CONFÉRENCE POUR L'HARMONISATION DES LOIS AU CANADA

SECTION CIVILE

LOI UNIFORME SUR LA PROTECTION DE LA VIE PRIVÉE (NOTIFICATION DES ATTEINTES À LA PROTECTION DES DONNÉES)

Groupe de travail sur le vol d'identité

RAPPORT DE 2010

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

Halifax,
Nouvelle-Écosse
Août 2010

CONFÉRENCE POUR L'HARMONISATION DES LOIS AU CANADA

Loi uniforme sur la protection de la vie privée (notification des atteintes à la protection des données)

Groupe de travail sur le vol d'identité

RAPPORT DE 2010

[1] La réunion conjointe des sections pénale et civile de 2008 a demandé au Groupe de travail sur le vol d'identité de rédiger une Loi uniforme pour obliger les organismes qui détiennent des données personnelles à aviser les personnes intéressées de tout événement compromettant la sécurité de ces données. La Loi uniforme devait suivre les recommandations du rapport présenté par le Groupe de travail à cette réunion.

[2] La réunion de 2009 a légèrement modifié les recommandations, examiné et commenté une ébauche de Loi uniforme et conseillé au Groupe de travail de consulter des autorités en matière de protection de la vie privée et des intervenants du secteur privé. Dans le courant de l'année, certains membres du Groupe de travail, voire tous les membres, ont téléphoné à la plupart des organismes indépendants de protection de la vie privée du Canada, c'est-à-dire les commissaires et ombudsmans et/ou leur personnel, et ont communiqué de vive voix ou par écrit avec des juristes et des groupes de protection de la vie privée, ainsi que des représentants d'entreprises, dont l'Association des banquiers canadiens, le Bureau d'assurance du Canada et d'autres.

[3] En 2009-2010, les membres du Groupe de travail étaient :

- Arghavan Gerami, ministère de la Justice du Canada, remplacé en cours d'année par Jennifer Bucknall
- John D. Gregory, ministère du Procureur général de l'Ontario (président)
- Josh Hawkes, Alberta Justice
- Heather J. Innes, Alberta Justice
- Gail Mildren, Justice Manitoba
- Jeanne Proulx, ministère de la Justice du Québec (à la retraite depuis avril 2010)

Clark Dalton de la Conférence pour l'harmonisation des lois au Canada (CHLC) a également participé aux travaux du groupe.

[4] Le Groupe de travail souhaite réitérer le fait qu'une loi sur la notification des atteintes à la sécurité des données ne constitue qu'une petite partie du travail de protection des données personnelles. En effet, la protection des données personnelles se situerait dans le cadre plus large de la protection de données de toute sorte contre l'abus. La Conférence a cependant raison de croire que la notification des atteintes à la sécurité des données personnelles peut justifier un régime législatif particulier.

[5] Comme on l'a fait remarquer les années précédentes, les lois canadiennes sur la protection de la vie privée sont très différentes les unes des autres. Toutes les autorités législatives ont une loi sur les données personnelles recueillies par le secteur public, mais peu nombreuses sont celles qui ont adopté une loi sur les données de ce genre recueillies par le secteur privé (quoique la loi fédérale ait une application large dans ce cas). Dans plusieurs provinces, les renseignements sur la santé, une catégorie importante de données personnelles, font l'objet de règles distinctes. Le responsable de l'exécution du régime varie selon la province : il peut s'agir d'un commissaire qui détient des pouvoirs d'investigation et d'ordonnance ou bien d'un ombudsman qui a le pouvoir de lancer des investigations en se concentrant sur la persuasion, la recommandation et la publicité.

[6] Le Groupe de travail a préparé une loi uniforme sur la notification des atteintes à la sécurité conçue pour s'adapter à ce contexte varié. L'uniformité est importante parce que des données sur une personne peuvent être détenues ou bien communiquées dans tout le pays, et que les détenteurs de données personnelles en détiennent souvent sur des personnes habitant des provinces différentes. Si la sécurité des données dont un détenteur a le contrôle est compromise, il ne sert les intérêts de personne que le détenteur soit soumis à une douzaine de règles incompatibles. Dans une situation idéale, le détenteur sait à quelles règles il est soumis, et les personnes dont les données sont détenues savent à quoi s'attendre.

[7] L'ébauche actuelle de la Loi uniforme vise donc à poser des principes harmonisés partout au Canada. On l'a rédigée pour qu'elle s'adapte aux lois de chaque autorité législative sur la protection de la vie privée. Elle dépend d'ailleurs de ces lois pour sa portée, soit la définition des données personnelles et les personnes responsables de la sécurité des renseignements personnels auxquelles la Loi uniforme

s'applique, et pour son application, c'est-à-dire l'autorité responsable de celle-ci. Le groupe de travail est conscient que la plupart voire la totalité des autorités responsables de la protection de la vie privée au Canada ont adopté des directives pour traiter d'une atteinte à la sécurité de données personnelles. Ces directives sont en général harmonisées à l'échelle nationale grâce à la collaboration active de ces autorités. On considère qu'une loi uniforme renforcera de façon utile ces dispositions.

[8] En bref, l'ébauche de la Loi uniforme s'applique au moment où une personne contrôlant des données personnelles a des motifs de croire que l'information a été consultée ou divulguée d'une manière contraire à ce qu'autorise la loi sur la protection de la vie privée dont les nouvelles règles uniformes feront partie. Si la consultation ou la communication non autorisées présentent un risque réel de préjudice grave pour les personnes auxquelles se rapportent les renseignements, le détenteur doit les aviser promptement de l'atteinte à la vie privée. Dans le cas d'une atteinte importante, le détenteur doit aviser l'autorité compétente, appelé « responsable de la protection de la vie privée » dans l'ébauche de la Loi uniforme. Le contenu de cet avis est laissé principalement au règlement. Le responsable de la vie privée peut obliger le détenteur de données personnelles à notifier les personnes intéressées si ce n'est pas encore fait, et aussi à notifier la police. On prévoit des règlements qui traitent du contenu de la notification à ces personnes. La contravention à la Loi uniforme est sanctionnée par des amendes.

[9] La version provisoire de la Loi uniforme a été touchée par des développements survenus au cours de la dernière année. Au début du projet, la seule loi qui comportait une exigence de notification des atteintes à la protection des données était la loi de l'Ontario sur les renseignements sur la santé[1]. En juin 2010, quatre provinces avaient adopté des lois de notification des atteintes à la protection des données et le gouvernement fédéral a présenté un projet de loi à ce sujet à la Chambre des communes[2]. En 2009, la Nouvelle-Écosse a présenté un projet de loi visant la protection des renseignements sur la santé, mais il n'a pas été adopté[3]. Les dispositions de ces différentes lois ne concordent pas.

- La loi de l'Ontario ne comporte pas de critère. Autrement dit, dès qu'un renseignement sur la santé d'une personne est dérobé, perdu ou consulté par des personnes non autorisées, le « dépositaire des renseignements sur la santé » doit aviser cette personne. Des restrictions à cette exigence pourraient être prescrites, mais il n'existe pour l'instant aucun règlement à cet effet.

- Les autres lois et le projet de loi fédéral comprennent tous des critères fondés sur le risque : il y a devoir de notification lorsqu'un risque de préjudice découle de l'atteinte. Selon la loi de l'Alberta, le commissaire doit être notifié en cas de perte ou de communication de renseignements personnels, ou d'accès non autorisé à ces renseignements, s'il y a un « risque réel de préjudice grave » pour les personnes intéressées. Le commissaire peut demander à la personne qui a le contrôle de l'information d'aviser ces personnes.
- Les lois de Terre-Neuve-et-Labrador et du Nouveau-Brunswick exigent que la personne dont les renseignements de santé ont été volés, perdus, éliminés, communiqués ou consultés d'une façon non autorisée doit être notifiée, à moins que le dépositaire des renseignements a des motifs raisonnables de croire que ce vol, etc. ne nuira ni à la fourniture des soins de santé à la personne, ni à sa santé mentale ou physique ou au bien-être économique ou social. Toutefois, le Nouveau-Brunswick prévoit une exception lorsque le dépositaire est d'avis que l'atteinte ne conduira pas à l'identification de la personne visée par ces renseignements. Terre-Neuve-et-Labrador exige également de signaler toute atteinte importante au commissaire, qui peut recommander d'aviser la personne intéressée même si ce n'est pas requis aux termes de la Loi.
- La nouvelle disposition de la *Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)* exige la notification à la personne intéressée lorsqu'il y a un risque réel de préjudice grave pour celle-ci, et la présentation d'un rapport au commissaire dans le cas d'une atteinte importante. L'incident nécessitant une notification ou un rapport est appelé « atteinte aux mesures de sécurité ».
- Le projet de loi de la Nouvelle-Écosse prévoyait la communication de la perte de données à la personne touchée, sauf si le dépositaire avait des motifs raisonnables de croire qu'il était peu probable qu'il y ait eu atteinte à la protection des renseignements personnels sur la santé ou que l'atteinte ne pouvait mener à un préjudice ou à une humiliation pour la personne.

[10] Le critère déterminé par la CHLC en 2008 et intégré à l'ébauche de la Loi uniforme en 2009 était « un risque de préjudice grave ». Certains intervenants du secteur privé ont critiqué cette formulation en disant qu'il s'agissait d'un critère trop faible, en ce sens qu'elle exigerait la notification même si le risque était hypothétique ou spéculatif.

[11] Industrie Canada a aussi publié en 2008 une proposition de loi accompagnée de commentaires, dans laquelle le critère était « un risque substantiel de préjudice grave »[4]. La commissaire à la protection de

la vie privée du Canada a critiqué ce critère comme étant trop rigoureux, en ce qu'il permettrait à trop d'incidents d'atteinte d'échapper à la notification, ce qui ferait courir trop de risques aux personnes dont les renseignements sont consultés sans autorisation[5]. À n'en pas douter, la formule « un risque réel » se voulait un compromis entre ces deux préoccupations.

[12] Le Groupe de travail recommande l'adoption de la formulation de l'Alberta et du gouvernement fédéral comme critère approprié de notification, soit « un risque réel de préjudice grave ». Cette formulation semble correcte en principe et pourrait devenir une tendance, ou du moins être généralement acceptée dans le domaine législatif. Le fait d'utiliser cette formulation maximise les chances d'adoption de la Loi uniforme. Le Groupe de travail préfère ce critère direct et positif à « l'option négative » des provinces atlantiques, selon laquelle on doit aviser la personne intéressée sauf si le dépositaire de l'information juge qu'il n'y aura aucune conséquence négative pour elle. Il se pourrait que la règle des provinces atlantiques produise davantage de notifications que celle de l'Alberta et du fédéral, car ni la menace, ni le préjudice y sont explicités.

[13] Il est à noter que les règles internes de l'Ontario pour les atteintes à la vie privée dans le secteur public paraissent dans une directive.[6] Cette directive exige une notification des personnes en cas d'atteinte, pour leur dire ce qui s'est passé, la nature du risque véritable ou potentiel et des actions appropriées pour se protéger. L'obligation de notification est sujette à des exceptions au cas où :

- la police fait savoir que la notification nuirait à une enquête criminelle;
- la notification n'est pas dans l'intérêt de la personne (par exemple la notification pourrait mettre la personne en danger ou produire des dégâts supérieurs à ceux produits par l'atteinte elle-même);
- la notification ne servirait à rien (par exemple si tous les renseignements personnels impliqués dans l'atteinte sont : déjà disponibles au public; récupérés avant qu'une personne non-autorisée aurait pu en profiter; protégées par la technologie, comme le cryptage, qui fait que la consultation ou l'emploi non-autorisé des données est en effet impossible) : ou
- il n'est pas possible de notifier les personnes (par exemple parce que l'on ne connaît pas l'identité des personnes touchées par l'atteinte).

[14] Selon les responsables de cette politique de l'Ontario, ces règles offrent plus de certitude qu'un test fondé sur le risque, quant à savoir si l'on devrait notifier les personnes touchées. D'autres provinces ont des dispositions similaires pour leur régime dans le secteur public. A cette heure, cependant, le groupe de travail ne recommande pas des régimes différents pour le secteur public et le secteur privé.

[15] Pour des raisons expliquées dans le rapport de l'année dernière[7], le Groupe de travail est d'avis que le premier devoir de notification devrait échoir à la personne qui a le contrôle de l'information, c'est-à-dire la personne responsable de sa sécurité. Cette règle permet de réduire les délais et met le fardeau de la responsabilité sur la personne responsable de la situation. Elle permet également de réduire la charge de travail des bureaux du responsable de la vie privée. Autrement dit, sur ce point, le Groupe de travail préfère le régime fédéral au régime albertain.

[16] Certains ont critiqué les amendements apportés par le gouvernement fédéral parce qu'ils laissent la décision à la personne qui a le contrôle des renseignements personnels, alléguant que cette personne a tout avantage à ne pas divulguer l'atteinte afin de ne pas nuire à sa réputation[8]. Toutefois, dans la plupart des cas, la seule façon de savoir qu'il y a eu atteinte à la protection des données est par l'entremise de la personne qui a le contrôle des données. Il est rare qu'une personne extérieure à l'organisation du détenteur soit capable de détecter une atteinte et de retracer son origine. La question est donc de savoir ce que la personne qui a le contrôle des données doit faire lorsqu'il y a atteinte, ce qui est explicité autant que possible dans les lois. Il n'existe pas de bonne méthode indépendante d'éviter ou de découvrir les cas où la vérité a été dissimulée. On peut décourager ce genre d'action par la persuasion, l'administration et l'imposition de pénalités en cas de non-conformité. Ce qui plus est, l'obligation générale d'aviser l'autorité responsable de la protection de la vie privée peut aider que ces incidents voient le jour.

[17] Toutes les lois qui s'appuient sur un critère précisent que le dépositaire doit avoir des motifs « raisonnables » de croire. Si cela peut sembler évident, au sens où les personnes qui contrôlent les renseignements personnels ne risquent pas d'agir selon des motifs déraisonnables, le fait d'adopter cette formulation ne nuit cependant aucunement à la cause de l'uniformité. Dans la version provisoire de 2009 de la Loi uniforme, il ne fallait satisfaire aux obligations de la Loi que si le détenteur de données personnelles « avait des raisons de croire » qu'il y avait eu accès non autorisé à l'information. Le fait de baliser le critère en termes de motifs raisonnables est conforme à cette idée.

[18] Le Groupe de travail, ainsi que certaines personnes du secteur privé, sont d'avis que l'idée d'imposer un devoir distinct de signaler au responsable de la vie privée toute atteinte importante est judicieuse[9]. Le critère à cet effet devrait être, comme dans les amendements à la LPRPDE, moins contraignant que celui concernant la notification au public. En pratique toutefois, la différence entre les deux critères aura probablement pour effet que le responsable de la vie privée ne sera pas informé des atteintes mineures qui pourraient conduire à des notifications aux personnes intéressées (un avis envoyé à quelques personnes ne peut sans doute pas être qualifié « d'important »), mais qu'il sera averti des atteintes importantes qui n'entraînent toutefois pas un risque assez important pour justifier des communications aux personnes intéressées.

[19] Dans le rapport de 2009, on débattait de la pertinence d'énoncer en toutes lettres que les obligations imposées à la personne qui a le contrôle des données s'appliquent également à quiconque a été mis au courant de l'incident par cette personne, par exemple un sous-traitant[10]. Aucune directive précise n'a été donnée à ce sujet lors de la réunion de 2009. L'ébauche actuelle de la Loi uniforme ne fait pas mention de cette obligation, elle est implicite dans le passage qui décrit la personne qui contrôle les renseignements personnels. Aucune des lois canadiennes de notification des atteintes à la protection des données ne traite explicitement des tierces parties. En fait, le détail d'un tel critère de « contrôle » peut figurer dans la loi générale sur la protection de la vie privée. Certaines lois visant le secteur public imposent directement des devoirs aux tierces parties. La question est soulevée dans un commentaire sur la Loi uniforme, de façon à ce que les autorités législatives puissent la traiter en fonction de leur contexte propre.

[20] La question de savoir si le responsable de la vie privée détient le pouvoir d'ordonner à la personne qui a le contrôle de l'information d'aviser les personnes intéressées lorsqu'elle a décidé de ne pas le faire est de nature délicate, du fait de la diversité des lois en vigueur au Canada. Certains responsables de la vie privée ont le pouvoir d'ordonnance, d'autres peuvent faire des recommandations et veiller à leur mise en œuvre par l'entremise de procédures judiciaires et d'autres enfin comptent sur la persuasion, les recommandations et la publicité. Le Groupe de travail recommande qu'il y ait entre crochets dans la Loi uniforme une alternative entre un pouvoir d'ordonner et un pouvoir de recommander la notification. Les

autorités législatives décideront quelle variante adopter après débat et dans le respect de la logique de leurs lois.

[21] La réunion de 2009 de la CHLC a exhorté le Groupe de travail de donner des précisions aux intéressés touchés par la loi au sujet de ce qui pourrait constituer un « préjudice grave ». La nouvelle ébauche de la Loi uniforme tient compte de cette recommandation, car on a adopté des formulations tirées de la loi albertaine et du projet de loi fédéral. Selon le projet de loi fédéral C-29, « préjudice grave vise notamment la lésion corporelle, l'humiliation, le dommage à la réputation ou aux relations, la perte financière, le vol d'identité, l'effet négatif sur le dossier de crédit, le dommage aux biens ou leur perte, et la perte de possibilités d'emploi ou d'occasions d'affaires ou d'activités professionnelles[11] ». Les éléments servant à établir s'il existe un risque réel d'un tel préjudice sont décrits dans le projet de loi C-29 comme étant « le degré de sensibilité des renseignements personnels en cause et la probabilité que les renseignements aient été mal utilisés ou soient en train ou sur le point de l'être[12] ». Pour déterminer si une atteinte constitue une « atteinte importante », on doit considérer le degré de sensibilité des renseignements personnels en cause, le nombre d'individus dont les renseignements personnels ont été touchés par l'atteinte et l'évaluation faite par l'organisation selon laquelle la cause de l'atteinte ou la récurrence d'atteintes dénote un problème d'ordre systémique[13]. On discute dans une note sur la rédaction de l'article 102 de la loi proposée si le préjudice devrait faire partie de ce critère.

[22] Le projet de loi fédéral prévoit que la personne qui doit aviser les personnes intéressées de l'atteinte aux mesures de sécurité doit aussi aviser toute organisation en mesure de limiter le préjudice résultant de l'atteinte[14]. Le Groupe de travail a reçu une lettre de Transunion, une société dans le domaine de l'évaluation du crédit. Ses représentants avaient tendance à s'opposer à l'obligation de fournir des rapports de solvabilité gratuitement aux victimes d'atteintes, mais ils ont ajouté que le fait d'être avisés d'une atteinte le plus tôt possible les aiderait à répondre aux personnes qui demanderaient ce genre d'information après avoir reçu la notification. Parmi les autres organisations qui pourraient être touchées par ce devoir additionnel de notification, on trouve les agences gouvernementales responsables de la délivrance de documents d'identification, les compagnies d'assurances, les partenaires d'affaires de l'organisation victime de l'atteinte, les banques et d'autres institutions financières[15]. Le Groupe de travail recommande d'inclure une disposition à cet effet dans la Loi uniforme.

[23] La loi de l'Alberta et le projet de loi du gouvernement fédéral comptent sur la réglementation et même aux lignes directrices des responsables de la vie privée pour compléter les détails du régime. Le contenu de l'avis qui doit être envoyé aux personnes intéressées en est un exemple, même si le texte du projet de loi en précise la règle de base, soit que l'avis doit contenir « suffisamment d'information pour permettre à l'intéressé de comprendre l'importance qu'a pour lui l'atteinte et de prendre, si cela est possible, des mesures pour réduire le risque de préjudice qui pourrait en résulter ou pour atténuer un tel préjudice, de même que tout autre renseignement réglementaire. »[16] Les cas où l'avis peut être donné de façon indirecte plutôt que directement à la personne sont laissés entièrement aux règlements.[17]. La CHLC n'a pas l'habitude de rédiger des règlements, peut-être parce que la plupart des lois uniformes établissent des règles de droit plutôt que des mécanismes qui doivent être administrés. La position du Groupe de travail est qu'il est acceptable dans le cas des règles de notification des atteintes à la protection des données de laisser la question des détails aux responsables des règlements, parce que les autorités de protection de la vie privée du pays ont l'habitude de collaborer ensemble à l'élaboration des normes et des pratiques. Ainsi, il y a bien des chances que ces questions soient abordées de façon uniforme. La Loi uniforme présente l'essentiel du contenu de l'avis dans une description assez détaillée du pouvoir de réglementation.

[24] Une différence notable entre les dispositions de la loi albertaine et du projet de loi fédéral est que la première prévoit des pénalités pour avoir omis d'aviser le responsable de la vie privée comme il se doit, tandis que le projet de loi C-29 ne contient aucune pénalité. Dans le commentaire joint au modèle de loi de 2008 d'Industrie Canada, on expliquait que, dans les faits, la commissaire à la protection de la vie privée n'avait pas de difficulté à faire appliquer ses recommandations par les entreprises. Dans les cas extrêmes, elle pouvait aller devant les tribunaux pour obtenir une ordonnance, mais cela ne s'était pas avéré nécessaire. On ne ressentait donc pas le besoin d'un régime plus sévère. Le Groupe de travail recommande que les dispositions prévoyant des pénalités soient maintenues dans la Loi uniforme, sous une forme semblable à celle de l'ébauche de la Loi uniforme de 2009.

[25] La loi albertaine prévoit une défense de diligence raisonnable en cas de poursuite pour contravention. Voici le texte du paragraphe 59(4) : « [traduction] Une organisation ou une personne ne sont pas coupables d'une infraction aux termes de la présente loi s'il est établi à la satisfaction du tribunal que l'organisation ou la personne, selon le cas, a agi de façon raisonnable dans les circonstances qui ont conduit

à l'infraction ». Plusieurs avocats du secteur privé qui ont commenté la version provisoire de 2009 de la Loi uniforme ont exprimé des préoccupations quant à la possibilité d'imposer des pénalités importantes pour des violations techniques de règles sujettes à une interprétation assez libre de ce qui seraient, dans les premières années, des obligations bien nouvelles. Il serait possible d'assujettir les pénalités à un critère traditionnel de *mens rea* pour les contraventions des exigences de forme ou de contenu des avis qui ne demandent pas d'évaluation, tout en permettant une défense de diligence raisonnable (ou de conduite raisonnable) pour les accusations de contravention qui impliquent un manquement au jugement sur l'importance d'une atteinte, la réalite d'un risque ou la gravité d'un préjudice. La loi uniforme proposée reflète cette distinction entre deux types d'infraction. La réunion voudrait bien réfléchir si la distinction ajoute trop de complexité à la loi..

[26] Dans le rapport de 2009 présenté à la CHLC, on soulevait la question de savoir si les poursuites et les pénalités étaient logiques lorsque les règles de notification d'une atteinte à la protection des données personnelles s'appliquaient au secteur public. Le ministère public devrait-il poursuivre l'État? La loi devrait-elle encourager le transfert de fonds d'une poche à l'autre de l'appareil étatique? Le risque de publicité et d'opprobre ne serait-il pas suffisant pour garantir la conformité à la loi? Par contre, le fait de proposer une loi exposant d'une part les sociétés privées à d'importantes pénalités et d'autre part les organismes publics à une seule sanction morale pourrait être perçu comme étant inapproprié. Qui plus est, les organismes publics ont des formats bien différents, des ministères aux sociétés d'État, en passant par toute une gamme d'agences, de conseils et de commissions. Ce qui est bon pour l'un ne l'est pas forcément pour tous. En conséquence, le Groupe de travail recommande de ne pas adopter de clause précise au sujet des pénalités imposées à des organismes publics. Les autorités législatives peuvent choisir d'alléger les dispositions pour certains ou tous les organismes publics selon leur préférence.

[27] En 2008, et de nouveau en 2009, la CHLC a décidé que la Loi uniforme ne devait pas prévoir de recours civils pour quelque type d'atteinte à la protection des données que ce soit. Cette politique a été conservée dans la version actuelle de l'ébauche de loi. Par conséquent, elle ne prévoit pas de disposition particulière pour les rapports de solvabilité obligatoires ou à coût modique, quoique le Groupe de travail ne prend pas position à savoir si une telle règle serait pertinente dans le domaine de compétence d'autres personnes, comme les ministres de la protection des consommateurs.

[28] De la même façon, la Loi uniforme ne prévoit pas de dommages-intérêts légaux pour l'atteinte à la protection des données ou pour ne pas avoir avisé alors que la loi le prescrivait. Elle note tout simplement que la possibilité d'un recours civil – pour l'atteinte à la sécurité ou pour l'absence de notification - n'est pas exclue par cette loi. Il est reconnu que l'absence de dommages-intérêts légaux peut rendre difficile l'obtention d'une compensation de la part de la personne qui avait le contrôle de l'information pour les personnes dont l'information personnelle a été compromise sans qu'elles en aient été avisées. À ce chapitre, l'expérience américaine montre que la plupart des poursuites de ce genre ont échoué, la plupart du temps à cause d'un manque de preuves des dommages allégués[18]. Il est possible que l'incapacité répétée à prouver les dommages dans de tels cas repose en grande partie sur l'absence de dommage réel. On peut soutenir que la loi ne devrait pas prévoir ce que l'expérience ne justifie pas. Cette conclusion s'impose avec d'autant plus de force lorsque l'on considère les dommages causés par la non-notification plutôt que par l'atteinte initiale, qui pourrait ou non être le résultat d'un non-respect de l'obligation de s'assurer de façon raisonnable que l'information personnelle est protégée.

[29] Une sanction moins officielle, mais potentiellement efficace en cas d'atteinte et de non-notification d'une atteinte, est la divulgation par le responsable de la vie privée de l'incident et de l'identité de l'organisme ayant le contrôle de l'information visée. Pour l'organisation en cause, une telle divulgation est une motivation en soi d'être la première à communiquer avec les personnes touchées. De plus, la divulgation rejoint le même objectif que la notification, soit d'informer les personnes intéressées qu'elles peuvent courir un risque. Certes, dans ce rôle, elle est moins efficace qu'un avis envoyé à chaque personne, mais c'est mieux que rien. Les lois de protection de la vie privée de chaque province permettent peut-être déjà à l'autorité de protection de la vie privée de faire une telle divulgation, mais le Groupe de travail recommande qu'une disposition de référence soit enchâssée dans la Loi uniforme pour s'assurer que toutes les lois applicables contiennent une disposition de ce genre.

[30] Voici les principaux changements apportés à l'ébauche de la loi de 2009 qui n'ont pas déjà été présentés :

- Art. 100 : la définition de « détenteur » est superflue. La nouvelle version emploie les formulations communes aux lois canadiennes de protection de la vie privée s'appliquant aux organismes qui contrôlent

les renseignements personnels. Un organisme s'entend de personnes naturelles, suivant l'exemple de la loi de l'Alberta, si elles agissent dans un rôle professionnel, commercial ou public et non pas purement personnel.

- Art. 101 : on se référera aux modèles de la loi de l'Alberta et du projet de loi fédéral pour les critères liés à l'atteinte à la protection des données et à la notification. Ces dispositions se trouvent maintenant aux articles 102 et 103.
- Art. 102 : les rapports envoyés au responsable de la vie privée auront les mêmes incidents que ceux proposés dans le projet de loi fédéral et il n'est pas nécessaire d'intégrer leur contenu en détail dans la loi.
- Art. 103 : le responsable de la vie privée devrait sans doute disposer du pouvoir de demander un supplément d'information et d'exiger ou de recommander certains types de mesures sans qu'il s'agisse nécessairement d'une notification, (p. ex., il pourrait demander un suivi de la situation plutôt qu'une notification ou en attendant la notification). Cette disposition est maintenant à l'article 105.
- Art. 104 : on devrait laisser les relations avec la police au bon sens ou à d'autres lois. La réunion de 2009 ne voulait pas donner à la police la décision si ou quand la notification aurait lieu.
- Art. 105 : le pouvoir de réglementation devrait être élargi pour couvrir d'autres sujets, à la manière de la loi fédérale. Cette disposition est maintenant à l'article 109.
- Art. 106 : le montant indiqué à la disposition relative aux infractions varie selon que l'accusé est une personne naturelle ou une autre entité. La loi proposée fait une distinction entre les infractions pour lesquelles la prudence est une défense – là où le jugement peut être difficile - et celles pour lesquelles il est plus simple de se conformer aux dispositions de la loi. La responsabilité des administrateurs sera conservée. Ces dispositions sont maintenant à l'article 107.

Conclusion

[31] Certaines provinces choisiront peut-être d'appliquer la Loi uniforme au secteur public seulement, confiant à la LPRPDE le soin de répondre aux questions de protection de la vie privée liées à leur secteur privé. La Loi uniforme a été rédigée en tenant compte de cette possibilité.

[32] Le commissaire de l'Alberta a déclaré que le critère de « risque réel de préjudice grave » constituait « la norme nationale »[19]. Comme cette norme se rapproche du principe approuvé en 2008 [20]et

répond aux critiques exprimées à l'égard du principe fédéral de 2008[21], il est logique pour la CHLC de l'adopter à son tour. Le Groupe de travail est d'avis que l'ébauche de Loi uniforme peut être adoptée par les autorités législatives et qu'elle s'harmonise bien avec les meilleures lois, y compris avec les seules dans la matière qui ont une application générale.[22]

LOI MODIFIANT LA LOI SUR LA PROTECTION DE LA VIE PRIVÉE (NOTIFICATION DES ATTEINTES À LA PROTECTION DES DONNÉES)

REMARQUE :
Le présent texte est rédigé sous forme de projet de loi modificatif qui ajoute une partie sur la notification des atteintes à la protection des données à la loi ou aux lois de l'autorité législative qui portent sur la protection de la vie privée. Par exemple, en Ontario, la partie proposée pourrait être intégrée, avec les adaptations appropriées, à la Loi sur l'accès à l'information et la protection de la vie privée, à la Loi sur l'accès à l'information municipale et la protection de la vie privée et à la Loi de 2004 sur la protection des renseignements personnels sur la santé. Afin de faciliter la consultation, la partie proposée est désignée «partie X» et commence à l'article 100.

On suppose que les Lois auxquelles la partie proposée pourrait être intégrée comprennent déjà une définition de «renseignements personnels» ou de termes semblables, comme «renseignements personnels sur la santé», aux fins de la protection de la vie privée. Par conséquent, la partie proposée utilise le terme «renseignements personnels» sans en donner d'autre définition.

De plus, on suppose que les lois auxquelles la partie proposée pourrait être intégrée prévoient la nomination d'un organisme ou d'un fonctionnaire (tel qu'un commissaire à la protection de la vie privée ou un ombudsman) qui est investi d'importantes responsabilités consistant à faire respecter les dispositions de la Loi portant sur la protection de la vie privée. Tel qu'il est utilisé dans la partie proposée, le terme «autorité de protection de la vie privée» s'entend de l'organisme ou du fonctionnaire

investi de cette responsabilité dans chaque province ou territoire. Il n'est pas défini dans la partie proposée étant donné que l'on suppose qu'un terme équivalent est défini ou précisé d'une autre façon dans la loi existante.

On suppose également qu'une loi (ou une partie d'une loi) à laquelle la partie proposée pourrait être intégrée précise quels sont les détenteurs de renseignements personnels auxquels s'applique cette loi (ou la partie de cette loi). Dans certains cas, l'application sera limitée aux organisations à caractère public. Dans d'autres cas, l'application sera plus générale. Le terme générique «organisation» est défini de façon large dans la partie proposée, mais ce terme et son sens seront différents selon la province ou le territoire, compte tenu de la terminologie et de la portée de la loi existante.

Pour terminer, on suppose que la loi existante impose au détenteur de renseignements personnels l'obligation de les protéger.

1. La Loi est modifiée par adjonction de la partie suivante :

PARTIE X
NOTIFICATION DES ATTEINTES À LA PROTECTION DES DONNÉES

Définitions

100. Les définitions qui suivent s'appliquent à la présente partie.

«organisation» S'entend des personnes morales, sociétés de personnes, associations, syndicats ou autres entités et des particuliers agissant dans le cadre d'une activité professionnelle, commerciale ou publique, mais non à titre personnel. («organization»)

Commentaire: L'autorité adoptante emploie le mot qui convient à sa loi cadre.

NOTE DE RÉDACTION: La loi proposée suit l'exemple de l'Alberta en comprenant la personne naturelle dans la définition d'organisation. Elle ajoute une référence aux activités professionnelles et publiques pour inclure les personnes du secteur public.

«préjudice» S'entend notamment de la lésion corporelle, de l'humiliation, du dommage à la réputation, du dommage aux relations, de la perte de possibilités d'emploi ou d'occasions d'affaires ou d'activités professionnelles, de l'effet négatif sur le dossier de crédit, du dommage aux biens ou de leur perte, de la perte financière et du vol d'identité. («harm»)

«prescrit» Prescrit par règlement pris en vertu de la présente loi. («prescribed»)

Atteinte à la vie privée

101. Pour l'application de la présente partie, une atteinte à la vie privée se produit à l'égard de renseignements personnels dans les cas suivants :

a)les renseignements sont consultés alors que la présente loi n'autorise pas la consultation;

b)les renseignements sont divulgués alors que la présente loi n'autorise pas la divulgation;

c)les renseignements sont perdus et la perte peut occasionner leur consultation ou divulgation sans autorisation prévue par la présente loi.

Déclaration obligatoire de l'organisation à l'autorité de protection de la vie privée

102. (1) L'organisation qui a connaissance ou a des raisons de croire qu'une atteinte à la vie privée est survenue à l'égard de renseignements personnels dont elle a la gestion est tenue de déclarer l'atteinte à l'autorité de protection de la vie privée, conformément au présent article, si l'atteinte est importante.

NOTE DE RÉDACTION: Le réunion voudrait bien réfléchir la question si l'expression « renseignements … dont elle a la gestion » devrait comprendre aussi « dont elle a la garde », comme c'est le cas dans

plusieurs lois canadiennes sur la protection de la vie privée. Les tiers fournisseurs de service auraient la garde mais non la gestion de renseignements personnels. Leur devoir au cas d'une atteinte à la sécurité serait d'en aviser le client qui en a gestion des renseignements.

Atteinte importante à la vie privée : facteurs

(2) Les facteurs servant à établir si une atteinte à la vie privée à l'égard de renseignements personnels dont une organisation a la gestion est importante comprennent :

a)le degré de sensibilité des renseignements personnels;

b)le nombre de particuliers dont les renseignements personnels ont été touchés par l'atteinte;

c)la probabilité qu'un préjudice sera causé aux particuliers dont les renseignements personnels étaient en cause;

d)l'évaluation faite par l'organisation selon laquelle la cause de l'atteinte est un problème d'ordre systémique.

NOTE DE RÉDACTION: L'obligation de déclarer une atteinte au responsable de protection de la vie privée provient du projet de loi fédéral C-29. Ce projet de loi ne mentionne pas la probabilité de préjudice parmi les critères pour la déclaration. L'on omet ce critère probablement parce que la déclaration vise une analyse de la sécurité des systèmes et la façon de gérer les renseignements et non pas l'impact de l'atteinte sur les individus. Les intérêts de ceux-ci sont protégés par le devoir de les notifier si le risque atteint le seuil légal. Est-ce que la loi uniforme devrait ajouter ce critère à la liste fédérale?

Délai de remise de la déclaration

(3) La déclaration exigée par le paragraphe (1) doit être faite dès qu'il est raisonnablement possible de le faire une fois que l'organisation a connaissance ou a des raisons de croire qu'il y a eu atteinte à la vie privée et qu'elle établit que celle-ci est importante.

Contenu de la déclaration

(4) La déclaration exigée par le paragraphe (1) doit décrire les mesures prises par l'organisation pour se conformer à l'article 103 et contenir les autres renseignements prescrits.

Modalités de la déclaration

(5) La déclaration exigée par le paragraphe (1) doit être faite selon la forme et la manière prescrites.

Obligation pour l'organisation d'aviser le particulier

103. (1) L'organisation qui a connaissance ou a des raisons de croire qu'une atteinte à la vie privée est survenue à l'égard des renseignements personnels concernant un particulier dont l'organisation a la gestion est tenue d'en aviser le particulier conformément au présent article s'il est raisonnable de croire, dans les circonstances, que l'atteinte à la vie privée présente un risque réel de préjudice grave à son endroit.

Risque réel de préjudice grave : facteurs

(2) Les facteurs servant à établir si une atteinte à la vie privée à l'égard des renseignements personnels concernant un particulier présente un risque réel de préjudice grave à son endroit comprennent :

a)le degré de sensibilité des renseignements personnels;

b)la probabilité que les renseignements ont fait l'objet ou sont en train ou sur le point de faire l'objet d'une utilisation abusive.

Délai de remise de l'avis

(3) L'avis exigé par le paragraphe (1) doit être donné dès qu'il est raisonnablement possible de le faire une fois que l'organisation a connaissance ou a des raisons de croire qu'il y a eu atteinte à la vie privée et qu'elle établit que celle-ci présente un risque réel de préjudice grave à l'endroit du particulier.

NOTIFICATION DES ATTEINTES À LA PROTECTION DES DONNÉES

Contenu de l'avis

(4) L'avis exigé par le paragraphe (1) doit contenir les renseignements suivants :

a)suffisamment d'information pour permettre au particulier :

(i)de comprendre l'importance, pour lui, de l'atteinte à la vie privée,

(ii)de prendre les mesures qui sont possibles pour réduire le risque de préjudice pour lui qui pourrait résulter de l'atteinte à la vie privée ou pour atténuer un tel préjudice;

b)tout autre renseignement prescrit.

Modalités de l'avis

(5) L'avis exigé par le paragraphe (1) :

a)doit être bien en vue;

b)doit être donné au particulier directement, sous réserve du paragraphe (6);

c)doit être donné selon la forme et la manière prescrites.

NOTE DE RÉDACTION: L'expression « bien en vue » paraît dans le projet de loi C-29. Est-ce la bonne expression? Est-ce qu'elle est nécessaire quand le gouvernement peut prendre un règlement sur la forme et la manière de la notification?

Exception

(6) S'il est prescrit des circonstances dans lesquelles l'avis ne peut pas être donné au particulier directement, l'avis doit, dans ces circonstances, lui être donné indirectement.

Obligation pour l'organisation d'aviser des tiers

104. L'organisation qui, conformément à l'article 103, avise un particulier d'une atteinte à la vie privée est également tenue d'en aviser en même temps toute institution gouvernementale ou subdivision d'une telle institution ou toute autre organisation si, selon le cas :

a)l'institution ou subdivision ou l'autre organisation peut être en mesure de réduire le risque de préjudice pour le particulier qui pourrait résulter de l'atteinte à la vie privée ou d'atténuer un tel préjudice;

b)il est satisfait à une condition prescrite.

Ordre de l'autorité de protection de la vie privée

105. (1) Si une autorité de protection de la vie privée reçoit une déclaration visée à l'article 102 au sujet d'une atteinte à la vie privée à l'égard de renseignements personnels dont une organisation a la gestion et qu'elle décide que l'atteinte à la vie privée présente un risque réel qu'un préjudice grave soit causé à un ou plusieurs particuliers auxquels se rapportent les renseignements, l'autorité peut ordonner à l'organisation de faire ce qui suit *[recommander à l'organisation de faire ce qui suit]* :

a)prendre les mesures qu'elle précise relativement à l'avis à remettre aux particuliers au sujet de l'atteinte à la vie privée si elle est d'avis que les mesures prises par l'organisation pour se conformer à l'article 103 ne sont pas suffisantes;

b)prendre les mesures qu'elle précise pour limiter les conséquences de l'atteinte à la vie privée;

c)prendre les mesures qu'elle précise pour empêcher que ne se reproduise une atteinte à la vie privée à l'égard de renseignements personnels dont l'organisation a la gestion, notamment :

(i)modifier ou limiter les catégories de personnel autorisé à consulter ou à divulguer des renseignements personnels,

(ii)modifier les règles ou la procédure à suivre pour consulter ou divulguer des renseignements personnels,

(iii)appliquer ou renforcer les mesures de sécurité au sein de l'organisation.

Commentaire : Si une autorité de protection de la vie privée dans une province ou un territoire n'a pas le pouvoir de donner des ordres, le présent article l'habiliterait à ne faire qu'une recommandation, auquel cas le paragraphe (2) serait supprimé ou modifié.

NOTE DE RÉDACTION: Est-ce la liste d'actions dans la clause (c) trop exigeante ou trop précise? Est-ce que l'action prévue par l'alinéa (c)(iii) serait suffisante? Devrait-on prèvoir un délai acceptable pour se conformer aux directions?

Obligation de se conformer et de faire rapport

(2) L'organisation à laquelle l'autorité de protection de la vie privée a donné un ordre en vertu du paragraphe (1) prend les mesures précisées dans l'ordre dans les délais qui y sont précisés et remet à l'autorité des rapports sur sa conformité à l'ordre dans les délais qui y sont précisés.

Divulgation par l'autorité de protection de la vie privée

106. Si une autorité de protection de la vie privée qui reçoit une déclaration visée à l'article 102 au sujet d'une atteinte à la vie privée à l'égard de renseignements personnels dont une organisation a la gestion et qu'elle décide que l'atteinte à la vie privée présente un risque réel qu'un préjudice grave soit causé à un ou plusieurs particuliers auxquels se rapportent les renseignements, l'autorité peut, malgré l'article X *[insérer l'article de la Loi qui interdit la divulgation par l'autorité de protection de la vie privée]* :

a)divulguer l'atteinte aux particuliers de la manière qu'elle estime appropriée, si elle a donné à l'organisation un ordre visé à l'alinéa 105 (1) a) et que cette dernière n'a pas pris les mesures précisées dans l'ordre dans les délais qui y sont précisés;

b)divulguer l'atteinte au public de la manière qu'elle estime appropriée, si elle est d'avis que la divulgation est dans l'intérêt public.

Commentaire: Le pouvoir du responsable de la protection de la vie privée de divulguer une atteinte constitue une protection importante pour les personnes affectées. Si une disposition de la loi cadre met en doute la capacité du responsable d'effectuer une telle divulgation, cette disposition devrait être replacée par le présent article. Sans une prohibition de la divulgation, la permission de la présent disposition va sans dire; il ne serait pas nécessaire de l'inclure l'article dans la loi de mise en oeuvre de la loi uniforme.

Infractions

107. (1) Est coupable d'une infraction l'organisation qui contrevient à l'article 102, 103 ou 104 ou au paragraphe 105 (2).

Employés et mandataires

(2) Dans la poursuite d'une organisation intentée pour une infraction prévue au présent article, tout acte ou toute omission d'un employé ou d'un mandataire de l'organisation qui agissait dans le cadre de son emploi ou de son mandat est réputé l'acte ou l'omission de l'organisation, que l'employé ou le mandataire ait été ou non identifié ou poursuivi pour cette infraction.

Particuliers qui dirigent la gestion des affaires de l'organisation

(3) Si l'organisation qui commet une infraction prévue au présent article n'est pas un particulier, chacun des particuliers qui dirigeaient la gestion des affaires de l'organisation au moment où celle-ci a commis l'infraction est également coupable de l'infraction s'il n'a pas fait preuve de diligence raisonnable pour empêcher l'organisation de la commettre, que l'organisation ait été poursuivie ou non pour cette infraction.

Fardeau de la preuve

(4) Au cours de son procès, il incombe au particulier visé au paragraphe (3) de prouver qu'il a fait preuve de diligence raisonnable pour empêcher l'organisation de commettre l'infraction.

Défense

(5) Aucun particulier ni aucune entité ne doit être déclaré coupable d'une infraction prévue au présent article si le particulier ou l'entité établit qu'il ou elle a agi raisonnablement dans les circonstances qui ont donné lieu à l'infraction.

NOTE DE RÉDACTION: Cette atténuation de la responsabilité du défendeur se trouve dans la loi de l'Alberta. Devrait-on exiger plus de diligence que la simple conduite raisonnable?

Puisque la défense d'action raisonnable incombe au défendeur en vertu du paragraphe (5), est-ce qu'il est nécessaire de prévoir le fardeau de la preuve au paragraphe (4)?

Exception

(6) Le paragraphe (5) ne s'applique pas à une contravention au paragraphe 102 (4) ou (5), 103 (4), (5) ou (6), à l'alinéa 104 b) ou au paragraphe 105 (2).

NOTE DE RÉDACTION: Ces exceptions se rapportent à des obligations claires imposées par la loi. Il ne s'agit pas ici d'évaluation difficile ni d'incertitude quant aux faits. Il n'est pas évident que le défendeur puisse ne pas se conformer à ces devoirs en alléguant que sa conduite était raisonnable. Par contre la mise à exécution des obligations pourrait devenir trop compliquée si on devra analyser la qualité de la diligence de l'activité du défendeur en vertu de chaque paragraphe de la loi. .

Peine

(7) Tout particulier qui est coupable d'une infraction prévue au présent article est passible, sur déclaration de culpabilité, d'une amende maximale de 100 000 $ et toute entité qui est coupable d'une infraction prévue au présent article est passible, sur déclaration de culpabilité, d'une amende maximale de 500 000 $.

Prescription

(8) Est irrecevable toute poursuite intentée pour une infraction prévue au présent article plus de deux ans après la date à laquelle l'infraction a été ou aurait été commise.

Commentaire: : L'autorité législative a deux options : soit qu'elle choisisse un délai de prescription déterminé et prenne des mesures pour éviter l'incompatibilité avec d'autres lois qui prévoient un délai de prescription différent, soit qu'elle choisisse d'appliquer à cette infraction le délai de prescription qui s'applique aux autres infractions sous le régime de la loi existante, auquel cas la présente disposition n'est peut-être pas nécessaire.

Aucune incidence sur les recours civils

108. La présente partie n'a pas pour effet de porter atteinte à la responsabilité d'une organisation dans le cadre d'une instance civile introduite contre elle relativement :

a)soit à une atteinte à la vie privée qui s'est produite à l'égard de renseignements personnels dont l'organisation a la gestion;

b)soit à un acte ou à une omission de l'organisation qui constitue une contravention à la présente partie.

NOTE DE RÉDACTION: Est-que les règles sur la notification en cas d'atteinte devraient constituer un code intégral sur la responsabilité, auquel cas la loi uniforme devrait interdire l'action civile pour les préjudices causés par la non-conformité? On mentionne le droit à l'action civile à la clause (a) pour donner une vue d'ensemble et pour être certain de la règle. Une loi sur la notification d'une atteinte ne devrait pas limiter la responsabilité civile pour l'atteinte elle-même.

Règlements

109. (1) Le lieutenant-gouverneur en conseil peut, par règlement :

a)régir le contenu de la déclaration exigée par le paragraphe 102 (1);

b)régir le contenu de l'avis exigé par le paragraphe 103 (1);

c)prescrire tout ce qui est mentionné dans la présente partie comme étant prescrit ou tout ce que la présente partie exige ou permet de faire conformément aux règlements ou comme le prévoient ceux-ci et pour lequel un pouvoir précis n'est pas par ailleurs prévu à la présente partie.

Contenu de l'avis

(2) Tout règlement visé à l'alinéa (1) b) peut exiger que l'avis décrive :

a)l'étendue des renseignements personnels en cause;

b)le genre de renseignements personnels en cause;

c)la nature et les circonstances de l'atteinte à la vie privée;

d)les mesures que l'organisation a prises, le cas échéant, pour limiter les conséquences de l'atteinte à la vie privée;

e)les mesures que l'organisation a prises, le cas échéant, pour empêcher que ne se reproduise une atteinte à la vie privée à l'égard de renseignements personnels dont elle a la gestion;

f)les plans que l'organisation a formés, le cas échéant, en vue de prendre les mesures du genre visé aux alinéas d) et e);

g)les mesures que les particuliers qui ont reçu un avis pourraient prendre, le cas échéant, pour réduire le risque de préjudice pour eux qui pourrait résulter de l'atteinte à la vie privée ou pour atténuer un tel préjudice.

---

1 *Loi de 2004 sur la protection des renseignements personnels sur la santé*, L.O. 2004, c. 3, art. 12.

2 La *Personal Information Protection Act*, S.A. 2003, c. P-6.5 de l'Alberta a été amendée en octobre 2009 par la *Personal Information Protection Amendment Act, 2009*. S.A. 2009, c. 50, art. 25. Les dispositions relatives à la notification des atteintes à la protection des données sont entrées en vigueur le 1er mai 2010. Terre-Neuve-et-Labrador a adopté sa *Personal Health Information Act*, SNL 2008, c. P-7.1, art. 15, entrée en vigueur le 1er juin 2010. Le Nouveau-Brunswick a emboîté le pas avec sa *Loi sur l'Accès et la protection en matière de renseignements personnels sur la santé*, L.N.-B. 2009, c. P-7.05, art. 49, qui n'est pas encore entrée en vigueur. Le projet de loi C-29 du gouvernement fédéral, intitulé *Loi protégeant les renseignements personnels des Canadiens*, a

été adopté en première lecture le 25 mai 2010, art. 11, créant un nouvel art. 10.1 à la *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, c. 5.

[3] *Personal Information Protection Act*, projet de loi 64, première lecture le 4 novembre 2009, art. 72-73 : http://www.gov.ns.ca/legislature/legc//bills/61st_1st/1st_read/b064.htm.

[4] Industrie Canada, *A Model for Data Breach Notification Reporting and Notification under the Personal Information Protection and Electronic Documents Act*, juin 2008.

[5] « Aperçu préalable de la LPRPDE 2.0, Commentaires à l'occasion de la Conférence juridique canadienne et exposition de l'Association du Barreau canadien (ABC) », http://www.priv.gc.ca/speech/2008/sp-d_080819_f.cfm, 19 août 2008.

[6] Ontario, Office of the Chief Information and Privacy Officer, "Taking the Right Steps – A Guide to Managing Privacy and Privacy Breaches" April 18, 2007.

[7] Rapport de 2009, paragraphes 13-14.

[8] M. Geist, « C-29: The Anti-Privacy Privacy Bill », http://www.michaelgeist.ca/content/view/5059/125, 26 mai 2010.

[9] Un tel devoir distinct figurait dans la version provisoire de 2009 au paragraphe 101(3) et à l'article 102 (où l'on en trouvait le détail).

[10] Rapport de 2009, paragraphe 11.

[11] Projet de loi C-29, art. 11, nouvelle version de la LPRPDE, para. 10.2(2).

[12] *Ibid.*, nouvelle version de la LPRPDE, para. 10.2(3).

[13] *Ibid.*, nouvelle version de la LPRPDE, para. 10.1(2).

[14] *Ibid.*, nouvelle version de la LPRPDE, para. 10.3(1).

[15] Cette liste est tirée de l'étude d'Industrie Canada, article 2.3, citée à la note 4 du présent rapport.

[16] Nouvelle version de la LPRPDE, para. 10.2(4). La loi de l'Alberta prévoit la notification au commissaire, mais le contenu de la notification est du ressort des règlements. Loi de l'Alberta, para. 34.1(2).

[17] Nouvelle version de la LPRPDE, art. 10.2(6).

[18] Voir le rapport de 2008, paragraphe [45].

[19] Lors d'une réunion qui a eu lieu à Toronto le 18 juin 2010.

[20] « un risque que l'atteinte cause un préjudice important » (rapport de 2008 au paragraphe 29)

[21] « un risque substantiel de préjudice grave » (législation modèle d'Industrie Canada, voir la note 4 ci-haut)

[22] Les autres lois canadiennes pertinentes ne touchent que les renseignements ayant rapport avec la sante. Le groupe de travail n'estime pas que ces renseignements méritent un traitement différent.