La sécurité précaire des données personnelles en Amérique du Nord

Une analyse des statistiques disponibles

Benoît Dupont & Benoît Gagnon

Note de recherche no. 1

Chaire de recherche du Canada en sécurité identité technologie

Cette recherche a été entreprise grâce, en partie, au soutien financier du Programme des chaires de recherche du Canada.

La Chaire de recherche du Canada en sécurité, identité et technologie de l'Université de Montréal mène des études sur les pratiques délinquantes associées au développement des technologies de l'information, ainsi que sur les mécanismes de contrôle et de régulation permettant d'assurer la sécurité des usagers. Elle collabore pour cela avec des organismes gouvernementaux et des entreprises.

Prof. Benoît Dupont
Centre International de Criminologie Comparée (CICC)
Université de Montréal
CP 6128 Succursale Centre-Ville
Montréal QC H3C 3J7 - Canada
benoit.dupont@umontreal.ca
www.edupont.net
Fax : +1-514-343-2269

Faits saillants

Au cours des dernières années, de nombreux incidents impliquant le vol ou la perte de données personnelles ont été rendus publics par des entreprises ou des organismes gouvernementaux, aussi bien aux États-Unis qu'au Canada. Même si ces pertes ou ces vols ne se traduisent pas systématiquement par des fraudes associées au vol d'identité, ils dénotent un déficit manifeste et systématique de sécurité en ce qui concerne la collecte, le traitement, le stockage et la gestion informatique des données personnelles. Cette note de recherche a pour objectif de mesurer la quantité d'informations personnelles compromises en Amérique du Nord au cours de la période 2005-2007, afin de comprendre quelles étaient les principales vulnérabilités auxquelles étaient exposées les organisations.

Pendant la période considérée, nous avons identifié 976 incidents de pertes ou de vols de données, ayant donné lieu à la compromission de 313 millions de dossiers personnels.

Nous avons pu recenser 23 événements ayant eu lieu au Canada pour un total estimé de 4,4 millions de dossiers personnels compromis, mais en l'absence d'une obligation légale de divulgation pour les organisations victimes, ce chiffre nous semble fortement sous-estimé.

Le nombre médian de dossiers compromis par incident est de 6000, avec des variations allant de quelques centaines de dossiers à 94 millions, comme ce fut le cas dans l'affaire TJX (magasins Winner's au Canada).

Tous les secteurs d'activités semblent également affectés par des défaillances en matière de protection des données personnelles. Les secteurs de l'éducation, de la santé, les divers services gouvernementaux ainsi que les institutions financières sont les quatre principaux pourvoyeurs d'incidents.

Plus de la moitié des incidents sont attribuables à des vols d'équipements informatiques tels que des ordinateurs portables, ou à la négligence d'employés des organisations concernées. Le piratage informatique ne concerne que 22,7% des affaires analysées. Il apparaît donc que ces incidents pourraient facilement être prévenus par une meilleure formation dispensée aux employés et le recours à des politiques plus strictes de transfert et de chiffrement des bases de données sensibles.

Les principales victimes individuelles de ces incidents sont les usagers des services publics (35,1%), devant les employés des organisations concernées (22,8%) et les clients des entreprises impliquées (20,9%). La diversité des victimes individuelles et leur répartition relativement équilibrée selon les catégories semblent indiquer que ce sont

bien les modes actuels de gestion des informations personnelles qui posent problème aux organisations, quelles que soient les personnes concernées.

Bien que l'on observe une diminution du nombre d'incidents déclarés pour l'année 2007, après une forte augmentation en 2006, il est encore trop tôt pour dire si cette tendance est durable et si elle peut être attribuée à l'entrée en vigueur aux États-Unis de lois obligeant les organisations à notifier publiquement les incidents dont elles sont victimes. Par ailleurs, le contexte actuel de crise économique dans les secteurs immobilier et financier risque de générer de fortes pressions sur les organisations et leur sécurité informatique, créant un risque accru de vols et de pertes.

L'absence de dispositions législatives de divulgation et de notification au Canada est problématique, dans la mesure où cela nous empêche d'avoir une image précise de la situation et des risques auxquels sont exposés les citoyens canadiens. Ce déficit d'imputabilité et de transparence limite également l'action des organisations et les individus qui souhaitent mettre en place des moyens efficaces de protection contre ces brèches de sécurité.

Il se passe rarement une semaine sans qu'une administration ou une entreprise égare ou se fasse voler les données personnelles de milliers ou de dizaines de milliers d'usagers, d'employés ou de clients. L'exemple le plus médiatisé au cours des derniers moins a sans aucun doute été l'affaire *TJX*. Cette entreprise, qui possède au Canada les enseignes *Winners* et *HomeSense*, s'est fait dérober en 2006 les numéros de carte de crédit de 94 millions de clients nord-américains et anglais (Kerber, 2007; Lemos, 2007). La multiplication de ce type d'incidents nous amène à nous questionner sur l'intégrité des données personnelles que détiennent les organismes publics et les entreprises. Même si ces pertes ou ces vols ne se traduisent pas systématiquement par des fraudes associées au vol d'identité, ils dénotent un déficit manifeste et systématique de sécurité en ce qui concerne la collecte, le traitement, le stockage et la gestion informatique des données personnelles. Cette situation est d'autant plus préoccupante que les citoyens sont constamment invités à communiquer dans leur vie quotidienne toujours plus de données personnelles, sous prétexte d'améliorer les services qui leurs sont offerts ou afin de vérifier la légitimité de leurs transactions financières ou administratives.

Afin de dépasser les analyses inévitablement fragmentées que nous offrent les médias à travers la litanie des grands titres annonçant quotidiennement des incidents de perte ou de vol de données, nous avons cherché à obtenir une image statistique générale des tendances dans ce domaine. À l'aide de données empiriques publiquement disponibles, nous avons tenté de mesurer l'ampleur du problème de la perte et du vol des données personnelles au cours des trois dernières années en Amérique du Nord, afin de comprendre quelles étaient les principales vulnérabilités à leur origine, et quels mécanismes règlementaires, technologiques et organisationnels seraient les plus efficaces pour les enrayer.

Méthodologie

Pour procéder à cette étude, nous avons constitué notre propre base de données d'incidents à partir de plusieurs sources publiques disponibles sur le sujet. Trois sources principales servent de support à notre étude. Notre principale source est la base de données de la *Privacy Rights Clearinghouse*[1], qui recense les incidents de pertes et de vols de données personnelles depuis le 1er janvier 2005. La seconde source utilisée est la liste d'incidents colligée par le *Wayne Madsen Report*[2], et la troisième est la liste élaborée par Rita Tehan (2007) pour le *Congressional Research Service*[3]. **La fiabilité de ces données est inégale pour les États-Unis et pour le Canada.** En ce qui concerne les États-Unis, la plupart des entreprises et des services publics sont soumis à une

[1] http://www.privacyrights.org/ar/ChronDataBreaches.htm#CP, consultée le 20 octobre 2008.

[2] http://www.waynemadsenreport.com/categories/20070503, consultée le 20 octobre 2008. Il est à noter que l'accès à cette page était gratuit jusqu'au début de l'année 2008.

[3] Depuis la fin de notre projet, une base de données interactive s'est ajoutée au trois sources principales que nous avons utilisées. Il s'agit de la Dataloss DB [database] de l'Open Security Foundation, accessible à http://datalossdb.org/, consultée le 20 octobre 2008.

obligation de divulgation et de notification des incidents impliquant la perte ou le vol de données personnelles[4], et ces derniers sont par conséquent largement médiatisés. Le Canada ou ses provinces ne disposant pas d'un tel cadre règlementaire, la décision de rendre publics de tels incidents relève de la bonne volonté des organisations impliquées, ou de la sagacité des journalistes. Nous avons par conséquent effectué des recherches approfondies dans les archives de trois grands organes de presse : *Radio-Canada* (et son pendant anglophone *CBC*), le quotidien francophone *La Presse*, et le quotidien national *Globe & Mail*.

La période retenue pour notre étude commence en janvier 2005 et se termine en janvier 2008. Nous disposons ainsi de trois années de données, ce qui nous permet d'observer l'évolution du nombre d'incidents sur une moyenne durée. Notre base de données est constituée pour ces trois années de **976 incidents**, qui varient de quelques dizaines de dossiers compromis à plusieurs dizaines de millions.

Dans bien des cas, l'information disponible dans les bases de données de référence n'était pas suffisante, et des recherches complémentaires sur les sites Internet de quotidiens nationaux ou locaux ont été menées, afin de préciser le secteur d'activité de l'organisation au cœur de l'incident, le type d'incident et ses causes, le nombre et le profil des victimes, ainsi que la chronologie de l'incident. Pour cette dernière variable, **lorsque plusieurs estimations étaient proposées, nous avons choisi de retenir systématiquement la plus conservatrice afin de ne pas céder à la surenchère statistique.**

Résultats

Comme nous l'avons précisé dans la section précédente, l'immense majorité des événements (97%) s'est produite aux États-Unis. Nous avons identifié seulement **23 affaires au Canada**, dont le détail est fourni dans le tableau 1. Cette faible représentation ne doit pas être interprétée comme le résultat d'une meilleure sécurité informatique mise en œuvre par les entreprises et les services publics canadiens, mais plutôt par l'absence d'obligation de déclaration publique qui ne permet pas de connaître le nombre réel d'incidents. En effet, dans son rapport annuel pour l'année 2007-2008, le Commissaire à la protection de l'information et de la vie privée de Colombie-Britannique signale que ses enquêteurs ont été amenés à examiner 96 affaires de données personnelles compromises au cours des 12 mois précédents, par contraste avec 86 incidents en 2006-2007 et seulement 34 incidents en 2005-2006 (Office of Information and Privacy Commissioner for British Columbia, 2008). Les incidents à l'origine de ces enquêtes n'ayant pas été rendus publics, et la Colombie-Britannique

[4] Au mois de juillet 2008, 43 états américains (ainsi que le District de Columbia) s'étaient dotés d'une telle loi. Une carte interactive et régulièrement mise à jour peut être consultée à l'adresse suivante : http://www.csoonline.com/article/221322/CSO_Disclosure_Series_Data_Breach_Notification_Laws_State_By_State, consultée le 20 octobre 2008.

étant la seule province à fournir des statistiques sur le sujet, on peut aisément imaginer que **le nombre réel d'incidents se produisant chaque année au Canada est beaucoup plus important que celui rendu public**.

Tableau 1 : Liste des incidents canadiens figurant dans la base de données

Nom de l'organisation	Date de l'incident	Type d'incident	Nombre de dossiers compromis
Equifax	2ème trimestre 2005	Piratage	2 000
Ministères du travail, de la Santé et de l'immigration de Colombie Britannique	3ème trimestre 2005	Négligence	30 000
Gouvernement de Colombie Britannique	3ème trimestre 2005	Négligence	250 000
Financière MD (Filiale de l'Association Médicale Canadienne)	3ème trimestre 2006	Vol	8 000
Brock University	3ème trimestre 2006	Vol	70 000
Talvest – CIBC	1er trimestre 2007	Perte	470 000
Toronto Hospital for Sick Children	1er trimestre 2007	Vol	2 860
TJX (Winners)	1er trimestre 2007	Piratage	Non disponible pour le Canada
Toronto Hospital for Sick Children	2ème trimestre 2007	Perte	3 300
McGill University	2ème trimestre 2007	Négligence	Non disponible
Coastal Community Credit Union (Nanaimo)	2ème trimestre 2007	Vol	120 000
Calgary Health Region	3ème trimestre 2007	Vol	1 000
Capital Health Edmonton	3ème trimestre 2007	Vol	20 000
TradeFreedom courtier en ligne (Montréal)	3ème trimestre 2007	Piratage	Non disponible
Capital Health Edmonton	4ème trimestre 2007	Vol	270
Ministère de la santé de Colombie Britannique	4ème trimestre 2007	Perte	618
Edmonton Catholic School District	4ème trimestre 2007	Vol	560
Passeport Canada	4ème trimestre 2007	Négligence	Non disponible
Laboratoire provincial de santé publique (Terre Neuve et Labrador)	4ème trimestre 2007	Négligence	Non disponible
Service Canada	4ème trimestre 2007	Vol	1 600
Eastern School District (St Jean - Terre Neuve et Labrador)	1er trimestre 2008	Perte	28 000
Gouvernement de Terre Neuve et Labrador	1er trimestre 2008	Négligence	694
Bell	1er trimestre 2008	Vol	3 400 000
Total			**4 408 902**

Nous disposons de données concernant le nombre de dossiers compromis pour seulement 781 des 976 incidents dans notre base de données. **Au total, pendant les trois années étudiées, le nombre de dossiers personnels compromis (qu'il s'agisse de pertes non élucidées, de négligences ou de vols) s'élève à un peu plus de 313 millions**. On doit préciser qu'il s'agit là de dossiers dont l'intégrité n'est plus assurée par les organisations détentrices, ce qui n'implique pas des fraudes systématiques qui pourraient être associées à un préjudice financier ou moral pour les victimes individuelles. Par contre, il s'agit d'un excellent indicateur de la porosité des systèmes informatiques de stockage et de traitement des données personnelles. **Le nombre médian de dossiers compromis par incident est de 6 000**. Ce chiffre peut paraître relativement bas en comparaison du nombre total, mais quelques brèches contribuent de manière disproportionnée à gonfler les statistiques, à l'image de l'entreprise TJX (notamment propriétaire au Canada des magasins *Winners* et *Homesense*) qui est accusée par les banques américaines de s'être fait dérober 94 millions de numéros de cartes de crédit à la fin de l'année 2006 (Kerber, 2007; Lemos, 2007).

Tous les secteurs d'activités semblent également affectés par des défaillances en matière de protection des données personnelles, comme en atteste le tableau 2.

Tableau 2 : Distribution des incidents et des dossiers compromis par secteur d'activité

Secteur d'activité	Pourcentage des incidents (N=976)	Pourcentage des dossiers compromis (N=781)
Éducation	29,0 %	32,1 %
Services gouvernementaux	17,1 %	17,9 %
Santé	15,6 %	15,5 %
Finance	15,6 %	14,3 %
Industrie	7,0 %	6,4 %
Commerce de détail	6,9 %	6,0 %
Sécurité	4,8 %	4,3 %
Autres	4,0 %	3,5 %
Total	**100,0 %**	**100,0 %**

Les organisations du secteur de l'éducation (Universités, collèges et écoles secondaires) semblent les plus touchées, puisqu'elles composent près du tiers de notre échantillon et du nombre de dossiers compromis pendant la période considérée. Les deux secteurs les plus exposés sont ensuite les différents services gouvernementaux et le secteur de la santé[5]. Les entreprises ne viennent qu'en quatrième rang avec d'abord les institutions financières, puis les autres entreprises de production de biens et de services[6] et le secteur du commerce de détail. Enfin, comme on peut le voir, le secteur de la sécurité,

[5] Nous avons décidé de distinguer les secteurs de la santé et de l'éducation de la catégorie « services gouvernementaux », car aux États-Unis, ces services sont offerts par une large palette d'acteurs publics et privés. De plus, leur forte représentation dans notre échantillon justifiait selon nous qu'on les distingue des autres services publics.

[6] Catégorie « industrie ».

qu'il s'agisse d'organismes publics (défense, services de police) ou d'entreprises de sécurité privée, n'est pas épargné.

On voit donc ici que **les données personnelles des citoyens ne sont pas mieux protégées par les services publics que par les intérêts privés**, et que **certains domaines comme l'éducation ou la santé sont même particulièrement à risques**. Ce constat est particulièrement problématique dans la perspective de la promotion qui est faite des services gouvernementaux en ligne (le *e-government*), puisque les services publics ne semblent pas en mesure de garantir l'intégrité des données personnelles et des transactions électroniques qui y sont associées. Dans la mesure où l'universalité d'accès aux services publics entraîne la création de fichiers qui regroupent des informations sur l'ensemble de la population, on peut aussi se poser la question de la prise de conscience au sein des administrations de l'intérêt que représente pour les fraudeurs l'accès à un tel gisement de données personnelles. Dans les deux cas, des investissements massifs devront être consentis au titre de la sécurité des données personnelles, aussi bien sur le plan des solutions technologiques que de la formation des fonctionnaires aux bonnes pratiques en ce domaine.

À ce stade, nous avons utilisé le terme d'incident pour désigner de manière générique l'ensemble des cas de compromission de données personnelles, quelle qu'en soit l'origine. Il est toutefois indispensable d'opérer une **distinction entre les différentes causes, afin notamment de comprendre quelles seraient les mesures de prévention les mieux adaptées** afin d'en réduire le nombre. Le tableau 3 offre, à partir des renseignements parcellaires à notre disposition, une image des failles les plus fréquemment observées.

Avant d'interpréter ces chiffres, il est nécessaire de préciser comment sont définies les catégories du tableau. La catégorie « vol » concerne les vols de supports physiques contenant des données personnelles, comme des ordinateurs portables, des disques durs, des clés de stockage USB ou encore des cédéroms. La négligence, quant à elle, fait référence à une erreur humaine, notamment en ce qui concerne les paramétrages techniques des équipements et des logiciels utilisés pour la gestion des informations personnelles. Il s'agira par exemple de la mise en ligne sur Internet d'informations résultant d'une mauvaise maîtrise des fonctions de sécurité d'un serveur informatique ou d'une base de données commerciale. Ces négligences pourraient souvent être prévenues par une meilleure formation dispensée aux gestionnaires ou aux opérateurs, ainsi que par l'augmentation des investissements « intelligents » consentis en matière de sécurité. Le piratage englobe l'ensemble des comportements malveillants, qu'ils proviennent de l'extérieur ou de l'intérieur de l'organisation ciblée, et qui se traduisent par une atteinte à l'intégrité des systèmes de gestion des données personnelles. Enfin, la perte correspond à une situation où la localisation des données est impossible, mais où il reste possible qu'elles n'aient pas quitté les systèmes ou les locaux de l'organisation. La dernière catégorie (causes multiples ou indéterminées) comprend les incidents dans lesquels plusieurs des causes mentionnées précédemment se sont

cumulées, ainsi que ceux pour lesquels nous ne disposions pas d'informations suffisantes pour procéder à un classement.

Tableau 3 : Distribution des causes d'incidents

Causes des incidents	Pourcentage du total des incidents recensés (N=976)
Vol	40,1 %
Négligence	24,7 %
Piratage	22,7 %
Perte	6,5 %
Causes multiples ou indéterminées	6 %
Total	**100,0 %**

On voit que **le piratage n'arrive qu'en troisième position, loin derrière le vol de supports physiques et les négligences**. Le vol de supports physiques est essentiellement le résultat de petits délinquants qui s'emparent d'ordinateurs portables dans des véhicules ou dans des espaces publics afin de les revendre pour leur valeur marchande, et qui ne cherchent que rarement à exploiter les données personnelles contenues dans ces machines, ne prenant pas le plus souvent la peine de vérifier les contenus des disques durs. Il est cependant préoccupant de constater à quel point **des quantités importantes de données sont compromises de manière aussi rudimentaire**, alors que des solutions de sécurité élémentaires et efficaces, comme le chiffrement des données à la volée, existent depuis des années et peuvent être utilisées sans détérioration notable des performances. La seconde cause de compromission, la négligence, pourrait également être facilement réduite, dans la mesure où elle n'implique pas l'activité d'un adversaire criminel plus ou moins organisé. Elle traduit cependant la complexité croissante des systèmes de gestion et de traitement des données personnelles, dont le fonctionnement technique devient de plus en plus opaque et difficile à contrôler, y compris pour des informaticiens chevronnés.

Enfin, une analyse de la répartition des victimes individuelles (c'est-à-dire les personnes physiques correspondant aux dossiers compromis) par catégorie démontre que **les organisations éprouvent autant de difficulté à sécuriser les informations de leurs clients ou leurs usagers[7] que celles de leurs employés**. Le tableau 4 illustre cette réalité, en tenant également compte des affaires dans lesquelles les données personnelles de plusieurs types de victimes ont été compromises simultanément.

[7] La distinction entre client et usager correspond à la nature payante ou non des services ou des biens offerts par l'organisation impliquée. Ainsi, les clients sont principalement concernés dans les incidents qui impliquent des institutions financières ou des commerces de détail, alors que les usagers pourront aussi bien être des patients du système de santé que des étudiants ou des contribuables.

Tableau 4 : Distribution des victimes individuelles

Type de victime individuelle	Pourcentage du total des incidents recensés (N=975)
Usagers	44,3
Employés	22,8
Clients	20,9
Usagers et employés	5,1
Employés et clients	1,1
Employés et fournisseurs	0,7
Usagers, employés et fournisseurs	0,3
Employés et contribuables	0,2
Non disponible	4,6
Total	**100,0**

La diversité des victimes individuelles et leur répartition relativement équilibrée selon les catégories semblent indiquer que ce sont bien les modes actuels de gestion des informations personnelles qui posent problème aux organisations, quelles que soient les personnes concernées. Si un tel constat démontre que nous sommes tous égaux devant les risques liés à de tels incidents, il peut aussi nous amener à identifier des groupes de pression et des mécanismes incitatifs permettant d'améliorer la sécurité et l'intégrité des données personnelles. Ainsi, devant le nombre significatif d'affaires impliquant des employés, les syndicats qui les représentent seraient tout à fait autorisés à inclure dans les négociations avec les employeurs des discussions relatives à la protection efficace des données personnelles. De même, dans le cadre de relations commerciales soumises aux lois de la concurrence, on pourrait très bien imaginer de rendre public les performances des entreprises par secteur d'activité en matière de sécurité des données privées, afin d'aider les consommateurs à faire un choix éclairé. Enfin, les systèmes d'évaluation de la performance des services publics et de leurs gestionnaires pourraient fort bien inclure des critères reliés à une bonne administration des informations personnelles dont ils ont la charge. La recherche de tels moyens alternatifs de pression sur les organisations semble indispensable, dans la mesure où dans près d'un cas sur cinq (19,6%), les organisations impliquées étaient à l'origine de plus d'un incident au cours de la période considérée, et que neuf d'entre elles avaient déclaré quatre incidents ou plus – la palme revenant sans conteste à l'Université *Purdue* avec six incidents subis en trois ans.

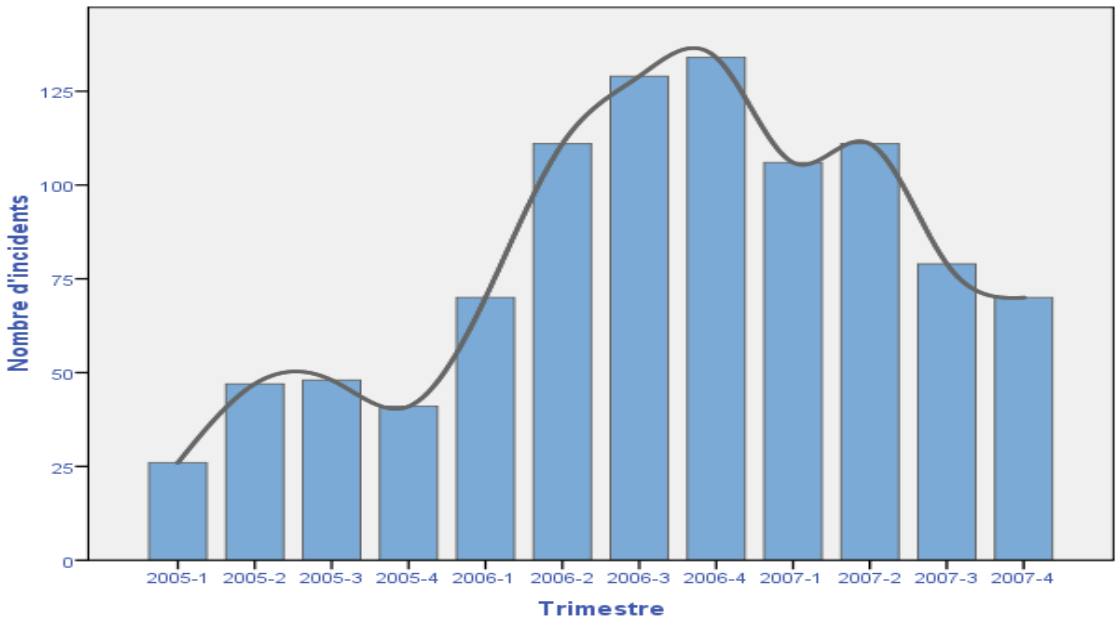
Évolution du phénomène

Étant donné la nature relativement récente des efforts de recueil systématique des statistiques, il est encore **difficile de dégager des tendances temporelles très robustes concernant l'évolution du phénomène**, particulièrement en ce qui concerne le nombre d'incidents enregistrés. Cet indicateur est pourtant essentiel, afin notamment de vérifier si le nombre d'incident est en croissance ou au contraire en repli, ce qui pourrait

confirmer la mise en œuvre de mécanismes de contrôle efficaces de la part des organisations. Le graphique 1 que nous présentons ci-dessous pour les trois années étudiées semble indiquer un **recul du nombre d'incidents à partir du premier trimestre 2007**, après une augmentation régulière au cours des quatre trimestres précédents.

Cependant, **le contexte juridique est selon nous responsable d'une large part de la variation observée**. En effet, la première loi obligeant les organisations à divulguer au public la compromission de données personnelles est entrée en vigueur en Californie en 2003. Ce n'est toutefois qu'à partir de 2005, à la suite d'incidents majeur impliquant les entreprises *Choicepoint* et *CardSystems*, qui perdirent plusieurs millions de dossiers, que les organisations prirent pleinement conscience de leurs obligations, et que d'autres États américains se dotèrent de lois équivalentes. Il paraît donc probable que la forte augmentation observée sur notre courbe de la fin de l'année 2005 à la fin de l'année 2006 ne traduise pas nécessairement une augmentation du nombre de cas, mais plutôt une **augmentation du nombre de cas rendus publics**.

Graphique 1 : Distribution du nombre d'incidents par trimestre



Quant à la **baisse** du nombre des cas déclarés, il est encore **trop tôt pour savoir si elle reflète la mise en œuvre de solutions efficaces de protection des données**. En effet, l'un des objectifs des lois de divulgation adoptées par la majorité des États américains est d'inciter les organisations à investir dans des solutions et des programmes de sécurité des données personnelles. Le raisonnement est le suivant : les organisations seront plus motivées à protéger les données personnelles de leurs usagers et clients si leur réputation risque d'être entachée sur la place publique par des révélations embarrassantes sur les piètres performances de leur sécurité informatique. Ce type d'annonce se traduit la plupart du temps par une perte de confiance de la clientèle ou des usagers, et une baisse de la valorisation boursière pour les entreprises cotées.

S'il est difficile de prédire dans quel sens évoluera la courbe, on peut imaginer que **le contexte économique actuel de crise dans les secteurs financier et immobilier risque de générer des risques supplémentaires pour les consommateurs**[8].

D'abord, la faillite de nombreuses entreprises et de courtiers indépendants liés à des activités de crédit s'accompagnera de la liquidation de leur équipement informatique. Celle-ci se fera le plus souvent de manière expéditive, sans que les supports informatiques de stockage (disques durs) ne soient correctement débarrassés des informations personnelles qu'ils contiennent. Ces ordinateurs qui inonderont le marché risquent ainsi de devenir de véritables mines de données pouvant être exploitées par des personnes mal intentionnées afin de commettre des fraudes comme l'usurpation d'identité.

Ensuite, on peut penser que la présente instabilité économique, et l'augmentation potentielle du taux de chômage qui s'en suivra, risque d'augmenter le nombre d'actes de délinquance informatique comme le piratage de bases de données. En effet, les individus compétents en informatiques privés d'emploi vont probablement développer des stratégies pour maintenir leurs revenus ou éviter une trop grande réduction de leur pouvoir d'achat. La délinquance informatique représente dans ce contexte une façon rapide et efficace de générer des revenus sans encourir des risques trop importants. Par exemple, certains employés mis à pied par leur entreprise emporteront avec eux des fichiers contenant des données personnelles afin de les monnayer auprès de la concurrence à des fins commerciales, ou avec l'objectif de les exploiter eux-mêmes de manière illégale. L'accès d'employés mis à pied à des bases de données informatisées risque également de poser de nombreux problèmes aux organisations qui ne disposent pas de systèmes efficaces d'attribution et de révocation des privilèges d'utilisation.

Enfin, on peut également anticiper que la majorité des entreprises, ainsi que de nombreux services publics, seront amenés à réduire considérablement leurs budgets de fonctionnement, et que les investissements consentis au titre de la sécurité informatique risquent d'être revus à la baisse tant que la situation économique ne se sera pas améliorée.

[8] L'*Identity theft resource centre*, qui collecte également des informations sur les brèches de données informatiques et papier dont sont victimes les organisations américaines prévoit ainsi une augmentation du nombre d'incidents pour l'année 2008. Selon ses statistiques (qui divergent légèrement des nôtres pour les trois années considérées dans cette étude), un nombre équivalent d'incidents à celui recensé en 2007 (soit 449), aurait en effet été atteint aux États-Unis le 22 août 2008, quatre mois avant la fin de l'année.
http://www.idtheftcenter.org/artman2/publish/lib_survey/ITRC_2008_Breach_List.shtml, page consultée le 20 octobre 2008.

Conclusion

En nous basant sur les statistiques publiquement disponibles, nous avons identifié 976 incidents de perte ou de vol de données en Amérique du Nord au cours de la période allant de janvier 2005 à janvier 2008, ayant résulté dans la compromission d'au moins 313 millions de dossiers personnels. Il s'agit là de statistiques conservatrices au vu de la méthodologie de recensement que nous avons privilégiée. Les résultats présentés dans cette note de recherche concernent directement les citoyens canadiens, même s'ils font principalement référence à des incidents survenus aux États-Unis. En effet, ils nous permettent d'abord de juger de l'ampleur d'un **problème qui reste relativement sous-estimé au Canada**, notamment en raison de l'absence d'obligation de divulgation pour les organisations qui en sont les victimes. À moins d'imaginer que les systèmes informatiques soient beaucoup mieux administrés et protégées par les administrations et les entreprises canadiennes que par leurs homologues américains, ce qui paraît fort improbable, on doit assumer que les citoyens canadiens sont beaucoup plus exposés qu'ils ne l'imaginent à des incidents compromettant l'intégrité de leurs données personnelles. Contrairement aux États-Unis cependant, aucun niveau de gouvernement ne s'est jusqu'à présent doté des moyens de connaître avec précision le nombre d'incidents survenus ou leurs caractéristiques, ce qui constituerait la première étape dans une stratégie intégrée de protection des données personnelles.

Les statistiques compilées mettent également en évidence l'exposition de l'ensemble des secteurs d'activité aux risques de compromission des données, et les nombreux incidents associés à la gestion des informations personnelles par les services publics, avec une **surreprésentation notable des secteurs de l'éducation ou de la santé**. Cela est particulièrement préoccupant alors que le Québec et d'autres provinces canadiennes s'apprêtent à implanter les dossiers de santé électroniques, sans avoir véritablement communiqué aux citoyens les risques associés à une telle démarche d'informatisation et les moyens mis en œuvre pour garantir la sécurité des données médicales et personnelles des patients. Il nous apparaît par conséquent impératif que les discours des organisations publiques soient revus, et ce, afin d'informer correctement les citoyens sur les implications de la numérisation grandissante des dossiers gouvernementaux. En effet, alors que bon nombre d'organisations prônent l'informatisation totale de leurs activités en invoquant à la fois des critères d'efficacité et de sécurité, force est d'admettre que le second argument est mis à mal lorsqu'il est confronté à la réalité.

Enfin, il n'existe pas à l'heure actuelle de loi contraignant les entreprises et les administrations canadiennes à divulguer les atteintes à l'intégrité des données personnelles et les brèches de sécurité dont elles sont victimes[9]. Une telle option a bien

[9] La Clinique d'intérêt public et de politique d'internet du Canada a produit une analyse détaillée du contexte juridique canadien, et du contenu des législations de notification votées ces dernières années aux États-Unis (CIPPIC 2007).

été examinée en 2007 à la Chambre des communes par le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique lors de l'examen de la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDÉ). Hélas, en dépit des recommandations de la Commissaire à la protection de la vie privée, et acceptant les arguments présentés par les groupes de pression défendant les intérêts des entreprises, le Comité s'est opposé à la création d'une obligation générale de déclaration en cas de brèche (Wappel, 2007 : 50). On trouve bien sur le site du Commissariat à la protection de la vie privée du Canada un document destiné aux organisations victimes d'une brèche et faisant la liste des critères pouvant être utilisés afin de déterminer si les personnes concernées doivent être informées ou pas[10]. Cependant, les directives figurant dans ce document sont d'application purement facultative.

En raison du coût financier et « réputationnel » de tels incidents pour les organisations qui en sont les victimes, la tentation est forte pour ces dernières de les passer sous silence. Ainsi, aux États-Unis, avant l'entrée en vigueur des lois relatives à la divulgation, un peu moins de la moitié des entreprises multinationales et du commerce de détail disposaient de procédures de notification en cas de brèche (Acoca, 2007 : 43). Dans ce contexte, **l'approche qui prévaut actuellement au Canada est collectivement indésirable**, car elle empêche les personnes dont les renseignements ont été compromis de prendre des mesures afin de se prémunir contre de possibles tentatives de fraude. En ne rendant pas ces incidents et leurs causes publics, les organisations victimes limitent également la capacité des autres organisations d'améliorer leurs pratiques et de mettre en place des programmes ou des solutions permettant de prévenir leur répétition.

Par conséquent, il nous semble souhaitable que le Canada se dote dans les meilleurs délais d'un cadre législatif de divulgation s'appliquant aussi bien aux entreprises privées qu'aux services public, et dont la portée pourrait s'inspirer des mesures déjà adoptées ou en cours d'adoption aux USA, en Australie ou encore au Japon (Acoca, 2007 : 40). La mise en œuvre d'un tel dispositif constitue à l'heure actuelle le moyen le plus efficace de connaître le degré réel de sécurité des données personnelles dans notre pays, et le meilleur levier pour inciter les organisations à améliorer la protection des données qui leurs sont confiées par leurs clients, usagers et employés.

[10] http://www.privcom.gc.ca/information/guide/2007/gl_070801_01_e.asp#_ftn1, page consultée le 20 octobre 2008.

Références

Acoca, Brigitte (2007). *Scoping paper on online identity theft : Ministerial background report*, OCDE : Paris.

Clinique d'intérêt public et de politique d'internet du Canada (CIPPIC) (2007). *Approaches du security breach notification : A white paper*. Université d'Ottawa: Ottawa.

Kerber, Ross (2007). « Court filing in TJX breach doubles toll: 94 million accounts were affected banks say », *The Boston Globe*. Consulté en ligne le 16 octobre 2008 : http://www.boston.com/business/globe/articles/2007/10/24/court_filing_in_tjx_breach_doubles_toll.

Lemos, Robert (2007). « Court filings double estimate of TJX breach », *Security Focus*. Consulté en ligne le 16 octobre 2008 : http://www.securityfocus.com/news/11493.

Office of Information and Privacy Commissioner for British Columbia (2008). *2007-2008 annual report*, OIPCBC : Vancouver. Consulté en ligne le 16 octobre 2008 : http://www.oipc.bc.ca/publications/annual_reports/2008AR/OIPC_AR_2007_08.pdf.

Tehan, Rita (2007). *Data Security Breaches: Context and Incident Summaries - CRS Report RL33199*, Congressional Research Service for Congress, Washington, consulté en ligne le 16 octobre 2008 : http://opencrs.com/document/RL33199/.

Wappel, Tom (2007). *Examen, prévu pa la loi, de la loi sur la protection des renseignements personnels et les documents électroniques (LPRPDÉ) : Quatrième rapport du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique*. Chambre des Communes : Ottawa.