CONFÉRENCE POUR L'HARMONISATION DES LOIS AU CANADA

SECTION CIVILE

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

RAPPORT INTÉRIMAIRE POUR 2009

Groupe de travail sur le vol d'identité

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

Ottawa Ontario
Du 9 au 13 août 2009

CONFÉRENCE POUR L'HARMONISATION DES LOIS AU CANADA

RAPPORT INTÉRIMAIRE POUR 2009

[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 concernées de tout événement pouvant compromettre la sécurité de ces données. La Loi uniforme devait suivre les recommandations du rapport présenté par le groupe de travail à cette réunion.[1]

[2] Le groupe s'est reconstitué à cause du caractère principalement civil du projet. Ses membres en 2008-2009 étaient :

- Arghavan Gerami, ministère de la Justice du Canada
- John D. Gregory, ministère du Procureur général de l'Ontario (président)
- Josh Hawkes, Alberta Justice
- Wilma Hovius, ministère de la Justice du Canada
- Heather J. Innes, Alberta Justice
- Gail Mildren, Justice Manitoba
- Jeanne Proulx, ministère de la Justice du Québec

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

[3] Le groupe de travail a fait des progrès considérables dans son analyse des enjeux et de la rédaction d'une loi sur la notification des atteintes à la protection des données, mais il n'a pas abouti à un texte à recommander à la Conférence comme Loi uniforme. L'ébauche de travail est annexée à ce rapport. Elle présente un bon nombre de questions sur lesquelles le groupe sollicite une orientation de la part de la réunion. Certaines questions nous invitent à examiner les recommandations de 2008 à la lumière des discussions plus approfondies du groupe de travail.

[4] Il importe de noter dès le début qu'une loi sur la notification des atteintes à la sécurité des données n'est qu'une partie de l'oeuvre de protection des données personnelles. En fait, la protection des données personnelles se situerait dans le cadre

plus large encore de la protection de données de toute sorte contre l'abus.[2] 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 l'an dernier, 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 ces données recueillies par secteur privé (quoique la loi fédérale ait une application large dans ce cas). Une catégorie importante de données personnelles, celle des renseignements qui traitent de la santé, se voit attribuer sa propre loi dans plusieurs provinces. Le responsable de l'exécution du régime peut être un commissaire qui détient des pouvoirs d'investigation et d'ordonnance ou bien un ombudsman qui a le pouvoir de lancer des investigations, mais qui n'a recours qu'à la persuasion et à la recommandation.

[6] Le groupe de travail a tenté de préparer une loi uniforme sur la notification des atteintes à la sécurité qui puisse s’adapter à ce contexte varié. L'uniformité est importante parce que des données sur une personne peuvent être détenues ou bien communiquées d'un bout à l’autre du pays, et que les détenteurs de données personnelles peuvent bien en détenir sur des personnes habitant des territoires différents. 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 en question savent à quoi s'attendre.

[7] L'ébauche de travail 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 – la définition des données personnelles auxquelles la Loi uniforme s'applique – et pour son application – l'autorité responsable de celle-ci.

[8] En bref, l'ébauche de la Loi uniforme s'applique au moment où le détenteur de données personnelles a des motifs de croire que l'information a été consultée ou divulguée contrairement à ce qu'autorise la loi sur la protection de la vie privée dont ces règles font partie. Si la consultation ou la divulgation non autorisée présente un risque de préjudice important pour les personnes auxquelles se rapportent les renseignements, le détenteur doit les aviser promptement de l'atteinte à la sécurité. De toute façon, le détenteur doit notifier l'autorité compétente, que l'ébauche de la Loi uniforme appelle le commissaire. Le contenu de cet avis est précisé en détail. Le commissaire peut obliger le détenteur de données personnelles à notifier les personnes intéressées si ce n'est pas encore fait, et aussi de notifier la police. La police peut retarder la notification aux fins de ses enquêtes. 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] Le groupe de travail souhaite attirer l'attention de la réunion sur les considérations suivantes.

[10] Bien que l'ébauche de Loi uniforme et la plupart des lois américaines qui l'ont inspirée traitent du « détenteur » des données personnelles, la majorité des lois canadiennes sur la protection de la vie privée s'appliquent aux entités qui ont la possession ou le contrôle de telles données. La possession et le contrôle – surtout le contrôle – sont des idées plus larges que la détention de l'information. Le groupe de travail a pesé le pour et le contre de deux scénarios en particulier : (i) quelqu'un recueille et détient des données personnelles pour le compte de quelqu'un d'autre (il pourrait s'agir d'un ministère qui s'en charge pour un autre) ; (ii) le principal responsable de la collecte ou de l'emploi de telles données passe un contrat avec une autre personne pour le stockage ou la gestion de l'information. De tels cas justifient-ils l'usage du mot « détenteur » ?

[11] Pour répondre à ces préoccupations, l'ébauche de Loi offre l'article 100, qui prévoit que les données personnelles sont détenues par une entité si elle est responsable de leur emploi, de leur garde ou de leur divulgation. Cette disposition vise à faire en

sorte qu'une personne n'échappe pas à sa responsabilité de donner notification d'une atteinte à la sécurité en prétendant que la gestion des données a été confiée à un tiers. Que ce tiers soit également assujetti à la Loi est peut-être moins évident. En principe, on devrait recevoir un seul avis par atteinte à la sécurité ; la Loi ne devrait donc pas obliger de multiples entités à en donner un. Cependant l'entité qui détient les données est peut-être la mieux placée pour savoir que la sécurité a été compromise. La Loi uniforme devrait-elle énoncer avec plus de détail que ne le fait l'ébauche les devoirs respectifs des entités tenues de protéger les données personnelles et de leurs fournisseurs de service de gestion des données ?

[12] L'ébauche de la Loi uniforme crée des obligations si des données personnelles ont été consultées ou divulguées contrairement à ce qu'autorise la Loi (dont les règles sur la notification font partie). Ce critère est-il assez clair ? Les obligations s'appliquent également si le détenteur « a des motifs de croire » que les renseignements ont été consultés ou divulgués d'une telle manière. Il n'est pas nécessaire d'en être certain. Le groupe de travail a débattu la possibilité d'appliquer des règles différentes aux cas où on sait qu'il y a eu atteinte et aux cas où on n'a qu'un « motif de croire » à une atteinte éventuelle. Le groupe a décidé que le but de la notification était de gérer le risque, et le risque est présent même sans certitude.

[13] Les directives issues de la réunion de 2008 étaient que le détenteur devrait notifier le commissaire de toutes les atteintes ou les possibilités d'atteinte, et que le commissaire déciderait du besoin de notifier les personnes concernées. Le groupe de travail a préféré éliminer l'intermédiaire et réduire les retards dans les cas clairs en imposant aux détenteurs des données l'obligation principale de donner notification. Si l'atteinte à la sécurité présente un risque de préjudice important (le critère adopté par la Conférence en 2008), le détenteur doit notifier les personnes concernées. Cependant, quels que soient le cas ou l'atteinte, le détenteur doit notifier le commissaire. Par conséquent l'appréciation du degré du risque est assujettie à l'opinion du commissaire et non pas laissée exclusivement au détenteur, qui pourrait avoir un conflit d'intérêts.

[14] Le groupe de travail a discuté de la politique consistant à obliger le commissaire à

décider si la notification était appropriée. Cette fonction du commissaire pourrait être lourde. En plus, elle pourrait inciter les détenteurs de données à éviter leur responsabilité en matière de notification en renvoyant tous les cas d'atteinte au commissaire pour attendre ses instructions. On a suggéré que le commissaire devrait s'occuper de mesures de sécurité et de prévention plus générales, et en aviser les détenteurs en conséquence. D'autre part, l'utilité d'une évaluation indépendante de la décision sur la notification était claire, et le commissaire aurait la compétence, et l'information au sujet des atteintes aux données personnelles, pour l'entreprendre.

[15] Le critère de notification, pour le détenteur comme pour le commissaire, est énoncé dans l'ébauche de la Loi uniforme : c'est le risque de préjudice important. Cette notion n'a pas de définition plus précise. Devrait-elle en avoir une ? Devrait-on dresser une liste de facteurs indicatifs de préjudice ou d'importance du préjudice, tels la nature de l'information ou le nombre de personnes concernées ? La réunion de 2008 a conclu que le commissaire devrait prendre en considération les coûts de la notification. Le groupe de travail hésitait à inclure ce critère, car il semble privilégier les intérêts du détenteur des données à ceux des personnes touchées par l'atteinte à la sécurité. A-t-on raison ? Le coût pour le détenteur, ou même le coût éventuel de mesures réparatrices pour ceux qui reçoivent l'avis, devrait-il être traité comme un facteur d'évaluation de l'importance du préjudice ?

[16] Comme on l'a noté ci-dessus et en 2008, ce ne sont pas tous les commissaires qui ont le pouvoir d'ordonner aux détenteurs de données de faire quoi que ce soit, ni tous les commissaires qui souhaitent un tel pouvoir. Comment donner suite à la décision du commissaire sur le besoin de notifier si celui-ci n'est pas en mesure d'ordonner l'obéissance ? Devrait-on autoriser, ou même obliger, le commissaire à publier ses décisions sur la notification ? Il serait difficile d'insister sur l'obéissance à « l'avis » du commissaire ; cet avis deviendrait alors une ordonnance.

[17] L'ébauche de Loi uniforme prévoit que le détenteur ne doit pas donner de notification si la police le lui ordonne. Malgré l'importance des besoins de l'investigation policière, peut-on donner à la police un droit sans limite d'empêcher les gens de se

protéger, parce que cela convient à l'investigation ? La réponse à cette question dépend-elle de qui a découvert l'atteinte (par exemple, le détenteur ; la personne dont les données personnelles ont fait l'objet d'un mauvais usage ; quelqu'un d'autre) ? Si la Loi uniforme ne répond pas à cette question, le détenteur de données personnelles qui n'a pas divulgué une atteinte à la sécurité à la requête de la police pourrait-il se défendre contre une accusation d'infraction à la Loi uniforme pour cette raison ?

[18] L'ébauche de Loi uniforme prévoit une sanction pour désobéissance à la Loi même (défaut de notifier le commissaire et de notifier les personnes concernées) et à une ordonnance du commissaire. Le groupe de travail a discuté de la possibilité et de la façon d'imposer ces sanctions au secteur public, et surtout à la Couronne. Devrait-on poursuivre la Couronne pour ne pas avoir donné notification d'une atteinte aux données ? Cette possibilité présente des questions d'ordre technique : l'entité assujettie à un devoir de protéger la vie privée est souvent un ministère du gouvernement, c'est-à-dire qu'elle n'est pas une personne juridique. Quoiqu'il en soit, n'est-il pas incongru de prélever une sanction financière sur un poste du Trésor pour le verser à un autre ? La Couronne devrait-elle répondre de son obéissance à la loi par un moyen autre que des sanctions pénales ? Comment préciser les organismes publics qui sont exposés à des poursuites - les sociétés d'État ? les municipalités ? - et ceux qui ne le sont pas ?

[19] La réunion de 2008 a recommandé que la Loi uniforme trouve un moyen de traiter des recours pour les personnes touchées par une atteinte, notamment les recours en matière d'évaluation du crédit. Le groupe de travail fait observer que quelques provinces ont déjà une loi sur la question. Par exemple, la Loi de l'Ontario sur les renseignements concernant le consommateur[3] permet aux consommateurs de recevoir des rapports gratuits et parfois d'exiger qu'une « alerte » soit placée dans leur dossier auprès de l'agence de renseignements. Des efforts sont en cours pour harmoniser les lois provinciales et territoriales sur ce sujet. Par conséquent, le groupe de travail préfère ne pas aborder ce sujet dans la loi sur la notification des atteintes à la sécurité.

[20] L'ébauche de Loi uniforme n'offre aucun recours civil, comme suite à la recommandation de la réunion de 2008 de ne pas interdire les recours civils, mais de ne pas prévoir non plus des dommages-intérêts légaux. Le groupe de travail devrait-il approfondir des options sur ce point ? Devrait-il considérer l'imposition de sanctions pénales ou civiles pour une atteinte à l'obligation générale d'assurer la sécurité des données personnelles, obligation que l'on retrouve dans la plupart des lois canadiennes sur la protection de la vie privée, sinon dans toutes ces lois. Comparer les dispositions des lois du Québec sur la protection de la vie privée dans le secteur public[4] et dans le secteur privé.[5]

[21] L'ébauche de Loi uniforme est muette sur les questions administratives en général. Par exemple on n'y dit rien sur les pouvoirs d'investigation du commissaire. Le groupe de travail pensait que les lois sur la protection de la vie privée ou d'autres lois applicables donnaient des pouvoirs adéquats aux commissaires pour découvrir les faits dans les cas d'espèce.

[22] Le groupe de travail sollicite des commentaires et des instructions sur n'importe quelle question soulevée dans ce rapport et dans les commentaires qui figurent dans l'ébauche de la Loi uniforme. Il se propose de continuer ses travaux enfin de présenter une Loi uniforme aux fins d'adoption en 2010. Entre-temps, il souhaite consulter les commissaires d'un bout à l'autre du pays, pour jauger l'aspect pratique de ses recommandations et leur acceptabilité. Nombre de commissaires ont exprimé leur opinion dans des documents publics, dont plusieurs sont cités dans le rapport de 2008 présenté à la Conférence ; en outre, des administrations publiques ont des directives internes pour gérer les données qu'elles détiennent.[6] Il est moins clair de savoir dans quelle mesure le groupe de travail ou bien la Conférence devraient s'aligner sur des expressions de volonté politique. On note, en terminant, que le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des Communes a décidé récemment de ne pas se prononcer sur les

observations qu'il avait reçues de la part de la Commissaire à la protection de la vie privée du Canada et de l'Association du Barreau canadien, qui recommandaient toutes deux des obligations plus strictes de notification.[7]

---

1 Le rapport de la réunion de 2008 est en ligne : http://www.ulcc.ca/fr/poam2/Joint%20ID%20theft%20Working%20Group%20Report%20ULCC2008_FR.pdf. La résolution adoptée à la réunion est en ligne : http://www.ulcc.ca/fr/poam2/index.cfm?sec=2008&sub=2008f. Voir le paragraphe 10.

2 Le cadre plus large était esquissé dans le rapport de 2008. Voir en particulier les paragraphes [104] à [108].

3 L.R.O. 1990, ch. C.33, articles 12, 12.1, 12.2 et 12.3.

4 L.R.Q. c. A-2.1, art. 63.1 et 162.

5 L.R.Q. c. P-39.1, art. 10 et 91.

6 Par exemple, les Lignes directrices sur les atteintes à la vie privée (Mars 2007) du Conseil du Trésor sont en ligne : http://www.tbs-sct.gc.ca/atip-aiprp/in-ai/in-ai2007/breach-atteint-fra.asp

7 *La* Loi sur la protection des renseignements personnels *: premiers pas vers un renouvellement*, juin 2009 est en ligne : http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=3973469&Mode=1&Parl=40&Ses=2&Language=F. Voir l'analyse de la « modification rapide numéro 12 ».

CONFÉRENCE POUR L'HARMONISATION DES LOIS AU CANADA

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

Ébauche de travail

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 ajoutée, 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.

On suppose que les Lois auxquelles la partie proposée pourrait être ajoutée comprennent déjà des définitions de «renseignements personnels» ou de termes semblables, comme «renseignements personnels sur la santé», aux fins de la protection de la vie privée. De plus, on suppose que ces lois prévoient la nomination d'un agent ou d'un commissaire qui est investi d'importantes responsabilités consistant à faire respecter les dispositions de la Loi portant sur la protection de la vie privée. Les termes «renseignements personnels» et «commissaire» sont utilisés dans la partie proposée en supposant que ceux-ci ou des termes équivalents sont définis dans la loi existante. Dans le cas d'une autorité législative qui n'a pas l'équivalent d'un agent de la protection de la vie privée ou d'un commissaire à la protection de la vie privée, les mentions de «commissaire» peuvent être remplacées par celles d'une autre personne appropriée, telle que le ministre ou son délégué ou un fonctionnaire qui a des responsabilités connexes.

On suppose également qu'une loi (ou une partie d'une loi) à laquelle la partie proposée pourrait être ajoutée 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 entités à caractère public. Dans d'autres cas, l'application sera plus générale. Tel qu'il est utilisé dans la partie proposée, le terme «entité» s'entend des entités qui sont assujetties à la loi existante ou à la partie pertinente de celle-ci en ce qui concerne les renseignements personnels que détient l'entité.

La partie proposée est désignée «partie X» et commence à l'article 100.

Les suppositions portent sur les deux premières recommandations énoncées aux paragraphes 11 et 13 du rapport de 2008, et la dernière recommandation énoncée au paragraphe 62.

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

PARTIE X
NOTIFICATION DES ATTEINTES À LA PROTECTION DES DONNÉES

Détenteur de renseignements personnels

100. Pour l'application de la présente partie, des renseignements personnels sont détenus par une entité si la présente loi lui attribue des responsabilités relatives à l'utilisation, à la conservation, à la divulgation ou à la consultation des renseignements.

REMARQUE : Voir le rapport ci-dessus aux paragraphes [10] et [11], qui traitent du but de cette disposition et des questions qui en relèvent.

Consultation ou divulgation non autorisée

101. (1) Le présent article s'applique si une entité sait ou a des motifs de croire que des renseignements personnels qu'elle détient ont été consultés ou divulgués contrairement à ce qu'autorise la présente loi.

REMARQUE : 1. Le passage «consultés ou divulgués contrairement à ce qu'autorise la présente loi» vise à rendre l'esprit du libellé contenu dans la recommandation 19 du rapport présenté à la réunion de 2008 : «consultés ou communiqués de manière inappropriée».

2. Les mots «a des motifs de croire» constituent un critère-seuil peu élevé, qui tient compte du texte précédant la recommandation.

Avis obligatoire

(2) Si la consultation ou divulgation non autorisée présente un risque de préjudice important pour les personnes auxquelles se rapportent les renseignements, l'entité les avise promptement de la consultation ou de la divulgation.

REMARQUE : Les articles 101 et 102 tiennent compte des recommandations énoncées aux paragraphes 19, 29, 38, 41 et 44 du rapport présenté à la réunion de 2008, avec la différence importante que l'entité est tenue, aux termes du paragraphe 101 (2) de l'avant-projet, d'aviser les personnes touchées sans avoir reçu d'ordre du commissaire. Il n'en demeure pas moins que le commissaire peut ordonner à l'entité de donner notification : voir le paragraphe 103 (3).

Obligation de faire rapport au commissaire

(3) L'entité dépose promptement auprès du commissaire un rapport en ce qui concerne toute consultation ou divulgation non autorisée.

Contenu du rapport

102. (1) L'entité veille à ce que le rapport déposé en application du paragraphe 101 (3) :

a) contienne le nom et les coordonnées de la personne qui dépose le rapport au nom de l'entité;

b) contienne des renseignements et des documents concernant les circonstances de la consultation ou de la divulgation des renseignements personnels, notamment des renseignements et des documents qui pourraient être utiles pour évaluer le risque de préjudice pour les personnes auxquelles se rapportent les renseignements;

c) contienne l'évaluation par l'entité du risque de préjudice associé à la consultation ou à la divulgation des renseignements personnels;

d) décrive les mesures que l'entité a prises, le cas échéant, pour aviser les personnes auxquelles se rapportent les renseignements;

e) indique les corps de police qui ont été avisés, le cas échéant, de la consultation ou de la divulgation.

Renseignements supplémentaires

(2) Dans le rapport exigé par le paragraphe 101 (3) ou dans un ou plusieurs autres rapports, l'entité informe le commissaire de ce qui suit :

a) les mesures que l'entité a prises, le cas échéant, pour limiter les conséquences de la consultation ou divulgation non autorisée;

b) les mesures que l'entité a prises, le cas échéant, pour empêcher que ne se reproduise une consultation ou divulgation non autorisée;

c) les mesures que l'entité a prises, le cas échéant, pour aider les personnes qui ont reçu un avis aux termes du paragraphe 101 (2) à se protéger;

d) les plans que l'entité a formés, le cas échéant, en vue de prendre les mesures du genre visé aux alinéas a), b) et c).

Autres rapports

(3) Le commissaire peut ordonner que l'entité dépose des rapports supplémentaires, qui, selon lui, pourraient l'aider à remplir ses obligations aux termes de l'article 103 et l'entité se conforme promptement à l'ordre.

Décision du commissaire

103. (1) Le commissaire qui reçoit un rapport d'une entité aux termes du paragraphe 101 (3) en ce qui concerne la consultation ou divulgation non

autorisée de renseignements personnels décide si un préjudice important risque d'être causé aux personnes auxquelles se rapportent les renseignements.

Idem

(2) S'il décide, aux termes du paragraphe (1), qu'un préjudice important risque d'être causé aux personnes auxquelles se rapportent les renseignements, le commissaire décide si les mesures que l'entité a prises, le cas échéant, pour aviser des personnes sont suffisantes.

Ordre d'aviser

(3) S'il décide, aux termes du paragraphe (2), que les mesures que l'entité a prises, le cas échéant, pour aviser des personnes sont insuffisantes, le commissaire ordonne à l'entité de prendre les mesures qu'il estime suffisantes pour aviser ces personnes.

Idem

(4) L'entité se conforme promptement à l'ordre donné aux termes du paragraphe (3).

Avis à la police

(5) S'il estime que les circonstances justifient l'avis donné au corps de police compétent de la consultation ou de la divulgation et que l'entité ne l'a pas déjà fait, le commissaire :

a) soit avise le corps de police compétent;

b) soit ordonne que l'entité avise le corps de police compétent.

Idem

(6) L'entité se conforme promptement à l'ordre prévu à l'alinéa (5) b).

Ordre de la police de ne pas aviser

104. Malgré le paragraphe 101 (2) ou un ordre donné en application du paragraphe 103 (3), une entité se conforme à l'ordre de la police de ne pas aviser les personnes de la consultation ou de la divulgation de renseignements personnels.

REMARQUE : Voir le rapport ci-dessus au paragraphe [17] pour des commentaires et des questions sur cette disposition.

Règlements : contenu de l'avis

105. Le lieutenant-gouverneur en conseil peut, par règlement, régir le contenu d'un avis donné en application du paragraphe 101 (2) ou 103 (3) à

l'égard de la consultation ou divulgation non autorisée de renseignements personnels, notamment exiger qu'un 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 la consultation ou divulgation non autorisée;

d) les mesures que l'entité a prises, le cas échéant, pour limiter les conséquences de la consultation ou divulgation non autorisée;

e) les mesures que l'entité a prises, le cas échéant, pour empêcher que ne se reproduise une consultation ou divulgation non autorisée;

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

g) les mesures que les personnes qui ont reçu un avis pourraient prendre, le cas échéant, pour se protéger.

Infraction

106. (1) Est coupable d'une infraction l'entité qui contrevient au paragraphe 101 (2) ou (3), à l'article 102, au paragraphe 103 (4) ou (6), à l'article 104 ou à un règlement pris en application de l'article 105 et passible, sur déclaration de culpabilité, d'une amende maximale de 25 000 $ si l'entité est un particulier et d'une amende maximale de 500 000 $ si l'entité est une personne morale.

Idem

(2) Si l'entité qui commet une infraction prévue au paragraphe (1) est une personne morale, ses dirigeants ou administrateurs qui ont ordonné ou autorisé la commission de l'infraction ou qui y ont consenti ou participé sont parties à l'infraction, en sont coupables, que la personne morale ait été poursuivie ou non pour cette infraction, et sont passibles, sur déclaration de culpabilité, d'une amende maximale de 25 000 $.

REMARQUE : L'article 106 tient compte de la recommandation énoncée au paragraphe 52 du rapport de 2008.