouverte pendant une certaine période au cours de laquelle une personne n'appartenant pas à l'organisation est peut-être entrée.
- Une atteinte physique : l'ordinateur portable contenant des renseignements personnels a été volé, que ce soit au bureau, dans la voiture ou au domicile d'un employé.
    a. On ne retrouve jamais l'ordinateur portable.
    b. On retrouve l'ordinateur portable, mais il (n'est pas) possible de dire si les renseignements ont été consultés.
    c. Les renseignements figurant dans l'ordinateur portable étaient protégés d'une certaine manière :
        i. Ils se trouvaient dans un fichier protégé par mot de passe
        ii. Ils étaient cryptés (par une méthode plus ou moins fiable)
        iii. Ils étaient anonymisés ou dissociés d'une autre manière de la personne
- Une atteinte virtuelle : un système électronique d'accès au renseignement personnel n'était pas sécuritaire contre les accès non autorisés, provenant de l'intérieur ou de l'extérieur de l'organisation.
- Une atteinte virtuelle : un système électronique d'accès au renseignement personnel n'était pas sécuritaire contre les accès non autorisés, provenant de l'intérieur ou de l'extérieur de l'organisation, et on a la preuve qu'il a été consulté sans autorisation.
- Une atteinte virtuelle : des pirates informatiques ont pénétré dans un système électronique d'accès au renseignement personnel en se servant d'une vulnérabilité connue du système.
- Une atteinte virtuelle : des pirates informatiques ont pénétré dans un système électronique d'accès au renseignement personnel en se servant d'une vulnérabilité nouvelle et jusque-là inconnue du système.

[16] Le but de la notification des atteintes à la confidentialité des renseignements personnels est de permettre aux gens de prendre des mesures pour se prémunir contre toute utilisation frauduleuse de leurs renseignements personnels. Ainsi, le risque d'utilisation frauduleuse constitue l'un des principaux éléments justifiant la nécessité d'une telle notification. Bien qu'une protection insuffisante des renseignements personnels puisse être constitutive d'une violation à la loi en cause (même si, comme nous l'avons indiqué, la plupart des lois manquent de précision quant au niveau de soin requis), il est permis de penser que l'obligation de notifier ne devrait intervenir qu'en présence d'un risque grave qu'une personne ait accédé dans les faits aux données en question. L'existence d'une simple possibilité ne suffit pas. Cependant, la durée pendant laquelle une telle possibilité existait peut avoir une incidence sur l'obligation. À titre d'exemple, si un site Internet a autorisé l'accès à des renseignements personnels pendant six mois, la sécurité des renseignements risque davantage d'être compromise que si cette vulnérabilité n'avait duré qu'une fin de semaine.

[17] Les lignes directrices en matière de notification des atteintes à la vie privée publiées par le Commissaire à la protection de la vie privée du Canada évoquent le cas d'un ordinateur portatif volé avec « des renseignements convenablement encodés ». Si l'ordinateur portatif a été récupéré et qu'une analyse démontre que les renseignements n'ont pas été altérés, alors le document du Commissaire à la vie privée suggère qu'il n'est peut-être pas nécessaire de procéder à une telle notification[9].

[18] L'atteinte dont nous faisons mention aboutit à la consultation ou à la divulgation inappropriée de renseignements personnels. Le présent rapport ne traite pas des manquements du détenteur des données à son devoir de les recueillir et de les utiliser de la manière requise[10]. Après tout, l'objet de la divulgation de l'atteinte est de permettre aux gens de se protéger contre l'utilisation abusive de renseignements qui se retrouvent entre les mains de tiers auxquels ils n'étaient pas destinés. Sur ce point, peu importe que le détenteur des données ait recueilli trop de renseignements ou qu'il les ait utilisés à des fins auxquelles ils n'étaient pas destinés.

[19] **Recommandation :** la politique devrait s'appliquer aux atteintes à la sécurité des renseignements personnels dont on sait qu'ils ont été réellement consultés ou communiqués de manière inappropriée ou pour lesquels il est raisonnable de penser qu'ils l'ont peut-être été.

d) Quand doit-on signaler qu'il y a eu atteinte ou que la confidentialité a été compromise?

[20] Même si l'on se trouve en présence d'une atteinte qui laisse craindre que des renseignements personnels ont peut-être été consultés ou communiqués, il peut arriver qu'il ne soit pas nécessaire de le signaler. La question essentielle est la suivante : quand devient-il nécessaire de notifier l'atteinte à la vie privée? Le but de la notification de l'atteinte est de réduire le préjudice causé aux intéressés du simple fait de la divulgation de leurs renseignements personnels au-delà de ce à quoi ils ont consenti ou pouvaient raisonnablement s'attendre. Quand cette protection devient-elle nécessaire? Quels pourraient être les critères à appliquer pour en décider? À titre d'illustration :

- La vulnérabilité des renseignements : lorsque les renseignements sont encodés avec un chiffrage important, la personne qui les a subtilisés ou consultés ne sera pas en mesure d'en faire une utilisation frauduleuse.
- Le nombre de gens dont les renseignements sont en jeu : quel est le nombre de personnes concernées? Une centaine, un millier, un million?
- Le niveau de sensibilité des renseignements et l'importance que leur accordent les personnes auxquelles ils se rapportent : les renseignements en cause concernent-ils leurs habitudes d'achats, leurs résultats académiques, leur situation financière ou leur santé?

[21] Pour évaluer de manière adéquate le risque de préjudice, il peut s'avérer utile de tenir compte de la nature du préjudice qui peut être subi. Quel est le risque ou la menace pour la personne dont les renseignements personnels ont été communiqués sans autorisation? La notion de risque comprend le préjudice physique, y compris sous la forme de harcèlement ou de harcèlement avec menaces, le vol d'identité, la perte financière, la perte d'opportunités d'affaires ou d'emploi, ainsi que l'humiliation, l'atteinte à la réputation ou au réseau de relations, par exemple par la perte de renseignements relatifs à la santé, tout particulièrement la santé mentale, ou à des mesures disciplinaires[11]. Il existe un marché noir bien organisé pour les renseignements relatifs aux cartes de crédit[12], et le risque d'atteinte à la sécurité des renseignements financiers doit être pris au sérieux. Le fait qu'une personne utilise des informations sur la santé d'une autre pour recevoir un traitement peut également représenter un risque pour la santé de la victime[13].

[22] Il semble qu'il n'y ait pas de facteur unique permettant de jauger le besoin de protection des gens. Il sera nécessaire d'avoir recours à une combinaison de facteurs, et même alors, le nombre de personnes concernées ne semble pas être pertinent. Si des renseignements hautement sensibles concernant une personne ont été communiqués de manière inappropriée, la loi ne devrait-elle pas exiger du détenteur des données qu'il informe cette personne de la menace qui pèse sur ses informations?

[23] La notification n'est pas sans coûts pour autant. Elle entraîne des coûts de deux ordres. Les premiers sont les frais qu'il en coûte au détenteur des données pour notifier l'avis, qui doivent inclure les coûts de marché (relatifs à la réputation) qui découleront de la connaissance par le public de la perte des données par le détenteur. Ce dernier aspect peut être plus onéreux que les frais relatifs à l'expédition ou à l'administration de la notification. La responsabilité civile du détenteur peut également être engagée pour le préjudice causé par l'atteinte, bien qu'à ce jour aucun litige aux États-Unis ou au Canada n'ait encore donné lieu à un jugement en faveur du demandeur[14]. La deuxième catégorie de coûts comprend les frais encourus par les personnes qui reçoivent l'avis. Ils peuvent avoir à supporter des frais pour faire vérifier leur cote de crédit ou pour revoir ou conclure à nouveau leurs accords financiers pour éviter des pertes ou les compenser. Ils peuvent aussi subir des répercussions d'ordre psychologique en raison de leur inquiétude quant à savoir si un quelconque préjudice découlera de la divulgation des renseignements, ou de leurs préoccupations quant à l'embarras dans lequel ils pourraient se retrouver si certains renseignements étaient portés à la connaissance de personnes dont l'opinion compte pour eux[15].

[24] En conséquence, il importe de trouver un juste milieu entre l'exigence de notifier dans tous les cas et une notification insuffisante. Cet équilibre dépend dans une certaine mesure de l'importance que l'on accordera aux coûts engagés par le détenteur de données en comparaison de l'intérêt des personnes concernées par l'atteinte à se protéger elles-mêmes. On pourrait songer à lier l'imposition de ces coûts à la faute éventuellement commise par le détenteur des données. Cependant, la nécessité de protéger les personnes visées par ces données ne dépend pas des causes de l'atteinte.

[25] Il est tout à fait concevable dans certaines circonstances qu'un contrat puisse être conclu entre la personne à laquelle se rapportent les renseignements et le détenteur des données, prévoyant que la notification doit être effectuée selon les modalités prévues au contrat. Cependant, dans de nombreuses circonstances, il n'est pas possible de conclure un tel contrat, soit en raison du fait que la personne auprès de laquelle les renseignements ont été recueillis n'est pas la personne à laquelle ils se rapportent, ou parce que les renseignements ont été recueillis sur la base d'un consentement négatif, avec possibilité de refus. Il serait maladroit d'imposer un contrat lorsque la seule chose qui a été demandée à la personne était de savoir si elle s'opposait à la collecte et à l'utilisation de ses renseignements personnels. En droit, il est possible de présumer qu'une personne a consenti à un contrat à défaut de s'y être opposée, mais il n'est pas certain qu'un tel rapport juridique serait plus clair ou plus recommandable qu'une règle législative qui s'appliquerait à tous, que l'on soit ou non lié par contrat.

[26] Le Commissaire à la protection de la vie privée du Canada propose que la notification ait lieu « [s]i l'atteinte à la vie privée pose un risque de préjudice pour les personnes concernées »[16]. Elle poursuit avec l'établissement d'une liste de facteurs, comprenant notamment le risque de préjudice pour les personnes concernées, le risque raisonnable de vol d'identité ou de fraude, le risque de préjudice physique, le risque d'humiliation ou d'atteinte à la réputation de la personne, et la capacité de la personne à éviter ou à atténuer son préjudice[17]. Son homologue de l'Ontario propose qu'un avis soit notifié dans tous les cas[18], bien que sa collaboration avec le Commissaire de la Colombie-Britannique mentionnée plus loin laisse croire à une approche plus nuancée. En Colombie-Britannique, la position officielle est que [TRADUCTION] « la notification peut constituer une importante stratégie d'atténuation du préjudice dans les circonstances appropriées.[19] » Le Commissaire de la Colombie-Britannique, en collaboration avec celui de l'Ontario, a publié un outil d'évaluation pour la notification des atteintes pour aider à déterminer quand notifier et de quelle manière[20]. Ce document évoque le risque du vol d'identité et s'interroge sur le degré de raisonnabilité du risque. Il s'interroge aussi sur le risque de préjudice physique, le risque de préjudice moral ou d'humiliation, ainsi que le risque de perte d'opportunités d'affaires ou d'emploi. En bref, les positions des commissaires du Canada se recoupent dans une large mesure.

[27] Le fait que la nécessité d'aviser les intéressés des atteintes à la confidentialité de leurs renseignements personnels doive tenir compte du besoin de ces derniers d'être protégés contre les conséquences de ces atteintes est un thème qui revient fréquemment dans les études sur le sujet. Ainsi, l'exigence de certitude quant à la réalité de l'atteinte doit être soupesée avec la menace apparente que suscite ce type d'atteinte (p ex. : un accès sans autorisation, le vol de matériel informatique, une attaque directe visant des données) et le degré de sensibilité des renseignements ainsi que le préjudice éventuel qui peut découler du fait qu'ils se retrouvent entre de mauvaises mains. Il n'est pas possible d'établir une pondération numérique de ces facteurs, et l'évaluation de l'importance de la notification ne procède pas d'un calcul mathématique ou exact. Il s'agit toujours d'une question de jugement, et chaque cas sera unique.

[28] La gamme de calculs possible peut se résumer en cinq possibilités. La terminologie est importante, bien qu'elle ne soit pas magique, à savoir que les mots sont supposés exprimer un choix de politique, et non pas être appliqués de manière automatique. Les cinq possibilités sont exprimées quant au degré de l'obligation de notifier l'atteinte. La faute du détenteur des données relativement à l'atteinte n'est pas pertinente pour déterminer la nécessité de donner avis et donc l'obligation de divulguer l'atteinte, même si l'obligation de divulguer peut être perçue comme une sorte de sanction pour le détenteur des données.

a. L'atteinte doit être divulguée aux gens dont la confidentialité des renseignements a été compromise, si les avantages découlant de la divulgation pour ces personnes l'emportent sur le coût que représente cette divulgation pour le détenteur de données (tout en gardant à l'esprit les aspects néfastes que la divulgation peut également entraîner pour les personnes concernées).
b. L'atteinte doit être divulguée aux gens dont la confidentialité des renseignements a été compromise, s'il existe un risque important que l'atteinte cause un préjudice grave à ces personnes[21].
c. L'atteinte doit être divulguée aux gens dont la confidentialité des renseignements a été compromise, s'il existe un risque que l'atteinte cause un préjudice important à ces personnes[22].
d. L'atteinte doit être divulguée aux gens dont la confidentialité des renseignements a été compromise, s'il existe un risque d'utilisation frauduleuse de ces renseignements personnels au sens des dispositions législatives applicables[23].

e. L'atteinte doit être divulguée aux gens dont la confidentialité des renseignements a été compromise, à moins que des circonstances exceptionnelles fassent que cela n'est pas souhaitable dans le cas d'espèce.

[29] **Recommandation :** l'atteinte à la confidentialité des renseignements personnels doit être divulguée aux gens dont les renseignements ont été compromis, s'il existe un risque que l'atteinte cause un préjudice important à ces personnes.

e) Qui détermine si une atteinte a eu lieu et si elle doit être signalée?

[30] En premier lieu, ce sera presque toujours le détenteur des données qui découvrira l'atteinte à la sécurité des renseignements. Revient-il au détenteur des données de déterminer si l'atteinte à la sécurité constitue une atteinte au regard des règles, et s'il y a lieu de signaler cette atteinte, à savoir d'appliquer les critères pour la divulgation qui ont été énoncés dans la section précédente? Le détenteur des données sera d'emblée mieux en mesure de connaître le type de renseignements en cause et le type de personnes auxquelles ces renseignements se rapportent. Ainsi, il sera dans une meilleure posture pour prendre une décision –mis à part le fait que le détenteur de données aura de fortes raisons pour ne pas divulguer l'atteinte. Les conséquences de la divulgation risquent de se révéler déplaisantes pour lui. La notification des avis entraînera des coûts substantiels. Parfois, les renseignements ne comprennent pas les adresses des personnes auxquelles ils se rapportent, et l'activité du détenteur de données peut ne pas donner lieu à des communications régulières avec eux, de sorte qu'il faudra mettre en place un processus entièrement distinct pour faire parvenir les avis. En principe, il en résultera une mauvaise publicité qui aura des conséquences néfastes pour la vente des biens et services du détenteur des données et pour le prix des actions si le détenteur des données est une société faisant appel public à l'épargne.

[31] Cet élément dissuasif constitue l'une des raisons pour lesquelles le critère pour l'identification des atteintes et la divulgation doit être le plus automatique ou facile à appliquer que possible. Plus les termes de qualité sont généraux – comme le risque ou le préjudice « important » – plus il sera facile pour le détenteur de données de décider qu'une atteinte particulière n'entraîne pas l'obligation de la divulguer.

[32] La principale solution de rechange au fait de laisser le détenteur de données décider s'il doit divulguer l'atteinte consiste à donner ce pouvoir décisionnel à l'autorité responsable de l'application de la loi sur la protection des renseignements personnels dans le ressort concerné. Il a été proposé plus haut de définir l'atteinte en référence à une loi particulière, et toutes les lois pertinentes renferment des dispositions pour leur application. Les atteintes relevant du secteur public seraient renvoyées à un agent d'examen indépendant qui veille au respect de la vie privée dans le secteur public. Au niveau fédéral, chez le Commissaire à la protection de la vie privée du Canada; en Ontario, chez le Commissaire à l'information et à la protection de la vie privée, au Manitoba, chez l'Ombudsman; etc. (par simple commodité, le terme de « commissaire » est parfois utilisé dans ce document pour renvoyer à tous ces types d'agents d'examen). Les atteintes du secteur privé seraient renvoyées au commissaire provincial dans la mesure où une loi provinciale du secteur privé trouve application; à défaut, elles seraient renvoyées au Commissaire à la protection de la vie privée du Canada, dans le cas d'une contravention à la LRPDE. Le commissaire étudierait les circonstances de l'atteinte avec le détenteur de données et déciderait ensuite de l'utilité de la notification.

[33] La norme pour divulguer l'atteinte au commissaire serait moins élevée que celle en vertu de laquelle il sera nécessaire de la divulguer aux personnes concernées par l'atteinte ou au public dans son ensemble, dans la mesure où le commissaire peut pondérer les considérations d'équité et les risques d'une autre divulgation, plutôt que de laisser le détenteur de données le faire. Le commissaire appliquerait ainsi la norme établie ci-dessus pour la divulgation aux personnes auxquelles se rapportent les renseignements. Le but de confier cette décision au commissaire est d'obtenir une décision plus objective sur ce point.

[34] Même l'obligation de saisir le commissaire des éventuelles atteintes laisse au détenteur de données la décision de déterminer s'il y a bien eu atteinte. La simple possibilité d'un accès non autorisé peut ne pas être constitutive d'une atteinte – quoique si l'on a entièrement perdu le support de données (tel un ordinateur portable ou un lecteur de disque dur), un tel accès devrait à tout le moins être présumé. Cette considération milite en faveur d'une définition claire et précise et d'une obligation de signalement d'application large, quand bien même l'obligation de notifier aux personnes concernées serait plus étroite. La principale sanction pour avoir tenté de s'y

soustraire pourrait être un embarras accru si l'atteinte était découverte plus tard, encore que d'autres sanctions pourraient également trouver à s'appliquer[24].

[35] Certains pourraient se demander s'il ne devrait pas y avoir une sorte de relation réciproque entre la norme relative à la divulgation et la détermination de la personne qui doit prendre la décision. Plus le seuil pour décider est élevé, et moins la décision devrait revenir au détenteur de données, du fait de l'intérêt qu'il aurait à ne pas signaler l'atteinte. Si les atteintes sont moins graves, alors le détenteur de données pourra prendre cette décision, et si cette décision se trouve être intéressée, alors cela ne posera pas un problème si grave. Cependant, la règle devra s'appliquer à toutes les atteintes, et non pas uniquement aux atteintes d'une certaine ampleur, puisque c'est la question de l'importance qui est en jeu ici. Si on laisse au détenteur des données le pouvoir de décider, alors on le lui concéderait pour toutes les formes d'atteintes. Cette dichotomie ne fonctionne donc pas très bien si on l'examine de façon plus approfondie.

[36] Dans certains cas, l'accès sans autorisation aux données sera constitutif d'une infraction criminelle, et il y aura bien sûr infraction criminelle dans la mesure où un ordinateur a été volé. Il existe parfois une tension entre la nécessité d'aviser rapidement les intéressés du fait qu'ils peuvent courir un risque en raison d'une atteinte et la nécessité de permettre à la police d'enquêter sans susciter la suspicion. On peut faire valoir qu'il devrait y avoir une obligation d'aviser la police dans les cas qui soulèvent des questions d'ordre pénal, que l'on se situe dans le cadre d'une obligation qui pèse sur le détenteur de données ou sur le commissaire à la protection de la vie privée une fois que l'atteinte lui a été notifiée[25] (il est fort probable que s'il n'y a pas lieu de notifier l'atteinte au commissaire, il ne sera pas non plus nécessaire de la notifier à la police).

[37] Outre la notification aux personnes concernées et à la police, la loi peut exiger la tenue d'une base de données publique sur les atteintes à la sécurité. La Clinique d'intérêt public et de politique d'Internet du Canada (CIPPIC) a recommandé que le Commissaire à la protection de la vie privée du Canada mette en place une telle base de données, et que toutes les atteintes, même les moins graves, doivent y figurer[26]. Cela inciterait davantage les détenteurs de données à être prudents, à se tenir hors de la base de données, et cela donnerait un aperçu utile de l'état de la sécurité des données dans le ressort concerné. Le CIPPIC ne traitait que de la LRPDE et ne s'est

donc pas interrogé quant à savoir si une base de données unique à l'échelle nationale pourrait être mise sur pied pour l'ensemble des ressorts. Le groupe de travail ne recommande pas pour l'instant la mise en place d'une telle base de données, mais se dit ouvert aux points de vue de la Conférence quant à savoir si elle devrait être rendue obligatoire et, dans l'affirmative, pour quel niveau d'atteinte.

[38] **Recommandation :** le détenteur des données devrait être tenu de notifier au commissaire à la protection de la vie privée compétent ou à l'agent d'examen de la protection de la vie privée toute atteinte ayant trait à la divulgation ou à la consultation non autorisée de renseignements personnels[27]. Le commissaire ou l'agent devrait avoir le pouvoir d'exiger que le détenteur des données notifie cette atteinte aux personnes concernées dans la mesure où le critère légal est rempli. Le commissaire ou l'agent devrait également être tenus de la notifier à la police si les conditions le justifient.

f) Quelle réponse doit-on apporter à l'atteinte?

[39] La réponse type à apporter à l'atteinte sera la divulgation de l'atteinte aux personnes concernées. La recommandation des commissaires à la protection de la vie privée et des agents d'examen – et il semble qu'ils soient unanimes sur ce point – est que la réponse appropriée à une atteinte doit comprendre une analyse de la cause de l'atteinte, une mesure visant à y mettre un terme le plus rapidement possible, un éventuel signalement à la police en présence d'actes illégaux, et à plus long terme, des mesures visant à éviter qu'une telle atteinte ne se reproduise à l'avenir. Mis à part la divulgation de l'atteinte, aucun de ces sujets ne semble adapté pour faire l'objet d'une disposition législative. Le fait de ne pas parvenir à faire cesser l'atteinte contribuera bien sûr à faire perdurer le risque d'accès aux renseignements personnels et augmentera d'autant le nombre de notifications nécessaires. En termes de relations publiques, le détenteur de données voudra être en mesure d'exposer les mesures qu'il a prises pour mettre un terme au problème. Le choix du moment pour prendre la mesure corrective ou divulguer l'atteinte peut dépendre des conseils de la police, dans la mesure où elle pourrait devoir enquêter au préalable sur les circonstances de l'atteinte.

[40] Là encore, le commissaire à la protection de la vie privée ou l'agent d'examen peut fournir son avis – et si le détenteur de données est amené à décider, alors il aura à le faire, et la

loi devra peut-être fournir des orientations – sur la manière dont il faut notifier l'atteinte. Faut-il contacter les personnes individuellement – par téléphone, courrier ou courriel? Les avis groupés dans les médias seront-ils appropriés pour les groupes très larges, ou pour les groupes dont le détenteur des données n'a pas les coordonnées?

[41] **Recommandation :** ne fournir aucune règle sur la manière dont les détenteurs des données devraient répondre à l'atteinte, à l'exception de ce qui concerne la notification de l'atteinte.

g) Que doit indiquer l'avis de notification de l'atteinte?

[42] La rédaction de l'avis ne fait pas de doute : la sécurité des renseignements personnels de la personne qui reçoit l'avis a été compromise. L'avis fournit aussi probablement la meilleure information disponible en ce qui concerne l'étendue des renseignements en cause, ainsi que le moment et les circonstances dans lesquelles l'atteinte est survenue. En d'autres termes, l'avis fournit aux personnes concernées autant de renseignements que possible pour leur permettre de se prémunir contre les conséquences préjudiciables de l'atteinte (certaines d'entre elles ont été énumérées plus haut[28]). La loi devrait-elle exiger que l'avis présente ces renseignements d'une manière particulière? Ou est-ce que le détenteur de données sera tenu par une obligation générale de trouver un moyen efficace de le faire, un manquement en ce sens pouvant devenir par la suite un problème d'application?

[43] Une question plus ouverte consisterait à se demander si l'avis devrait contenir plus d'informations quant aux droits de la personne visée par les données, ou la conseiller sur la façon dont elle pourrait protéger ses droits ou ses intérêts dans la mesure où ses renseignements personnels font désormais partie du domaine public. Les lignes directrices des commissaires à la protection de la vie privée auxquelles il a été fait référence plus haut fournissent des exemples de textes possibles, d'une manière générale ou quant à la rédaction à utiliser. Certains des sujets retenus sont les suivants :

- Des conseils pour connaître sa cote de crédit et une explication quant à la façon d'y procéder.

- Des renseignements sur le droit d'obtenir le gel de l'accès au crédit (de sorte que personne ne puisse obtenir un crédit en notre nom sans autorisation expresse) ou d'autres mesures correctives[29].
- Des renseignements quant à la manière de changer un numéro de carte d'assurance-maladie.
- Des renseignements sur les coordonnées de l'organisation du détenteur de données, afin d'obtenir davantage d'informations.
- Des renseignements sur les coordonnées du commissaire à la protection de la vie privée et de l'agent d'examen compétents afin d'obtenir davantage d'informations et la possibilité de déposer une plainte relative à l'atteinte.
- Les autres sources de renseignements sur la manière de se protéger soi-même dans de telles circonstances, tel que le site d'Industrie Canada ou les sites des commissaires à la protection de la vie privée[30].

[44] **Recommandation :** si le choix de politique est d'exiger des détenteurs de données qu'ils divulguent les atteintes aux commissaires à la protection de la vie privée et aux agents d'examen et qu'ils suivent leur recommandation, alors il n'est pas nécessaire que la loi expose en détail le contenu des avis. Cette question sera du ressort du commissaire à la protection de la vie privée ou de l'agent d'examen et du détenteur de données. Si le pouvoir de décider de la divulgation revient au détenteur de données, alors la loi devrait fournir une recommandation sur le contenu des avis, au moins dans des termes génériques.

h) Comment assure-t-on l'application de ces obligations?

[45] Il existe trois moyens de faire appliquer les obligations énoncées dans la nouvelle loi : au niveau civil, réglementaire et pénal. Le recours civil prendrait la forme d'une action entre la personne visée par les données et dont la sécurité des renseignements a été compromise, et le détenteur de données. En principe, l'introduction des actions en justice ne nécessite pas d'autorisation spéciale conférée par la loi, que le recours envisagé soit individuel ou collectif. La seule raison de le considérer autrement ici tient à l'expérience des demandeurs au civil aux États-Unis qui ont été en grande partie incapables d'obtenir réparation à l'issue de telles actions. Le problème était qu'ils n'avaient pas été en mesure d'associer un quelconque préjudice en particulier à la divulgation inappropriée de leurs renseignements. Dans la plupart des cas, la

partie demanderesse n'avait non seulement subi aucun préjudice, mais elle avait en outre des difficultés à établir un lien de causalité entre un préjudice subi et la divulgation qui s'y rapportait, même lorsqu'il y avait eu usurpation d'identité. Jusqu'à présent, le mieux que les gens aient pu réussir à obtenir est de recouvrer les coûts de la vérification de leur solvabilité[31]. Parfois, les sociétés procédant à la notification s'acquitteront volontairement de ces coûts pour des raisons de relations publiques.

[46] Il serait possible de prévoir dans la loi un droit à des dommages-intérêts légaux lorsqu'une action en justice est accueillie. Cela éviterait d'avoir besoin de recourir à la preuve du préjudice réel qui découle de l'atteinte. Cela renforcerait aussi l'effet dissuasif de la loi, ou plutôt l'effet incitatif qui encourage les détenteurs de données à préserver soigneusement les renseignements. Il est permis de penser que des dommages-intérêts légaux ne devraient s'appliquer que dans les cas où le détenteur de données a commis une faute et non dans ceux où l'atteinte aurait été inévitable même si celui-ci avait fait preuve de diligence raisonnable. Il pourrait cependant s'avérer difficile de fixer un montant de dommages-intérêts légaux d'une manière qui serait équitable pour toutes les parties au litige, que l'on soit dans une affaire ne touchant que peu de gens ou une affaire visant potentiellement des milliers, voire des millions de clients. Il pourrait s'avérer plus utile de prévoir des remèdes de fond, plutôt qu'un montant d'argent qui sera forcément arbitraire[32].

[47] Les mesures réglementaires d'application seraient entre les mains des commissaires à la protection de la vie privée et des agents d'examen. Elles pourraient comprendre une simple ordonnance de procéder à une divulgation ou une ordonnance plus détaillée prescrivant la rédaction ou la manière dont la divulgation doit être faite ou même l'imposition de pénalités en cas de manquement à l'obligation de signaler une atteinte au commissaire ou à l'agent d'examen ou de défaut de s'être conformé aux ordonnances antérieures. Il conviendrait cependant de noter que seuls certains commissaires ont le pouvoir de rendre des ordonnances en vertu de la loi actuelle. Certains commissaires et agents d'examen ne font que fournir des recommandations, avec des pouvoirs similaires à celui d'un protecteur du citoyen. En vertu de la LRPDE, l'exécution des décisions du Commissaire à la protection de la vie privée du Canada peut être recherchée dans certaines circonstances devant la Cour fédérale, mais seule l'ordonnance de la Cour a force de loi. À titre subsidiaire, la Conférence pourrait laisser cette question à

l'appréciation des autorités du ressort d'édiction : veut-on préserver la cohérence avec le reste de la législation en matière de protection de la vie privée en matière de surveillance? Les gouvernements peuvent se montrer très réticents à l'idée d'accroître les pouvoirs de leurs commissaires de façon aussi drastique.

[48] Les pénalités administratives – c'est-à-dire les amendes directement imposées par une autorité règlementaire, sans déclaration de culpabilité devant un tribunal – se sont développées au Canada et ailleurs ces dernières années. Elles ont été accueillies devant les tribunaux dans la mesure où elles sont assujetties à un certain niveau de contrôle judiciaire. Ainsi, le commissaire ne serait pas à lui seul à la fois celui qui rend l'ordonnance, le poursuivant et le juge final. Cependant, le pouvoir d'imposer de telles pénalités constitue un écart encore plus marqué par rapport au rôle de médiateur ou de facilitateur que jouent beaucoup de commissaires et d'agents d'examen, que la prise d'ordonnances. Un autre facteur contribue à rendre incertaines de telles pénalités en cas de défaut de la part d'entités publiques : les commissaires et leurs homologues sont souvent des agents du corps législatif (ou du Parlement, dans le cas du gouvernement fédéral). Il peut ne pas être approprié pour eux de percevoir des sommes d'agent auprès de la Couronne à titre de pénalités – mais si les peines sont versées au revenu consolidé, c'est tout simplement prendre quelque chose dans une poche pour le remettre dans l'autre.

[49] L'application du point de vue pénal ou quasi-pénal ne s'appliquera probablement qu'à certaines infractions graves à l'obligation de notifier. Plutôt que (ou en plus) de conférer aux commissaires à la protection de la vie privée et aux agents d'examen le pouvoir de rendre des ordonnances, les autorités législatives pourraient créer une infraction visant le défaut de se conformer aux exigences de notification prévues par la loi (si d'autres activités criminelles étaient en jeu, les dispositions pénales traditionnelles s'appliqueraient bien entendu). Les poursuites peuvent se révéler être une solution de rechange utile aux mesures réglementaires dans les ressorts où l'organisme de réglementation ne peut pas émettre d'ordonnance directement ou dans lesquels le législateur ne veut pas donner à ses commissaires le pouvoir d'imposer des sanctions. De telles procédures peuvent être instituées par les procureurs de la Couronne, si les commissaires à la protection de la vie privée ne se sentent pas à l'aise de le faire. Il pourrait être utile que des discussions aient lieu entre les participants éventuels avant que les autorités d'un ressort ne préparent une loi sur le sujet.

[50] Il serait possible de prévoir expressément le degré de responsabilité pour la nouvelle infraction, si cela est souhaitable. À titre d'exemple, la violation d'une obligation de notifier ou d'une obligation de se conformer à une ordonnance du commissaire à la protection de la vie privée ou d'un agent d'examen en matière de notification pourrait être expressément désignée comme une infraction de responsabilité stricte, de sorte que la personne fautive aurait à faire la preuve de sa diligence raisonnable pour éviter une déclaration de culpabilité à son égard.

[51] L'application de l'obligation de notifier les atteintes est distincte d'une éventuelle poursuite pour avoir fait défaut de conserver de façon sécuritaire les données à leur lieu initial, comme cela est désormais requis (habituellement) par la loi sur la protection de la vie privée. Certains cas d'atteintes peuvent donner lieu à des poursuites de ce genre, même si l'atteinte a été notifiée aux personnes concernées. Au Royaume-Uni, le commissaire à la protection de la vie privée s'est vu récemment octroyer le pouvoir d'imposer des amendes aux organisations si leurs procédures de fonctionnement contreviennent de manière importante aux principes régissant la protection des données. Il s'agit d'une sanction administrative imposée pour avoir fait défaut de conserver les renseignements de manière sécuritaire, plutôt que d'avoir fait défaut de signaler les incidents relatifs à la sécurité[33].

[52] **Recommandation** : créer une infraction sanctionnant le manquement à l'obligation de notifier ainsi que le manquement de se conformer à une ordonnance du commissaire ou de l'agent d'examen, lorsque cet agent dispose du pouvoir d'émettre des ordonnances. Les autorités des différents ressorts sont invitées à étudier la possibilité de conférer le pouvoir de rendre des ordonnances pour ces infractions particulières, même si de tels pouvoirs n'existent pas ailleurs dans la loi sur la protection de la vie privée. Les commissaires ou leurs homologues devraient avoir la responsabilité principale mais non exclusive de faire enquête pour déterminer si les détenteurs des renseignements se sont conformés à leurs obligations légales. Le groupe de travail ne formule aucune recommandation quant à savoir qui devrait prendre l'initiative de poursuivre, chaque ressort d'édiction devant déterminer ce qui lui paraît le plus sensé au regard de son régime sur la protection de la vie privée. N'excluez pas les recours civils, mais ne prévoyez pas de dommages-intérêts légaux pour les manquements à l'obligation de notifier les atteintes à la sécurité des renseignements.

i) Que doit-on inclure d'autre dans le cadre en cause?

[53] L'objectif qui sous-tend cet ensemble de propositions est de protéger les personnes dont les renseignements personnels ont été divulgués en contravention de la loi sur la protection de la vie privée. La notification d'un avis à ces personnes relativement à la divulgation non autorisée est la première étape, mais cela ne les avance pas beaucoup. En particulier, la menace du vol ou de l'usurpation d'identité plane sur les têtes de ces personnes, et sa gravité dépend de la nature des renseignements divulgués de manière inappropriée. Dans ces circonstances, la recommandation générale est que ces personnes devraient vérifier leur cote de crédit. Cependant, cela pourrait s'avérer difficile sur le plan administratif et coûteux et prendre beaucoup de temps. La loi pourrait en faciliter le processus en fournissant aux personnes concernées le droit d'accéder à leur dossier de cote de crédit moyennant des frais minimes. Certaines législations américaines prévoient un certain nombre de demandes d'accès gratuit[34]. Elles requièrent également que les trois plus importantes agences de notation américaines coopèrent les unes avec les autres, de sorte que la demande de la personne auprès d'une agence soit transmise aux autres, afin que la personne obtienne dans le cadre d'une seule et même demande les renseignements en provenance des trois agences de notation[35].

[54] En outre, une simple vérification périodique peut sembler être un remède peu efficace – voire en fait une absence de remède, si ce n'est de faire ressortir les problèmes qu'il faudra résoudre si la vérification révèle un problème[36]. Certains états américains ont prévu un gel volontaire de l'accès au dossier de crédit, grâce auquel une personne à risque peut s'assurer que personne ne puisse ouvrir un compte sur la base de son crédit sans qu'une vérification particulière ait été menée auprès d'elle. En d'autres termes, le voleur de données ne sera pas capable de faire usage des renseignements volés pour obtenir un crédit[37]. Bien sûr, il sera également plus difficile pour la véritable personne d'obtenir un crédit, mais on peut considérer qu'il s'agit d'un équilibre acceptable. Les agences de notation voient en ce genre de dispositions une nouvelle obligation[38]. Si des frais devaient être facturés, leur montant pourrait être facturé au détenteur de données dont le manquement est à l'origine du gel de l'accès au dossier de crédit.

[55] Il n'est pas non plus clair si de telles mesures seront efficaces pour bloquer l'usage non autorisé de l'identité. Dans tous les cas, un gel de l'accès au dossier de crédit ne peut servir qu'à empêcher un abus relatif au crédit. D'autres utilisations inappropriées résultant de l'usurpation

d'une identité, comme dans le cadre de transactions ou d'activités criminelles, ne sont pas couvertes par une telle mesure. Le fait qu'une mesure ne remédie qu'à certains aspects d'un préjudice ne constitue pas un argument valable pour ne rien faire.

[56] On pourrait étudier en profondeur la législation applicable aux États-Unis, où au moins 40 États ont édicté des lois (souvent incompatibles) relatives à l'obligation de notifier, pour trouver des idées constructives pour compléter la règle fondamentale de l'obligation de notifier[39]. Toute législation canadienne serait de nature provinciale ou territoriale, pour réglementer une industrie qui relève de la compétence provinciale. Il serait nécessaire d'apporter une attention toute particulière pour coordonner les questions inter-juridictionnelles, étant donné que les agences ont leur siège à un lieu précis mais poursuivent leur activité à travers tout le pays. En tant que partie intégrante de la législation visant les agences d'évaluation du crédit, la loi uniforme pourrait réglementer les frais d'agence facturables pour ces services ou imputer les frais à la personne responsable de l'atteinte – que cette personne ait ou non commis une faute.

[57] **Recommandation :** prévoir une certaine coopération entre les agences d'évaluation du crédit lorsqu'elles répondent aux demandes. Ne pas prévoir un gel obligatoire de l'accès au dossier de crédit sans avoir plus de preuve quant à sa probable efficacité.

j) Quelle forme devrait prendre la loi uniforme?

[58] Comme cela a été indiqué plus haut, toutes les provinces et territoires disposent de lois sur la protection de la vie privée visant tout ou partie du secteur public et certaines parties du secteur privé. Quelques provinces disposent d'une loi générale sur la protection de la vie privée applicable au secteur privé. Le gouvernement fédéral dispose d'une loi visant le secteur public et d'une loi visant le secteur privé qui s'applique aux activités commerciales réalisées dans l'ensemble du pays, sauf lorsqu'une loi provinciale trouve à s'appliquer. La loi uniforme sur la notification des atteintes devrait être compatible avec chacune d'elles, puisque la Conférence recommandera probablement à tous de l'adopter.

[59] Deux principales options sont possibles :

a. la rédaction d'une loi dans une forme qui puisse être intégrée directement aux dispositions existantes de la loi sur la protection de la vie privée du ressort d'édiction;

b. rédiger une loi indépendante qui pourrait être adoptée en elle-même, en vue d'imposer cette obligation aux entités même si elles ne sont pas par ailleurs assujetties à la législation provinciale ou territoriale sur la protection de la vie privée.

[60] Les avantages de la première possibilité sont la simplicité et le respect des décisions politiques du ressort quant à sa législation sur la protection de la vie privée. Les inconvénients résident dans le fait que certains groupes de résidents provinciaux peuvent ne pas bénéficier de la protection de la notification des accès non autorisés à leurs renseignements.

[61] Les avantages de la deuxième possibilité sont l'universalité : chacun bénéficie du régime de notification des atteintes, même si d'autres obligations du secteur privé ne sont pas énoncées dans la loi. Il serait nécessaire de rédiger cette mesure législative de manière à intégrer les normes de protection de la vie privée dont la violation entraînerait l'application de la loi, puisque l'on ne peut pas simplement renvoyer à une violation de la règle législative actuelle. D'un autre côté, cela pourrait s'avérer quelque peu bancal dans une province où la LRPDE s'applique, si la loi fédérale contient une règle relative à la notification des atteintes différente de celle applicable dans la province ou le territoire. Cependant, la loi provinciale ou territoriale pourrait imposer une obligation de notification aux détenteurs de renseignements personnels qui ne sont pas régis par la LRPDE, tels que des renseignements relatifs à l'emploi ou des renseignements qui n'ont pas été recueillis, utilisés ou communiqués à des fins commerciales[40].

[62] **Recommandation :** rédiger la loi uniforme pour l'intégrer à chacune des lois sur la protection sur la vie privée des ressorts d'édiction.

Conclusion

[63] Le groupe de travail sur le vol d'identité recommande que la loi rende obligatoire la notification des atteintes à la confidentialité des renseignements personnels dans certains cas graves, en conférant aux commissaires à la vie privée ou aux agents d'examen indépendants des ressorts d'édiction la responsabilité de prendre la décision importante consistant à déterminer si l'atteinte est assez importante pour justifier les coûts de la notification à l'égard de l'ensemble des parties. Pour l'instant, le groupe de travail ne recommande pas d'adopter une loi comportant plus de détail sur d'autres éléments des atteintes à la protection des données, tels que des

dispositions relatives à la réparation de la réputation après le fait ou des recours civils exprès, au-delà de la création d'une infraction en cas de défaut de se conformer aux obligations principales de la loi.

[64] On pourrait se demander, cependant, si une loi est tout simplement nécessaire. Pourquoi ne pas se contenter d'un exposé des principes applicables, tels que énoncés dans ce rapport (ou tels que modifiés par une résolution de la Conférence), en laissant chaque province et territoire légiférer par soi-même? La réponse du groupe de travail est en deux temps :

a. D'abord, cela ne nous mènerait pas beaucoup plus loin que là où nous en sommes en ce moment, puisque les commissaires à la protection de la vie privée et les agents d'examen qui ont écrit sur le sujet sont en parfait accord sur ces principes. L'objet des travaux de la Conférence est de donner à tous les ressorts leur mot à dire sur l'élaboration de ces principes, de façon à y ajouter une certaine valeur, mais l'incidence du point de vue pratique peut être un peu différente.

b. Ensuite, il est important pour des détenteurs de données qui exercent leurs activités sur le territoire de plus d'un ressort canadien d'être tenu à une obligation prévisible et, idéalement, uniforme à l'égard de toutes les personnes visées par ces données à travers le pays. Il est permis de penser que le besoin de compatibilité à l'échelle nationale des entités du secteur public est moindre, puisque les gens au sujet desquels ils détiennent des renseignements se trouvent généralement dans un même ressort, et le fait que les lois puissent différer dans une certaine mesure en comparaison de celles en vigueur à l'extérieur des frontières provinciales ou territoriales, il peut s'agir d'un inconvénient mineur. Ce n'est pas vrai pour les organisations qui ont des activités dans plusieurs ressorts. Le seul moyen de parvenir à une certaine uniformité, ou même une certaine harmonie, avec suffisamment de certitude, est de légiférer dans le même sens.

[65] Le groupe de travail reconnaît que les lois uniformes ne sont pas nécessairement adoptées littéralement à travers le pays. En particulier, le Québec trouve souvent un moyen de légiférer différemment en raison des particularités de son Code civil ou pour d'autres raisons. Néanmoins,

l'objectif commun de trouver un principe national et de l'appliquer à l'échelle national est mieux atteint à partir du socle commun que constitue une loi uniforme.

Le vol d'identité et les possibilités d'aide aux victimes à l'égard des dossiers judiciaires entachés d'erreur en matière pénale

[66] Le terme de « vol d'identité criminel » est fréquemment employé pour faire référence à des situations dans lesquelles l'auteur du vol utilise le nom d'une victime innocente, soit seul ou en combinaison avec d'autres documents d'identité, dans leurs rapports avec des agents de l'application de la loi et d'autres autorités du système judiciaire. De telles rencontres donnent lieu à une documentation erronée, des ordonnances et des dossiers qui exposent la victime au risque d'arrestations ou d'autres sanctions officielles. L'État de la Californie a défini le vol d'identité criminel comme le 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[41].

[67] En 2005, le département américain de la Justice et le bureau des statistiques judiciaires ont réuni un groupe national de réflexion sur le vol d'identité et les dépositaires de dossiers judiciaires en matière pénale. Le rapport de ce groupe de discussion dresse un exposé utile des trois différentes manières selon lesquelles le vol d'identité ou les méprises sur l'identité peuvent avoir lieu et occasionner des erreurs dans les bases de données relatives aux dossiers judiciaires :

a. **le vol d'identité intentionnel –** lorsqu'une personne utilise délibérément le nom ou l'identité d'une autre personne en vue d'éviter une arrestation ou d'entraver une enquête de police.

b. **Le vol d'identité par inadvertance –** lorsqu'une personne fournit un nom fictif ou une identité qui appartient ou ressemble de très près, **par coïncidence**, à celui d'une personne réelle en vue d'éviter une arrestation ou d'entraver une enquête de police.

c. Les méprises sur l'identité ne découlant pas d'un vol d'identité – lorsqu'une personne fournit son véritable nom, mais qu'il est **identique** ou étroitement lié à l'identité d'une personne innocente et qu'on lui associe cette dernière par erreur[42].

[68] Un dossier judiciaire ou un autre document officiel peut être créé au nom de la victime à différentes étapes. À titre d'exemple, les représentants de la Californie ont identifié cinq manières dont un dossier judiciaire ou d'autres documents sont susceptibles d'être créés par erreur au nom de la victime. Le voleur peut être cité (accusé), poursuivi ou déclaré coupable sous le nom de la victime, ou le nom ou l'identité de la victime peut de manière erronée être associé au casier judiciaire d'une autre personne ou à un autre document la concernant[43].

L'ampleur du problème

[69] Il est difficile de donner des chiffres précis concernant les incidents de vol d'identité. Il est nécessaire d'approfondir la recherche sur plusieurs aspects du vol d'identité, notamment pour déterminer comment le vol d'identité a lieu, quelles en sont les répercussions à court et à long terme, et quels sont les groupes au sein de la population qui sont les plus touchés[44]. Le manque de recherche sur ces questions et d'autres questions connexes contraste avec certaines recherches très détaillées qui sont à présent accessibles sur le sujet ainsi que d'autres sujets connexes concernant le vol d'identité qui entraîne un préjudice de nature financière ou autre mais qui n'expose pas la victime à des conséquences sur le plan pénal[45].

[70] Malgré ces difficultés, les recherches confirment l'ampleur du vol d'identité de nature criminelle. À titre d'exemple, une enquête nationale sur les victimes de la criminalité réalisée en 2004 a conclu que 4 p. 100 des personnes qui se sont elles-mêmes identifiées comme des victimes de vol d'identité ont indiqué qu'elles avaient fait l'objet d'une enquête criminelle en raison de l'usurpation de leur identité[46]. Selon les conclusions d'une étude réalisée en 2006 par la United States Federal Trade Commission, 27 p. 100 des victimes avaient déclaré que l'auteur du vol avait utilisé leur nom au moment de son arrestation par la police ou lors de leur accusation pour une infraction criminelle, et 17 p. 100 de ces personnes ont fait l'objet d'une enquête

criminelle en conséquence[47]. Les différences entre les études, d'ordre méthodologique et autre, empêchent de comparer directement ces résultats. Néanmoins, elles constituent une indication claire de l'importance du problème. Bien qu'aucuns renseignements statistiques détaillés et comparables ne soient disponibles dans une perspective canadienne, des études ont fait remarquer que le vol d'identité commis pour couvrir une autre activité criminelle ou terroriste constitue un problème important[48].

La nature du préjudice causé

[71] Cette forme du vol d'identité donne lieu à la fois à un préjudice direct et à un préjudice indirect. Les victimes sont directement touchées lorsque de nouveaux dossiers ou de nouvelles entrées dans les fichiers et les bases de données des organismes d'application de la loi leur sont associés ou attribués à la suite d'une erreur. Ces répercussions se propagent et deviennent de plus en plus difficile à corriger dans la mesure où ces dossiers ou entrées sont partagés avec d'autres organismes d'application de la loi ou d'autres organismes officiels d'autres juridictions. Les victimes prennent conscience de ces répercussions lorsqu'elles ont ensuite affaire à des policiers qui cherchent à faire exécuter un mandat ou une autre procédure découlant de cette entrée ou lorsqu'ils font des démarches telles que le renouvellement de leur permis de conduire ou de l'immatriculation d'un véhicule automobile. Les conséquences de ces entrées injustifiées peuvent être graves, et conduire notamment à leur arrestation ou à leur détention à tort, ou au refus de leur permis ou de leur immatriculation ou une autre mesure administrative du genre. Malheureusement, contrairement à ce qui existe en ce qui concerne le préjudice financier associé au vol d'identité, il n'existe pas d'étude empirique qui donne des détails sur l'étendue de ce préjudice ou sur le temps qui est nécessaire pour en surmonter les effets[49].

[72] Le préjudice indirect peut aussi survenir lorsque les registres publics sont utilisés à d'autres fins, y compris la vérification du casier judiciaire comme condition préalable au recrutement, à une activité bénévole, à une location, ou la production du dossier du conducteur ou un document similaire dans des circonstances analogues. Lorsque des tiers peuvent avoir accès à ces dossiers, le préjudice causé peut être généralisé et insidieux. C'est particulièrement le

cas lorsque la donnée est fournie sur la base d'une recherche simplement nominative, par opposition à celle qui découle de la prise d'empreintes digitales ou d'autres identifiants. Cet aspect du problème peut être plus aigu aux États-Unis, ou beaucoup de registres publics sont accessibles dans le commerce et utilisés dans une multitude de contextes. Le problème est en outre aggravé par le fait qu'aucune exigence ne pèse sur le tiers pour donner avis du fait qu'une telle recherche a été menée[50].

Les possibilités pour aider les victimes

Les États-Unis

[73] Les démarches en faveur de l'aide aux victimes, décrites de manière détaillée ci-dessous, présentent au moins deux traits communs. En premier lieu, elles fournissent un mécanisme pour régler la question des dossiers qui ont été créés par erreur à la suite d'un vol d'identité. En second lieu, ces mécanismes visent à prévoir des moyens officiels par lesquels les personnes innocentes peuvent s'identifier comme ayant été des victimes du vol d'identité auprès des autorités chargées de l'application des lois ou d'autres autorités.

La correction de dossiers et la prévention

[74] Un groupe de réflexion national chargé d'étudier cet aspect de la question aux États-Unis a décrit trois différentes démarches qui pourraient être adoptées. Le groupe n'a recommandé aucune de ces approches, en prenant acte des lacunes de chacune d'entre elles. Bien que le groupe ait reconnu l'importance du problème, ils en sont arrivés à la conclusion qu'on n'en savait que trop peu sur certains aspects de la question, y compris la mesure dans laquelle certaines des solutions proposées ne porteraient pas préjudice à l'application de la loi[51].

[75] Ces approches, ainsi que les préoccupations formulées par le groupe de discussion se résument comme suit :

a. **Radier les renseignements relatifs au vol d'identité** – bien que certains membres du groupe aient affirmé qu'il s'agissait de la mesure la plus efficace du point de vue de la victime, d'autres ont fait observer que la radiation des renseignements n'était

pas appropriée dans plusieurs circonstances, parce que même les pseudonymes assumés volontairement constituent des éléments d'information précieux à des fins d'application de la loi. En outre, si l'auteur du délit apprend que le pseudonyme a été supprimé, il pourrait être en mesure de l'utiliser à nouveau en toute impunité. Enfin, si le nom de la victime est le seul qui apparaisse au dossier, soit parce que le contrevenant n'a été arrêté qu'une seule fois, soit parce qu'il a utilisé le même pseudonyme lors de multiples arrestations, la radiation des renseignements peut rendre difficile, voire impossible la consultation de la base de données[52]. D'autre part, les dossiers radiés peuvent causer des difficultés pour les vérifications d'antécédents, puisque les renseignements peuvent toujours être inclus ou mélangés avec les dossiers de délinquants primaires, qui peuvent également être « radiés » dans certains ressorts[53].

b. Sceller le ou les dossiers en cause – en principe, le scellement d'un dossier constitue une mesure moins drastique que celle qui consiste à le radier. Un dossier scellé demeurerait accessible à des fins limitées – telles que les seules fins de la justice pénale – mais non à d'autres fins comme celles de la vérification d'antécédents [54].

c. **Signaler le ou les dossiers en question** – en vertu de cette démarche, le renseignement demeurerait disponible et accessible, mais il porterait la mention qu'il est frauduleux et qu'il ne reflète pas la véritable identité de la personne, qu'il a servi à un vol d'identité ou qu'il a donné lieu à une méprise sur l'identité de la personne. Cette mention pourrait également indiquer que d'autres mesures ont été prises pour s'assurer de la véritable identité de la personne, telles que la prise d'empreintes digitales. Bien que certains membres du groupe de réflexion se soient dits d'avis que cette démarche serait utile, des préoccupations ont été exprimées au sujet du fait qu'elle pourrait ne pas être pleinement efficace, notamment dans les situations autres que celles qui relèvent de la justice pénale, en raison du fait que certains, tels que les employeurs éventuels, pourraient ne pas tenir compte de l'avertissement se rapportant au dossier ou ne pas confirmer, à l'aide d'empreintes digitales ou autrement, que le dossier en cause concerne vraiment la personne qui fait l'objet de l'enquête. Certains ont proposé que les États adoptent des lois qui exigent des employeurs ou des

destinataires des dossiers qu'ils confirment l'identité au moyen d'empreintes digitales dans de telles circonstances[55].

L'identification des victimes

[76] L'identification officielle de la personne comme étant la victime d'un vol d'identité pourrait permettre de réduire autant que possible le risque d'arrestations ou de détentions injustifiées ou d'autres mesures de la sorte. Elle pourrait également permettre de régler certaines difficultés qui peuvent découler des vérifications d'antécédents ou de casier judiciaire.

Les trois démarches pour l'identification des victimes

A. Le registre des vols d'identité

[77] La Californie a entrepris cette démarche pour assister les victimes de vol d'identité criminel par la mise en place en 2001 d'un système de registres pour les victimes. Sept autres États ont adopté une démarche similaire[56]. L'accès au registre de la Californie n'est pas un processus facile. En fait, il suppose la réalisation de huit étapes distinctes[57].

[78] Le plus difficile dans tout cela consiste à obtenir une ordonnance du tribunal qui puisse servir de déclaration d'innocence factuelle. Le processus visant à présenter une requête pour une telle ordonnance est complexe et requiert le dépôt d'une requête, la preuve de la signification, la préparation de l'ordonnance, des copies de la documentation et des éléments de preuve[58]. Les renseignements qui viennent au soutien de la requête sont présentés sous la forme d'une déclaration qui a le même effet qu'un serment. Il est conseillé aux requérants d'éviter d'y inclure leurs avis, conclusions ou preuves par ouï-dire[59]. Le critère préliminaire pour accueillir la demande est qu'il n'y ait aucun motif raisonnable de croire que la personne a commis l'infraction pour laquelle le voleur d'identité a été arrêté, accusé ou condamné. Si la demande est accueillie, l'ordonnance rendue exigera le scellement et la destruction des dossiers en cause[60]. 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[61].

[79] Une fois que toutes ces étapes sont terminées, la victime est ajoutée au registre, et elle se voit remettre un numéro NIP ainsi qu'un numéro de téléphone accessible vingt-quatre heures sur

vingt-quatre. Si elle est arrêtée par la police, la victime donne son numéro NIP ainsi que le numéro de téléphone pour permettre à l'agent de confirmer qu'elle a été victime d'un vol d'identité.

[80] Il n'est pas surprenant que la complexité du processus de demande ait entraîné des difficultés importantes dans la mise en œuvre du registre. Les témoignages devant le Sénat américain ont indiqué qu'au cours des quatre premières années du registre, il y avait moins de cinq personnes enregistrées. En mars 2007, ce chiffre n'était que de 70 personnes[62].

B. Le « passeport relatif au vol d'identité »

[81] L'Ohio a entrepris une nouvelle démarche pour aider les victimes, appelée [TRADUCTION] « passeport relatif au vol d'identité ». Cette démarche a été instituée en décembre 2004 en Ohio à titre de projet pilote financé par le département fédéral de la Justice. Le passeport identifie la personne comme la victime d'un vol d'identité et peut être utilisé dans des contextes d'ordre civil et pénal. Il comprend la photographie, les empreintes digitales, la signature ainsi que d'autres renseignements biométriques relatifs à la victime. Le passeport renferme des renseignements permettant d'avoir accès à une base de données sécuritaire, qui n'est accessible qu'aux seuls agents d'application de la loi. Cette base de données contient d'autres renseignements relatifs à la plainte relative au vol d'identité. Les renseignements contenus dans le passeport sont également transmis à la base de données relative aux véhicules automobiles pour s'assurer qu'aucune autre inscription erronée ou autre mesure du genre ne soit entreprise sur la base du vol d'identité[63].

[82] Selon la Conférence nationale des législatures d'État, six autres États ont adopté ce modèle – le Delaware, l'Iowa, le Maryland, le Montana, le Tennessee et la Virginie[64]. En outre, le groupe de travail du Président sur le vol d'identité (*President's Task Force on Identity Theft*) a recommandé que ce modèle, ainsi qu'un programme mis au point par le FBI, et décrit ci-après, soient examinés pour servir de base à un programme national d'aide aux victimes de vol d'identité[65].

[83] Un rapport de 2006 concernant le recours au programme en Ohio indique qu'il a été largement utilisé. Depuis 2005, 602 passeports ont été émis au total sur 694 demandes[66]. La conduite d'une analyse empirique approfondie sur l'efficacité de ce programme est une des conditions du financement du projet pilote et est envisagée par le groupe de travail sur le vol d'identité dont il est fait mention plus haut.

C. Le fichier des vols d'identité du National Crime Information Center

[84] Le FBI tient une base de données nationale qui peut être consultée par les organismes chargés de l'application de la loi. Le fichier des vols d'identité constitue l'une des composantes de cette base de données. Le fichier a été activé en 2005 et contient environ 2 600 dossiers consignés par 29 États. À la suite du dépôt d'un rapport de police qui comprend des détails sur le vol d'identité ainsi que des renseignements permettant l'identification de la victime, tels qu'une photographie ou des empreintes digitales, le rapport peut être consigné dans le fichier des vols d'identité du National Crime Information Center (NCIC). La victime choisit un mot de passe qui est inclus comme partie intégrante du rapport. Le mot de passe doit ensuite être confirmé par la police, en même temps que d'autres renseignements permettant d'identifier la victime et de s'assurer que la personne ne fait pas l'objet de mesures d'application de la loi qui sont inappropriées[67].

Le contexte canadien

[85] Tant l'approche du « passeport » que celle du fichier national des vols d'identité font l'objet d'évaluations et d'études en cours aux États-Unis. Même si cette évaluation apportera des renseignements utiles qui devraient guider l'élaboration des politiques au Canada qui portent sur cette question, au moins trois facteurs empêchent l'adoption globale de leur approche, à savoir :

1) La séparation des pouvoirs et le cadre constitutionnel.

2) L'usage limité de la prise d'empreintes digitales comme moyen d'identification au Canada.

3) Le caractère plus restreint de l'utilisation et de la divulgation des casiers judiciaires au Canada.

[86] La séparation constitutionnelle du pouvoir législatif ajoute un niveau important de complexité à toute proposition visant à créer un registre national au Canada. Comme cela ressort clairement de l'examen des initiatives législatives lancées aux États-Unis, bon nombre d'entre elles sont destinées à répondre aux conséquences civiles et pénales du vol d'identité. Dans le contexte canadien, le fondement législatif d'un tel registre poursuivant un double objet est loin d'être clair. Les registres nationaux poursuivant un objet double ou multiple qui sont créés en vertu de la compétence législative fédérale doivent régler cette question[68].

[87] En outre, toute base de données nationale devra également s'attaquer à la question des renseignements détenus dans les bases de données provinciales. Bien que la coordination des travaux législatifs et des normes et des pratiques en matière de données puisse faire l'objet de travaux futurs de la Conférence, d'autres questions fondamentales doivent être réglées avant d'entreprendre ces travaux.

[88] Ensuite, il semble que la collecte des empreintes digitales lors de l'identification et le traitement des personnes arrêtées soit plus répandue dans les États américains que dans les ressorts canadiens. Par conséquent, les systèmes qui reposent sur la vérification des empreintes digitales à des fins d'identification ne pourraient pas être simplement importés ou adoptés au Canada sans qu'il soit tenu compte de cette différence. Au Canada, dans de nombreuses circonstances, les empreintes digitales ne sont pas prises lors du processus d'arrestation, notamment dans le cas des infractions punissables par voie de déclaration sommaire de culpabilité ou des infractions désignées en vertu de la *Loi sur les contraventions*[69]. L'élargissement des catégories d'infractions pour lesquelles les empreintes digitales sont recueillies n'est pas une solution aisée, notamment lorsque ces catégories sont susceptibles de porter sur des questions touchant à la réglementation.

[89] Enfin, comme cela est indiqué plus haut, il semble que les dossiers des tribunaux, criminels ou autres, peuvent être consultés à titre gratuit ou sur une base commerciale aux États-Unis. En conséquence, ces dossiers sont fréquemment consultés, dans un grand nombre de circonstances, souvent sans que l'intéressé ne le sache ou n'ait donné son consentement. En outre, bon nombre de ces consultations sont effectuées à partir du nom, sans référence aux empreintes digitales ou à d'autres renseignements. La différence avec le régime législatif et les

pratiques existant au Canada est importante[70]. Par exemple, une vérification de casier judiciaire de la CCCPR nécessite une demande de la personne visée par la consultation, un ensemble complet d'empreintes digitales, ainsi qu'un formulaire de consentement lorsqu'il est prévu que les résultats soient communiqués à un tiers[71].

[90] L'accessibilité plus réduite de ces dossiers au Canada, combinée avec les différences existant au niveau des pratiques de consultation, peut aboutir à une plus grande incidence du préjudice indirect aux États-Unis qu'au Canada. Par conséquent, toute proposition fondée sur la nécessité de régler ce préjudice devra tenir compte de ces différences.

Les pratiques actuelles de conservation des dossiers au Canada

[91] Toute tentative visant à élaborer un modèle analogue doit également tenir compte des pratiques actuelles de la police et des pratiques en matière de conservation des dossiers. Afin de bien comprendre ce contexte, la première étape a été la diffusion d'un bref questionnaire à l'ensemble des provinces et des territoires en vue de déterminer la nature et l'étendue des bases de données utilisées pour conserver et consulter les renseignements relatifs aux condamnations antérieures, aux mandats non exécutés, aux accusations en instance, aux ordonnances judiciaires (mise en liberté, probation, peines avec sursis, ADN, etc.) et la mesure dans laquelle les différents ressorts se partagent ces renseignements. En outre, on leur a demandé quelles mesures avaient été adoptées pour vérifier les allégations suivant lesquelles un accès était la conséquence du vol d'identité, et quelles avaient été les mesures prises une fois cette allégation vérifiée. Le questionnaire avait également pour but de confirmer si la question des déclarations de culpabilité, par voie sommaire ou non, non vérifiées à l'aide d'empreintes digitales étaient la source de préoccupations particulières dans ce contexte. D'autre part, le questionnaire cherchait à déterminer s'il y avait une personne ou un groupe ressource dans chaque ressort qui était chargé de vérifier ou de faire enquête sur cette réclamation, et si la diffusion de cette liste de contacts à travers le pays serait utile.

[92] Nous avons reçu huit réponses d'administrateurs de tribunaux, de bases de données et de services de police provenant de cinq provinces différentes. Les réponses donnaient certaines

indications quant aux pratiques actuelles et aux difficultés que pose le vol d'identité criminel. Elles ont confirmé le fait que les renseignements relatifs à la justice pénale qui sont susceptibles d'être visés par le vol d'identité sont conservés dans diverses bases de données électroniques et des archives sur papier qui sont administrées par les services de police locaux et nationaux, des administrateurs de bases de données sur les véhicules automobiles et du personnel judiciaire. L'objet de ces bases de données et de ces pratiques et les processus qui y sont liés présentent certains traits communs. Il existe cependant des différences importantes.

[93] Parmi les bases de données communes en usage dans l'ensemble du pays, on trouve notamment :

1) **Le Centre d'information de la police canadienne (CIPC)** – une base de données informatique nationale tenue par la GRC, qui comprend un grand nombre de renseignements, y compris les condamnations pénales, les mandats et les alertes. Les renseignements sur les antécédents criminels sont vérifiés par des empreintes digitales, mais ce n'est pas le cas de tous les autres renseignements.

2) **Les bases de données de la police ou du système judiciaire provincial** – les provinces qui ont répondu disposent également de bases de données de la police ou du système judiciaire à l'échelon provincial qui contiennent des renseignements concernant les accusations en instance, les affaires closes, les conditions de libération, les ordonnances de probation ou de peine avec sursis et autres restrictions. Ces systèmes se fondent sur les renseignements recueillis auprès des services de police ou des dossiers des tribunaux. Bien que la majorité de ces systèmes ne contiennent pas de mandats non exécutés, ce n'est pas le cas de tous. La plupart de ces renseignements ne sont pas confirmés par des empreintes digitales, notamment lorsqu'ils concernent des infractions provinciales, règlementaires ou punissables par voie de déclaration sommaire de culpabilité.

3) **Les bases de données provinciales relatives aux véhicules automobiles** – toutes les provinces qui ont répondu tiennent également des bases de données qui comprennent les renseignements relatifs à l'enregistrement des véhicules automobiles et des renseignements connexes. Ces bases de données comprennent

également des dossiers relatifs aux condamnations pour infraction au Code de la route, ainsi que des renseignements concernant le statut des permis et les suspensions ou les retraits de permis de conduire au niveau provincial. Ces renseignements ne sont pas confirmés par des empreintes digitales. Toutefois, certaines provinces utilisent des photographies en même temps que des systèmes de reconnaissance automatique des visages afin d'aider à la vérification de l'identité des détenteurs de permis.

4) **Les bases de données de la police locale** – bon nombre de services de police municipaux et régionaux d'une certaine taille tiennent également des bases de données qui comprennent des constats et d'autres renseignements sur les enquêtes.

[94] Dans toutes ces provinces, les forces de police et le ministère public partagent les renseignements contenus dans ces bases de données, tant au sein-même de la province qu'avec d'autres ressorts. Certains font même une utilisation plus large des bases de données relatives aux véhicules automobiles, en partageant les renseignements provenant de celles-ci avec d'autres organismes gouvernementaux à d'autres fins, telles que l'application des pensions alimentaires pour enfants.

La correction des dossiers

[95] Toutes les provinces qui ont répondu tentent de corriger les dossiers erronés de diverses manières. Elles demandent toutes une enquête visant à vérifier l'allégation de vol d'identité. Dans certaines provinces, ce sont les agents situés le plus près du plaignant qui mènent ces enquêtes, tandis que dans d'autres, ce sont des unités ou des groupes spécialisés qui s'en chargent. De nombreuses provinces ont soulevé la complexité de ces enquêtes, et en particulier la nécessité de soupeser les intérêts des véritables victimes de vols d'identité et ceux des personnes qui tentent de se soustraire à des obligations légitimes ou d'entraver le système judiciaire.

[96] L'obtention des empreintes digitales de la victime et d'autres renseignements d'identification uniques peut s'avérer utile au cours de l'enquête. Cependant, le fait que bon nombre des dossiers en question concernent des infractions punissables par voie de déclaration sommaire de culpabilité, des infractions au Code de la route ou d'autres circonstances qui ne

donnent pas lieu à la prise d'empreintes digitales complique nettement la recherche de la véritable identité de l'auteur du délit. Sur ce point, les ressorts canadiens se distinguent de bon nombre des États américains. La question de savoir quelles sont les données d'identification qui devraient être recueillies dans ces circonstances doit être approfondie davantage et nécessite une vaste consultation avec les organismes d'application de la loi et les autres parties intéressées.

[97] De nombreuses provinces ont également fait part de leur intérêt pour l'établissement d'une liste comprenant les coordonnées des personnes ou des groupes qui prennent part à ces enquêtes. Une telle liste serait utile non seulement dans le cadre des enquêtes mettant en présence plusieurs ressorts, mais également pour corriger les renseignements erronés partagés avec les autorités d'autres ressorts. Elle faciliterait d'autre part la diffusion de « pratiques exemplaires » qui aideraient à rationaliser ces enquêtes et à adopter une démarche cohérente à l'égard de ces questions.

[98] Il existe également un certain nombre de démarches différentes pour la correction des dossiers une fois l'enquête terminée. Ces démarches correspondent généralement à celles qui ont été dégagées par le groupe de discussion dont il a été fait mention plus haut. Certaines provinces ont répondu qu'elles corrigeaient les dossiers erronés générés par le vol d'identité, tandis que d'autres conservent les données saisies avec une annotation indiquant que l'individu identifié a été la victime d'un vol d'identité.

L'identification des victimes

[99] Les réponses au questionnaire ont révélé trois démarches différentes en matière d'identification des victimes. Tout d'abord, certains ressorts ont inscrit une annotation au CIPC indiquant qu'un ou des dossiers étaient associés au vol d'identité, et que la personne nommée a été victime d'un vol d'identité. Il n'est pas clair si ces annotations contenaient des renseignements détaillés au sujet de l'identité de la victime, tels que des empreintes digitales, des photographies ou d'autres éléments d'identification, comme c'est le cas des dossiers de vol d'identité de la base de données du NCIC décrite plus haut. Ensuite, certains organismes locaux de police remettent aux victimes de vols d'identité des lettres qu'ils peuvent produire aux autorités, notamment aux forces de police, pour établir l'allégation de vol d'identité. Enfin, certains ressorts donnent un NIP aux victimes de vol d'identité qu'elles peuvent utiliser pour

permettre leur identification et faire en sorte que les inscriptions erronées ne soient pas ajoutées à la base de données sur les véhicules automobiles, ou encore pour aider une enquête sur un vol d'identité en cours qui porte sur le nom de cette personne.

[100] Bien qu'il existe certaines similitudes importantes entre certaines de ces mesures et celles qui ont été mises sur pied aux États-Unis, il apparaît clairement nécessaire d'étudier la question de manière plus approfondie et de consulter les parties intéressées, notamment celle qui sont chargées de l'application de la loi, avant de pouvoir recommander l'une ou l'autre de ces approches. Il est également clair qu'une telle consultation devrait viser un groupe bien plus large d'agents d'application de la loi, d'administrateurs de bases de données relatives aux véhicules automobiles et de personnel des tribunaux et des registres.

Conclusions

[101] Même s'il reste à déterminer quelles sont l'ampleur et la nature précise du préjudice causé par le vol d'identité criminel au moyen de recherches et d'études empiriques approfondies, il est clair que cette forme de vol d'identité touche un nombre important de personnes et peut causer un préjudice substantiel. Bien que certaines mesures décrites dans ce rapport laissent entrevoir la possibilité d'atténuer ce préjudice, elles font toutes l'objet d'études en cours. Il serait prématuré de recommander l'adoption de l'une quelconque de ces mesures avant de connaître les résultats de ces études.

[102] En outre, une recherche importante est nécessaire pour déterminer les pratiques et les procédures actuelles des organismes d'application de la loi et des autres organismes et participants du système judiciaire en ce qui a trait à la création et à la correction des dossiers et des autres renseignements touchés par le vol d'identité criminel. Il est nécessaire d'avoir une compréhension complète et exacte des pratiques actuelles afin d'être en mesure d'étudier convenablement les répercussions des modifications proposées.

[103] Il faut espérer que cet aspect du rapport permettra de poser certaines des bases de cette recherche. Cependant, le groupe de travail n'a pas la composition, la capacité ou l'expertise requise pour mener cette recherche. L'étude de ces questions nécessiterait un groupe composé,

entre autres, de représentants des forces de police, du ministère public, des administrateurs de tribunaux et des registres de véhicules automobiles. Par conséquent, le groupe recommande de faire parvenir ce rapport aux sous-ministres de la Justice afin qu'ils déterminent quel est le meilleur lieu pour examiner cette importante question.

[104] En plus du mandat découlant de la résolution adoptée lors de la précédente conférence, le groupe de travail a également étudié quelles mesures pourraient être prises pour prévenir le vol d'identité ou pour renforcer la protection des renseignements relatifs à l'identité. La première étape de l'identification de la manière dont des renseignements personnels, y compris des renseignements relatifs à l'identité, peuvent être détournés a nécessité une analyse détaillée de ces activités. Cette analyse s'interroge quant à savoir qui peut obtenir indûment des renseignements, comment ils les obtiennent, comment ils peuvent les utiliser, et qui peut en être victime en conséquence[72].

[105] Avec cette analyse, il est ainsi possible d'étudier quelles sont les mesures qui pourraient être prises pour prévenir ces activités. L'une des manières d'aborder un tel examen est exprimée dans le tableau reproduit ci-dessous. Il décrit la nature générale du problème de l'usurpation de renseignements d'identification ou autres, les renseignements qui sont obtenus, de qui ils sont obtenus et comment ils sont obtenus et utilisés. Sur l'axe horizontal, le tableau délimite une série de mesures qui sont susceptibles de régler le problème. Les mesures décrites relèvent d'un ensemble d'initiatives qui comprend des mesures préventives, administratives, éducatives, réglementaires, législatives et techniques.

[106] L'examen détaillé des diverses activités susceptibles de constituer un risque pour les renseignements sur l'identité et des diverses mesures législatives, procédurales et éducatives qui ont été prises afin de compenser ces risques peut constituer une base solide pour l'élaboration de politiques visant à prévenir ou à limiter l'utilisation abusive des renseignements sur l'identité. En outre, une telle analyse peut révéler des lacunes dans les réponses apportées à l'usurpation de renseignements sur l'identité dans un ressort, ou montrer quelles sont les mesures utilisées dans d'autres ressorts qui peuvent être adoptées à plus grande échelle. L'adoption de mesures adéquates afin de renforcer la sécurité des renseignements et les procédures d'authentification peuvent constituer la meilleure protection contre le vol d'identité.

[107] La conduite d'une telle analyse à l'échelle nationale pourrait constituer un domaine productif pour une étude approfondie du groupe. À des fins d'illustration, voici un extrait de ce second tableau :

PROBLÉMATIQUE APPROPRIATION DE L'INFORMATION	SOLUTIONS PRÉVENTIVES	VOLET ADMINISTRATIF	VOLET ÉDUCATIF	VOLET JURIDIQUE LOIS	VOLET JURIDIQUE RÈGLEMENTS	VOLET TECHNIQUE
	Ne pas donner l'information	Catégoriser l'information pour déterminer celle qui peut être exigée d'une personne ou celle dont on peut exiger la consultation Gestion de la consultation et de la diffusion des documents quels qu'en soient les supports. (ne pas limiter cette gestion aux documents circulant sur l'Internet). Exiger l'épuration des documents contenus dans les dossiers judiciaires, y compris dans les décisions judiciaires.	Programme de sensibilisation sur le fait qu'il ne faut pas donner de l'information sans que cela soit nécessaire et justifié, en particulier sur la nécessité de la protection des renseignements personnels, des identifiants ou des identificateurs de personnes ou d'objets (cartes)	Législation sur la protection de la vie privée. Interdire la cueillette de renseignements non nécessaires à l'objet de la communication. Déjà fait au Québec, tant dans les secteurs publics que privé. Rendre explicite que cette législation s'applique aussi lorsque l'information est consignée dans un document technologique. Déjà fait au Québec dans la LCJTI.	Réglementation sur la diffusion et la destruction de l'information.	Prendre les moyens techniques et opérationnels pour assurer l'habilitation des accès aux documents ou à une partie de l'information qu'ils portent.
	Prévoir l'anonymisation des documents	Faire une directive administrative sur l'anonymisation de	Faire de la formation sur la nécessité et les		Vérifier la possibilité d'appliquer la	Prendre avantage des techniques

		l'information, en particulier lors de la cueillette. de l'information dans le cadre, par exemple, d'une recherche ou d'une enquête ou d'un examen. Rendre la directive applicable dans l'ensemble du gouvernement et, par voie contractuelle ou d'ententes, dans les relations avec ses partenaires.	méthodes d'épuration de l'information contenue dans des documents, particulièrement pour y soustraire les renseignements personnels, avant de rendre ces documents disponibles pour consultation.		règle de l'anonymisation dans le secteur privé, en application de la Loi sur la protection des renseignements personnels dans le secteur privé (L.R.Q., c. P-39.1.)	pour masquer certains renseignements et des techniques de chiffrement de l'information.
	Permettre l'utilisation balisée de pseudonymes, de manière à tenir compte du droit des personnes légalement autorisée à obtenir la véritable identité de l'usager du pseudonyme.			Ex: second alinéa de l'article 48, de la LCJTI: «Le nom distinctif d'une personne physique peut être un pseudonyme, mais le certificat doit alors indiquer qu'il s'agit d'un pseudonyme. Les services de certification sont tenus de communiquer le nom de la personne à qui correspond le pseudonyme à toute personne légalement autorisée à obtenir ce renseignement.»		

	Gérer la destruction des documents	Prendre et appliquer une Directive sur la destruction sécuritaire des documents	Publiciser la nécessité de détruire les documents qui ont terminé leur cycle de vie. Par exemple, proposer les techniques de déchiquetage des documents sur support papier.	Appuyer législativement la prise de règles préalables à la destruction de documents et à la protection des renseignements personnels. Ex: l'article 20 de la LCJTI.		
Qui s'approprie l'information?						
Un inconnu	**Empêcher les intrusions par les inconnus**	Mesures opérationnelles: Identification et authentification de l'identité du personnel et des autres personnes ayant droit d'accès aux locaux, à des objets, dont des serveurs, les dossiers ou certains des documents qu'ils comportent. Établir une politique de sécurité de l'information, tant dans les entreprises publiques ou privées, qui tienne autant compte de la sécurité physique, logique qu'opérationnelle et des mesures de gestion documentaire, de manière que des	Faire une campagne de sensibilisation sur l'importance: 1) de déchiqueter les documents papiers que les personnes mettent au rebut, 2) sur les risques des technologies qui permettent l'intrusion, à partir de l'externe ou de l'interne, dans les ordinateurs (notamment la technologie sans fil) et sur l'acquisition de technologies qui bloquent les	Adopter un cadre juridique qui favorise: 1) l'emploi d'une diversité de moyens d'identification et d'authentification d'identité, 2) la mise en place de procédés de certification pour établir un ou plusieurs faits dont l'identification d'une personne, d'un de ses attributs, droit, pouvoir ou privilège ou l'identification d'un objet ou de leur localisation ou de leur usage. Voir le chapitre III de la LCJTI.		Mettre en place des mesures de contrôle d'accès à des lieux géographiques, à des immeubles ou à des objets. Adopter des technologies qui ne permettent pas l'intrusion à distance, sans autorisation, dans les objets porteurs de documents technologiques. Faire installer des «paravents» sur les guichets automatiques ou des «isoloirs» près des lieux de

		inconnus n'aient pas accès à de l'information qui a de la valeur.	intrusions dans les objets qui servent à la communication.			services où s'effectuent les paiements, afin qu'un inconnu ne voie pas ou n'entende pas l'information associée à la transaction et, en particulier, ne puisse prendre connaissance de l'information permettant le paiement d'un bien ou d'un service.

[108] Malheureusement, la longueur de ce document, à savoir 33 pages, empêche de l'inclure dans le présent rapport. Cependant, il peut constituer un cadre de travail utile pour un examen approfondi des questions liées à l'utilisation frauduleuse des renseignements sur l'identité et une illustration précieuse des mesures qui peuvent être prises pour réduire autant que possible le risque d'utilisation frauduleuse.

---

[1] Ce document peut être consulté en ligne : http://www.ulcc.ca/fr/poam2/Identity_Theft_Paper_Fr.pdf. Le groupe de travail a pris acte des préoccupations soulevées par l'expression « vol d'identité », tout en reconnaissant que ce terme est couramment utilisé pour des raisons de commodité. L'adoption de solutions à plus long terme à ce problème suppose toutefois une analyse plus subtile, et ne devrait pas se limiter aux questions d'identité ni se concentrer uniquement sur l'aspect d'usurpation. L'extrait du tableau figurant en conclusion du rapport donne une bonne illustration d'une telle démarche.

[2] La version intégrale de la résolution peut être consultée à l'adresse suivante : http://www.ulcc.ca/fr/poam2/Joint_Civil_and_Criminal_Resolutions_2007.pdf.

[3] La question de savoir s'il y a lieu de légiférer sur les avis d'atteinte concernant les renseignements personnels qui ne sont pas autrement protégés par les lois sur le respect de la vie privée fait l'objet d'une discussion à la section j) (paragraphe 58). Une province ou un territoire qui ne dispose pas d'une loi sur la protection de la vie privée pourrait se voir demander d'adopter notre loi uniforme à titre d'obligation distincte. Dans une telle province, la LPRPDE s'appliquerait à la plupart de ces renseignements, mais non à tous.

[4] Voir, par exemple, l'art. 4.7 de l'annexe 1 de la LPRPDE pour connaître les principes relatifs aux mesures de sécurité applicables aux renseignements personnels.

[5] Voir le site du Payment Card Industry Security Standards Council : https://www.pcisecuritystandards.org. Il demande aux commerçants détaillants qui acceptent des cartes de paiement de suivre certaines règles concernant la remise, le stockage et la transmission des fiches de cartes de crédit. En voici un bref aperçu : http://en.wikipedia.org/wiki/PCI_DSS. Le code type sur la protection des renseignements personnels proposé par l'Association canadienne de normalisation constituait à l'origine une norme privée (ou norme privée/publique),

avant qu'elle ne devienne une partie intégrante de la LPRPDE. L'annexe de la partie I de la LPRPDE reproduit cette norme en partie mais non dans son intégralité.

[6] Voir par exemple les suggestions relatives aux normes de chiffrement pour les appareils mobiles publiées par le Commissaire à la protection de la vie privée de l'Ontario en 2007 : « Safeguarding Privacy in a Mobile Workplace; Protect the information you keep on your laptops, cellphones and PDAs », http://www.ipc.on.ca/images/Resources/up-mobilewkplace.pdf.

[7] Cela pourrait paraître plus sensé dans ce contexte, par conséquent, d'évoquer le fait que la sécurité des renseignements personnels a été « compromise », plutôt que de parler d'« atteinte ». Le dernier terme est ambigu, et pourrait davantage faire référence à la violation des normes applicables plutôt qu'à une atteinte à la sécurité. Seule la dernière question nous intéresse ici. Cependant, la documentation sur le sujet a tendance à employer les deux termes de manière interchangeable. Qu'il y ait eu une « atteinte » ou que la « sécurité ait été compromise » est une question différente de celle qui consiste à se demander s'il y a eu une « perte » suffisante pour justifier l'émission d'un avis. Selon ce rapport, cette question est indépendante du niveau de conformité à la norme applicable. La question de savoir s'il y a lieu de signaler l'atteinte est traitée au paragraphe 20 *in fine*.

[8] Voir par exemple : « A Chronology of Data Breaches », Privacy Rights Clearinghouse, fréquemment mis à jour : http://www.privacyrights.org/ar/ChronDataBreaches.htm.

[9] Le Commissaire à la protection de la vie privée du Canada, « Principales étapes à suivre par les organisations en cas d'atteintes à la vie privée », http://www.privcom.gc.ca/information/guide/2007/gl_070801_02_f.asp, étape 2(ii) (« Principales étapes »). Pour des conseils similaires de la part du United Kingdom's Information Commissioner, voir « Notification of Data Security Breaches to the Information Commissioner's Office », http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/breach_reporting.pdf.

[10] Le Commissaire à la protection de la vie privée du Canada définit l'atteinte à la vie privée comme étant la collecte, l'utilisation ou la divulgation non autorisée de renseignements personnels. Voir « Introduction au document intitulé "Principales étapes à suivre par les organisations en cas d'atteinte à la vie privée" », http://www.privcom.gc.ca/information/guide/2007/gl_070801_01_f.asp. Le Commissaire à l'information et à la protection de la vie privée de l'Ontario s'exprime de la même manière, dans : « What to do if a Privacy Breach Occurs: Guidelines for Government Organizations », http://www.ipc.on.ca/images/Resources/up-1prbreach.pdf, p. 3 (« What to do »). Néanmoins toutes les recommandations, et toutes les lois sur le sujet, ne renvoient en pratique qu'à l'accès à des renseignements ou à leur divulgation sans autorisation.

[11] Le Commissaire à la protection de la vie privée du Canada, « Principales étapes », ci-dessus, note 9, étape 2(iv) et les Commissaires à l'information et à la protection de la vie privée de la Colombie-Britannique et de l'Ontario, « Assessment Tool », ci-dessous, note 19, étape 1.

[12] K. Kiefer Peretti, « Data Breaches: What the Underground World of 'Carding' Reveals », 25 Santa Clara Computer and High Technology Jl, à venir, en ligne : http://www.cybercrime.gov/DataBreachesArticle.pdf.

[13] M. Minik, « Medical ID Theft: A Threat to your Life and Wallet », The National Notary, mars 2008, p. 48. Le risque d'utilisation de renseignements médicaux peut être plus important lorsque le voleur peut tirer profit de l'assurance de santé privée acquise par la personne dont les renseignements sont utilisés, y compris pour tirer le maximum de prestations en vertu de la police.

[14] Voir les références à la jurisprudence, note 31. Voir également une discussion sur la possibilité pour les détenteurs de données de s'assurer : K.P. Kalinich, « Legal Exposure to the Maxx: Insurance for Breaches of Data Privacy and Information Security », assurance Aon 2008 : http://aon.mediaroom.com/index.php?s=55&item=70 et un blogue de discussion sur ce document sur Network World : http://www.networkworld.com/community/?q=node/26203&nlhtsecstrat=rn_032508&nladname=032508securitystrategiesal.

[15] Les détenteurs de données ont également des coûts à supporter. À titre d'exemple, si un commerçant compromet la sécurité des renseignements des détenteurs de cartes de crédit, l'émetteur de la carte peut avoir à supporter des frais considérables pour la délivrance de nombreuses nouvelles cartes. Aux États-Unis, les émetteurs de cartes ont poursuivi en justice les commerçants pour recouvrer ces frais, bien que cela n'ait pas encore abouti. D. Rice, « Civil Actions for Privacy Violations 2007: Where are we? » site internet de Howard Rice : http://www.howardrice.com/uploads/content/Civil%20Actions%20For%20Privacy%20Violations%202007%20-%20Where%20Are%20We.pdf aux pp 2-4. Certains États ont adopté une loi pour exiger des commerçants qu'ils indemnisent les émetteurs de cartes de crédit dans certaines circonstances. Voir les lois du Minnesota ch. 325E, Bill H.F. 1758, http://wdoc.house.leg.state.mn.us/leg/LS85/HF1758.3.pdf. D'autres États sont en train d'étudier la possibilité d'une telle législation. T. Probin, Privacy Law Blog, « In response to TJX Privacy breach, one state

enacts legislation imposing new security and liability obligations; similar bills pending in five other states », 29 mai 2007. http://privacylaw.proskauer.com/2007/05/articles/security-breach-notification-l/in-response-to-tjx-data-breach-one-state-enacts-legislation-imposing-new-security-and-liability-obligations-similar-bills-pending-in-five-other-states.

[16] Le Commissaire à la protection de la vie privée du Canada, « Principales étapes », ci-dessus, note 9, étape 3.

[17] *Ibid*.

[18] « barring exceptional circumstances. » CIPVP Ontario, « What to do », ci-dessus, note 10, p. 4.

[19] Le Commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique, « Key Steps in Responding to Privacy Breaches », http://www.oipcbc.org/pdfs/Policy/Key_Steps_Privacy_Breaches_(Dec_2006).pdf. p. 3. (« Key Steps – C.-B. »).

[20] CIPVP – BC et CIPVP – ON, « Breach Notification Assessment Tool », décembre 2006, http://www.oipc.bc.ca/pdfs/Policy/ipc_bc_ont_breach.pdf.

[21] C'est en substance ce que le gouvernement général semble vouloir proposer pour la LPRPDE selon les communiqués de presse.

[22] Cela élimine le critère de l'importance pour le risque, mais maintient le critère de la gravité pour le préjudice.

[23] Cela nécessite que le risque se rapporte aux normes législatives pour le traitement des renseignements. Il n'est pas question du préjudice en tant que tel, mais on présume que les normes législatives ont été créées pour empêcher le préjudice. C'est ce que recommande le CIPPIC dans son mémoire au Parlement en janvier 2008. Mémoire du CIPPIC à Industrie Canada concernant les enjeux de la réforme de la LPRPDE : http://www.cippic.ca/uploads/CIPPIC_PIPEDAsubm_15Jan08.pdf, page 8 *in fine*.

[24] Voir la discussion ci-dessous au paragraphe 45 en matière de contrôle de l'application.

[25] K. Kiefer Peretti, « Data Breaches », ci-dessus, note 12, à la page 28 : [TRADUCTION] « Ces exigences en matière de déclaration sont essentielles à la capacité des policiers d'enquêter sur ce types d'actes criminels qui mettent en cause des atteintes à la protection des données à grande échelle. » L'auteur est un avocat du département américain de la Justice.

[26] Voir le mémoire du CIPPIC sur la LPRPDE, ci-dessus, note 23 page 6.

[27] Le terme commissaire à la vie privé « compétent » évite les préoccupations relatives à la constitutionnalité des lois particulières. Le Québec a contesté la constitutionnalité des règles relatives au respect de la vie privée de la LPRPDE. L'issue de cette contestation peut avoir une incidence sur la question de savoir quel commissaire à la vie privée aura le pouvoir d'agir, et ainsi sur les questions de savoir lequel est « compétent » à l'égard de cette obligation. Cette question dépasse l'objet de cette étude.

[28] Voir ci-dessus le paragraphe 25.

[29] L'étude des autres recours – en particulier de nature civile – que la loi peut permettre et, a fortiori, leur formulation dépassent l'objet de cette étude. Voir cependant la discussion au paragraphe 53 *in fine*.

[30] Les renseignements d'Industrie Canada sont accessibles à http://www.ic.gc.ca/epic/site/oca-bc.nsf/fr/h_ca02226f.html.

[31] Voir par exemple *Pisciotta* v. *Old National Bankcorp*, (2007) 7th circuit Court of Appeals : http://www.techlawjournal.com/courts/2007/pisciotta_onb/20070823.pdf. À l'instar des tribunaux canadiens, les tribunaux américains sont réticents à l'idée d'accorder des dommages-intérêts au titre de la simple perte économique, comme ils ont caractérisé le préjudice résultant du vol d'identité, en dépit du stress psychologique et le temps consacré à se construire une bonne réputation. Voir A. Ramasastry, « Stolen Laptops and Data Theft », Findlaw.com le 15 juin 2006 : http://writ.news.findlaw.com/ramasastry/20060615.html; cependant un tribunal a récemment refusé de rejeter un recours collectif basé sur des faits similaires.

[32] Voir la discussion sur les mesures de rechange au paragraphe 53 *in fine* ci-dessous. Une étude britannique sur les dommages-intérêts accordés en cas d'atteintes intentionnelles au respect de la vie privée prouve qu'ils sont encore peu élevés. Farrer & Co., « Privacy Damages and Harassment », janvier 2008, http://www.farrer.co.uk/Default.aspx?sID=17&cID=974&ctID=11.

[33] La loi est rapportée sur Out-law.com le 12 mai 2008 : http://www.out-law.com/page-9110.

[34] Le droit américain en général offre une vérification gratuite par an. Les victimes du vol d'identité bénéficient toujours de droits additionnels pour procéder à une vérification gratuite.

[35] Les dispositions sur le gel de l'accès au crédit en particulier sont analysées par les associations de consommateurs : http://www.consumersunion.org/campaigns//learn_more/003484indiv.html. Voir aussi http://www.financialprivacynow.org et http://www.pirg.org/consumer/credit/statelaws.htm.

[36] Un certain nombre de services privés offrent ce qu'ils prétendent être des méthodes pour empêcher le vol d'identité ou y remédier. Pour une étude de ces services, voir http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9083098.
[37] Il y a encore un risque que quelqu'un utilise un compte existant, plutôt que d'en ouvrir un nouveau.
[38] Le groupe de travail de la CHLC n'a pas encore consulté les agences d'évaluation du crédit des consommateurs sur l'opportunité ou la gestion d'une telle exigence.
[39] Pour un bref résumé à la fin de l'année 2006, voir le rapport du Commissaire à la protection de la vie privée du Canada pour le Parlement, annexe VI : « Aperçu des lois américaines en matière de notification des atteintes à la protection des données » : http://www.privcom.gc.ca/parl/2007/sub_070222_06_f.asp. Un tableau très approfondi en matière de notification des atteintes à la sécurité est fourni par le cabinet d'avocats Perkins Coie à http://www.digestiblelaw.com/files/upload/securitybreach.pdf.
[40] L'auteur n'est pas certain si la LPRPDE est censée s'appliqué à tous les renseignements personnels dans les territoires.
[41] La nature, l'étendue et la fonction de ces dispositions sont décrites dans des documents du bureau de protection de la vie privée du ministère californien des affaires des consommateurs. Un aperçu en est fourni dans le document intitulé « How to Use the California Identity Theft Registry: A Guide for Victims of 'Criminal' Identity Theft », accessible à l'adresse suivante : http://www.privacy.ca.gov/cover/identitytheft.htm.
[42] « Report of the BJS/SEARCH National Focus Group on Identity Theft Victimization and Criminal Record Repository Operations », du Bureau of Justice Statistics et du National Consortium for Justice Information and Statistics (SEARCH), page 3, accessible en ligne à l'adresse suivante : http://www.search.org/files/pdf/NatFocusGrpIDTheftVic.pdf.
[43] « How to use the California Identity Theft Registry: A Guide for Victims of 'Criminal' Identity Theft », California Department of Consumer Affairs Office of Privacy Protection, page 2, accessible en ligne à http://www.oispp.ca.gov/consumer_privacy/consumer/documents/pdf/cis8englsih.pdf.
[44] Présentation de Beth Givens, Directrice, Privacy Rights Clearinghouse, lors du sommet tenu en Californie sur le vol d'identité en 2005, accessible en ligne à http://www.privacyrights.org/ar/CASummit-CrimIT.htm, « Establishing a National Research Agenda on Identity Management and Information Protection: Report of the CIMIP Identity Management Research Workshop », pages 16, 28. Center for Identity Management and Information Protection, Utica College, juillet 2007. Les documents de recherche de cette organisation sont accessibles en ligne à www.cimip.org.
[45] Voir, par exemple, « Identity Fraud Trends and Patterns: Building a Data-Based Foundation for Proactive Enforcement », Gordon, Rebovich, Choo, Gordon, Center for Identity Management and Information Protection, Utica College, octobre 2007.
[46] « First Estimates from the National Crime Victimization Survey: Identity Theft, 2004 », Katrina Baum, Bureau of Justice Statistics Bulletin, avril 2006.
[47] Federal Trade Commission 2006 Identity Theft Survey Report, aux pages 61-4, Synovate, novembre 2007.
[48] Voir, par exemple, « Report on Identity Theft », Groupe de travail binational sur les fraudes transfrontalières par marketing de masse, octobre 2004, disponible à l'adresse suivante : http://www.ps-sp.gc.ca/prg/le/bs/report-fr.asp#ftn02.
[49] De nombreux rapports comprennent des déclarations anecdotiques convaincantes. Voir, par exemple, « Identity Theft » dans Problem Oriented Guides for Police: Problem Specific Guide Series No. 25, pages 17-19, Office of Community Oriented Policing Services, United States Department of Justice, presentation de Beth Givens, *supra*.
[50] De nombreux articles décrivent ces aspects du problème, notamment Report of the BJS/Search Focus Group, *supra*, aux pages 4-5, « Report of the National Task Force on the Commercial Sale of Criminal Justice Record Information », The National Consortium for Justice Information Statistics, 2005, disponible à l'adresse suivante : http://www.search.org/files/pdf/RNTFCSCJRI.pdf.
[51] Groupe de réflexion, *supra,* à la page 8.
[52] Groupe de réflexion, *supra,* à la page 6.
[53] Voir, par exemple, « Do you have the Background Check Blues » dans Privacy Update No.1:8, 17 décembre 2003, Privacy Rights Clearinghouse. Ce document est disponible à l'adresse suivante : http://www.privacyrights.org/newsletter/031217.htm#3.
[54] Groupe de réflexion, *supra,* à la page 6.
[55] Groupe de réflexion, *supra,* à la page 7.
[56] Minnesota HF 1943, Session 84, Wyoming Senate File SF0053, Arizona HB 2716, Illinois, 20 ICLS 2630/5(b).
[57] How to use the California Identity Theft Registry, *supra*, aux pages 2-3.

[58] How to use the California Identity Theft Registry, *supra,* à la page 5.
[59] How to use the California Identity Theft Registry, *supra,* à la page 6.
[60] California Penal Code 530.6, 851.8(a)-(d).
[61] California Penal Code 851.8(h).
[62] Témoignage de Joanne McNabb, Chief, California Office of Privacy Protection, 21 mars 2007, Senate Judiciary Committee. Ce témoignage est disponible à l'adresse suivante : http://judiciary.senate.gov/testimony.cfm?id=2582&wit_id=6196. Voir également « Locking up the Evil Twin: A Summit on Identity Theft Solutions », 1er mars 2005, à la page 8. Ce document est disponible à l'adresse suivante : http://www.idtheftsummit.ca.gov/2005_report.pdf.
[63] « Identity Theft Victim Verification/Passport Demonstration Program », Office for Victims of Crime, Department of Justice, février 2004, disponible à l'adresse suivante : http://www.ojp.usdoj.gov/ovc/fund/pdftxt/idtheftsolicitation.pdf, « Passport Helps Rescue Ohio Identity Theft Victims », Nevin Barich, National Notary Association, Notary News 15 août 2005, Voir également http://www.haskinspolice.org/pages/programs/passport-program.php.
[64] « Identity Theft Statutes and Criminal Penalties », 13 juin 2006, « 2007 Enacted Identity Theft Legislation », National Conference of State Legislatures, disponible à l'adresse suivante : http://www.ncsl.org/programs/lis/privacy/idt-legis.htm.
[65] « Combating Identity Theft: A Strategic Plan », avril 2007, President's Task Force on Identity Theft, disponible à l'adresse suivante : http://www.idtheft.gov/reports/StrategicPlan.pdf.
[66] « Identity Theft Verification PASSPORT Program: Fiscal Year 2006 Annual Report », Crime Victim Services Section, Office of the Ohio Attorney General, disponible à l'adresse suivante : http://www.ag.state.oh.us/victim/pubs/06passport_report.pdf.
[67] « The National Crime Information Center Identity Theft File » Vernon M. Keenan, Director, et Marsha O'Neal, Criminal Justice Information System Operations Manager, Georgia Bureau of Investigation, Decatur, Georgia, disponible à l'adresse suivante : http://policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=1186&issue_id=52007. Voir également, Groupe de réflexion, *supra,* à la page 8, « National Crime Information Center (NCIC) Technical and Operational Update », 06-1, 28 avril 2006, disponible à l'adresse suivante : http://judiciary.senate.gov/testimony.cfm?id=2582&wit_id=6196. Ce renseignement ne peut être inclus qu'avec le consentement de la victime, « National Crime Information Center (NCIC) Technical and Operational Update, 06-1, 06-1, 28 avril 2006, disponible à l'adresse suivante : http://judiciary.senate.gov/testimony.cfm?id=2582&wit_id=6196, « Information Bulletin 05-14BCIA », National Crime Information Center (NCIC) Identity Theft File, California Department of Justice, 1er juin 2005.
[67] Par exemple, les questions constitutionnelles sur ce sujet ont été un élément abordé dans les consultations portant sur la création d'un Fichier de données génétiques sur les personnes disparues, disponible à l'adresse suivante : http://ww2.ps-sp.gc.ca/publications/Policing/mpi/index_f.asp#7.
[68] Par exemple, les questions constitutionnelles sur ce sujet ont été un élément abordé dans les consultations portant sur la création d'un Fichier de données génétiques sur les personnes disparues, disponible à l'adresse suivante : http://ww2.ps-sp.gc.ca/publications/Policing/mpi/index_f.asp#7.
[69] *Loi sur l'identification des criminels*, L.R.C. 1985, c. I-1, paragr. 2(1).
[70] Loi sur la protection des renseignements personnels et les documents électroniques 2000 c.5, Annexe 1, Principe 4.3. L'exemption relative aux organismes d'enquête désignés ne s'applique pas dans le cadre des vérifications d'antécédents.
[71] Voir, par exemple, les instructions du service de dactyloscopie à des fins civiles de la GRC disponibles à l'adresse suivante : http://www.rcmp-grc.gc.ca/crimrec/finger2_f.htm.
[72] Les deux documents mentionnés dans ces paragraphes ont été préparés par Jeanne Proulx, avocate-légiste, Québec. Ils s'intitulent « Protection contre l'appropriation d'information, volet prévention » et « Appropriation d'information, grille d'analyse ». Malheureusement, en raison de la taille de ces documents, ils ne pouvaient pas être inclus au présent rapport, mais ils peuvent être mis à disposition sur demande.