

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.

«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.

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.

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 prévus par règlement.

Modalités de la déclaration

(5) La déclaration exigée par le paragraphe (1) doit être faite selon les modalités réglementaires.

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.

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, si cela est possible, des mesures pour réduire le risque de préjudice qu'il pourrait subir du fait de l'atteinte à la vie privée ou pour atténuer un tel préjudice;
- b) tout autre renseignement réglementaire.

Modalités de l'avis

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

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

- c) doit être donné selon les modalités réglementaires.

Exception

(6) S'il est prescrit par règlement des circonstances dans lesquelles il n'est pas possible de donner l'avis au particulier directement, l'avis doit, dans ces circonstances, lui être donné indirectement.

Commentaire : La rédaction des règlements devrait donner aux organisations une direction des plus claires sur les circonstances dans lesquelles un avis indirect suffira.

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 précisée par règlement.

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 pour 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.

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.

Divulgarion 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 remplacée par le présent article. Sans une prohibition de la divulgation, la permission de la présente disposition va sans dire; il ne serait pas nécessaire de l'inclure l'article dans la loi de mise en œuvre de la loi uniforme.

Si le responsable de la protection de la vie privée n'est pas compétent pour donner d'ordres, la rédaction et l'opération de l'alinéa a) seront à revoir, bien que le pouvoir de divulgation puisse rester dans la forme prévue ci-haut.

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) Lorsqu'une organisation est poursuivie 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.

Défense

(4) 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.

Peine

(5) 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

(6) 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.

Règlements

108. (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.